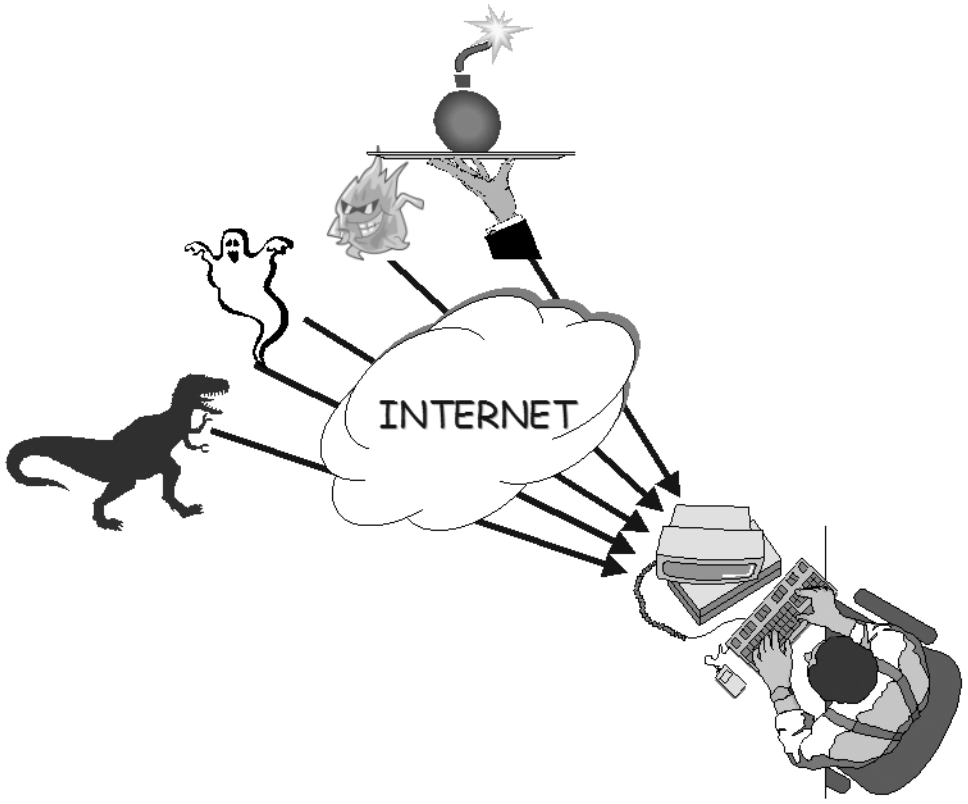
chapitre 4



Les réseaux, autoroutes de l'intrusion

Il faut constater avec regrets que l'objet essentiel des réseaux n'est pas d'acheminer des flux honnêtes. Il est très difficile d'aborder le délicat problème de la protection des ordinateurs sans une bonne perception de l'état d'esprit du pirate et de ses pratiques d'intrusion.

SOMMAIRE

MOTS-CLÉS

- IP
- TCP, UDP, ICMP
- Telnet, FTP, TFTP, SNMP
- NetBIOS
- HTTP
- WI-FI

Votre PC est une formidable machine à communiquer. On pourrait le comparer à une grande ville reliée au monde extérieur par l'intermédiaire de 65 000 routes partant dans toutes les directions ! Chaque route quitte la ville par une porte pouvant être ouverte à la circulation dans les deux sens. Poursuivons notre métaphore : chaque route impose à celui qui l'emprunte l'utilisation d'une langue ou d'un dialecte particulier, que seuls quelques spécialistes de la ville, en charge de la communication, sont capables de comprendre. Quelle aubaine pour les trafiquants polyglottes ! Sous couvert d'une crédibilité accordée d'office (par le seul fait qu'ils sachent communiquer dans ces langages hermétiques), ils se glissent incognito dans l'immense flot des échanges, exploitent à leur profit cette incroyable diversité des moyens de communication, et font librement circuler, au nez et à la barbe des douaniers qui ne comprennent rien à ce qu'ils racontent, toutes sortes de marchandises – y compris les plus douteuses. Ils s'installent et dissimulent leur quartier général au cœur de cette ville immense, spolient subrepticement ses richesses, acquièrent le pouvoir et prennent petit à petit son contrôle.

Votre PC ressemble vraiment beaucoup à cette ville. C'est une machine capable de dialoguer avec le monde entier à travers plus de 65 000 ports d'entrée/sortie. Chaque port est associé à un protocole de communication spécifique capable d'établir, en un clin d'œil, un lien direct d'égal à égal avec n'importe quel ordinateur situé sur Internet. Avec un tel dispositif, comment les tricheurs pourraient-ils résister et ne pas détourner à leur profit des protocoles qui ne demandent qu'à communiquer, infiltrer votre machine et s'installer au cœur de votre système ?

Contrairement aux informaticiens, les entreprises en bâtiment spécialisées dans la construction des banques le savent très bien : il ne suffit pas de construire des murs épais ou de concevoir des systèmes d'alarme sophistiqués, encore faut-il prévoir les stratagèmes des tricheurs, qui sauront par exemple exploiter élégamment la cartographie des égouts ou la situation des toilettes du bâtiment d'à côté. Il ne faut jamais oublier que nos vrais adversaires, ceux qui conçoivent les redoutables outils d'intrusion prêts à l'emploi, sont de grands professionnels de l'informatique et des réseaux. Ils connaissent à fond les détails de l'implémentation (et les faiblesses) des souches de protocoles IP de chaque constructeur. Ils maîtrisent les systèmes d'exploitation – y compris les fonctions système non documentées. Ils désossent les applications sous toutes leurs coutures, ils étudient les spécifications, analysent les codes sources ou désassemblent les exécutables, et finissent tôt ou tard par découvrir la faille fatale, celle dont l'exploitation mène à la reddition pure et simple de la machine distante. Ils échangent entre eux le fruit de leurs précieuses découvertes, capitalisent sur cette connaissance en produisant avec brio et efficacité des outils passés maîtres dans l'art de tri-

cher, de tromper, d'abuser, de contourner, d'infiltrer et de tenir en échec bien des lignes de défense. À l'heure actuelle, le monde de l'intrusion dispose d'une force de frappe mettant en jeu des techniques d'une incroyable complexité, dont les informaticiens professionnels, pour la plupart, ignorent jusqu'à l'existence.

C'est la raison pour laquelle une protection efficace contre les intrusions – et la manière dont il faut configurer les pare-feux – découle de concepts difficiles à appréhender pour l'utilisateur non informaticien. Nous présenterons de façon simple quelques méthodes utilisées pour détourner les protocoles les plus ciblés, afin de mettre en lumière la manière dont agissent les pirates, et de vous enseigner les principaux réflexes à acquérir pour vous défendre. Cette présentation a en outre l'objectif de vous préparer au sujet des pare-feux, traité au chapitre suivant.

Messagerie, forums ou navigation sur Internet : les risques induits par les protocoles de transmission

Rôle majeur des protocoles « IP » dans les communications sur Internet

Sans entrer dans les détails techniques, vous avez certainement entendu parler des réseaux dits « IP », et vous savez que toutes les communications sur Internet les utilisent. Pour configurer son pare-feu en vue de se protéger efficacement contre les attaques venues d'Internet, il est indispensable de comprendre succinctement ce que sont les réseaux IP et comment ils fonctionnent.

Adressage IP

Il est important que vous disposiez de connaissances minimales en adressage IP : vous ne pourrez vous en passer au cours de ce chapitre et lorsque vous vous attaquerez à la configuration de votre pare-feu.

La notion d'adresse IP est absolument fondamentale ; elle est considérée comme l'adresse postale, le numéro de téléphone ou le numéro de fax dans le monde des ordinateurs. En IPv4, une adresse IP n'est ni plus ni moins qu'un simple nombre de 32 bits. Voici par exemple l'adresse IP d'un ordinateur :

```
11001000010001011110000001010001
```

Hmm !… Vous en conviendrez, ce nombre est plutôt difficile à retenir. Afin de rendre son utilisation plus commode, il a été convenu de longue date de représenter une adresse IP sous la forme « w.x.y.z », où w, x, y et z sont des valeurs décimales comprises entre 0 et 255. Pour convertir l'adresse précédente en notation décimale à points, on la divise d'abord en groupes de 8 bits, qu'on convertit en leur équivalent décimal :

- Notation binaire : 11001000 01000101 11100000 01010001
- Notation décimale : 200 69 224 81

L'adresse IP de l'ordinateur désigné ci-dessus est donc notée « 200.69.224.81 ». Ceci est effectivement beaucoup plus exploitable que « 11001000010001011110000001010001 ».

En fait, une adresse IP regroupe deux informations essentielles : le numéro du réseau et le numéro de la machine à l'intérieur de ce réseau. On distingue trois cas :

- Le nombre de gauche est compris entre 0 et 126 : c'est un réseau de classe A. Le réseau est identifié par le premier nombre et la machine par les trois suivants. Il existe donc seulement 127 réseaux de classe A dans le monde, mais ils sont gigantesques puisqu'ils peuvent contenir environ 16 millions d'ordinateurs (2^{24}) chacun.
- Le nombre de gauche est compris entre 128 et 191 : c'est un réseau de classe B. Le réseau est identifié par les deux premiers nombres et la machine par les deux suivants. Il existe 16 384 réseaux de classe B, comptant chacun jusqu'à 65 636 hôtes (2^{16}).
- Le nombre de gauche est compris entre 192 et 223 : c'est un réseau de classe C. Le réseau est identifié par les trois premiers nombres et la machine par le dernier. Il peut y avoir 2 097 152 réseaux de classe C pouvant héberger un maximum de 254 hôtes (2^8), l'adresse 255 étant réservée pour la diffusion.

À RETENIR Adresse commençant par 127

127 est une adresse réservée pour le « bouclage », c'est-à-dire pour qu'une machine puisse se référencer elle-même.

Transmission d'informations avec le protocole IP

IP (Internet Protocol) est en quelque sorte aux ordinateurs ce que le fax, DHL ou UPS est à chacun d'entre nous : un service express qui permet d'envoyer et de recevoir de l'information (un lettre, un colis, une transaction commerciale) vers et en provenance de n'importe quel ordinateur dans le monde.

Très schématiquement, lorsque vous désirez envoyer une information vers un ordinateur situé quelque part sur la planète (un message électronique, un morceau de musique, une photo, un ordre d'achat, etc.), votre application se contente de placer cette information à l'intérieur d'un colis et d'écrire en gros sur ce colis l'adresse de votre correspondant. Cela se passe exactement comme avec les services postaux, sauf que, dans le

monde virtuel, l'adresse est matérialisée par l'adresse IP du correspondant, par exemple 172.27.5.202 (pour simplifier, partons du principe que l'adresse IP d'un destinataire est unique au monde).

Ce colis est ensuite déposé dans une boîte aux lettres située à l'intérieur de votre ordinateur ; disons qu'il s'agit par exemple de la case *courrier-départ*.

À ce stade, voici comment on pourrait représenter (très schématiquement, cela s'entend) la suite des événements : un coursier rapide, dont l'une des tâches consiste à inspecter en permanence le contenu de votre case *courrier-départ*, attrape votre colis au moment même où vous le déposez dans la boîte aux lettres. Tel un joueur de rugby, il le lance, à une vitesse à peine imaginable, vers son coéquipier le plus proche sur la route des buts. Les buts, ici, matérialisent votre correspondant, mais à la différence du rugby, il peut y en avoir dans toutes les directions et à des distances très rapprochées ou très éloignées. En outre, nous ne parlerons pas encore de l'existence d'une équipe adverse, qui pourrait à la rigueur symboliser la présence de pirates ; nous verrons cela plus tard. Autre point qu'il convient de noter : malgré la rapidité extrême avec laquelle le coursier vient de faire partir votre colis, considérez qu'il a eu le temps au préalable de déterminer, parmi ses coéquipiers les plus proches, lequel était situé sur la route des buts à atteindre. Lorsque le coéquipier suivant dans la chaîne se saisit de votre colis, le coursier considère que son travail est terminé : peu lui importe comment la transmission se poursuivra, il part du principe qu'il a bien fait son travail et retourne surveiller le contenu des boîtes aux lettres.

La suite est à peu près analogue au cheminement du ballon ovale sur le terrain (à condition bien sûr que l'équipe ne soit pas constamment dérangée par ses adversaires) : votre colis passe à la vitesse de l'éclair de joueur en joueur jusqu'à atteindre son but final, c'est-à-dire la case *courrier-arrivée* de votre correspondant. Tel le coursier que nous évoquions, chaque joueur se préoccupe d'envoyer votre colis vers le joueur situé immédiatement après lui dans la chaîne qui vous relie à votre correspondant, et s'en désintéresse tout à fait dès qu'il l'a transmis.

Réseau IP

Chaque joueur tient en quelque sorte le rôle de centre de tri ; cette fonctionnalité, sur un réseau de communication tel qu'Internet, est assurée par un équipement appelé « routeur ». Internet est en effet constitué par un maillage extrêmement complexe de routeurs, dont la tâche essentielle consiste à « router », à acheminer vos données à travers le réseau, en se servant de la simple information que vous leur avez fournie : l'adresse IP de votre correspondant. Notez au passage que ces routeurs (certes, avec l'aide des applications) effectuent ce travail avec un certain talent, puisqu'il est rare qu'une information se perde en cours de route.

Entre le moment où le coursier vient se saisir de votre colis sur votre ordinateur et celui où le joueur en bout de chaîne le dépose sur l'ordinateur de votre correspondant, votre message aura peut-être beaucoup voyagé. Toutefois, peu importe l'itinéraire suivi ; que votre paquet emprunte le réseau Transpac, les faisceaux de lignes posées sur le fond de l'Atlantique, le réseau satellitaire, le réseau téléphonique via modem ou des artères haut débit, ce qui importe c'est que le réseau public connaisse votre adresse IP et celle de votre correspondant. L'acheminement d'un message fait appel à des mécanismes complexes de transmission, mais dont il est inutile de connaître les subtilités, puisque les routeurs s'en chargent pour nous avec une maîtrise exceptionnelle.

Voici donc, de façon simplifiée, en quoi consiste le réseau IP : tel un tissu organique observé au fort grossissement du microscope, il s'agit d'un gigantesque maillage déployé autour de la planète, constitué de câbles et de liaisons radio interconnectés, et desservant une infinité de branches dont vous êtes l'une des extrémités. Ce maillage s'accompagne d'un service universel installé absolument partout dans le monde, sur chaque appareil contenant un microprocesseur : le service IP, capable de traiter, d'envoyer ou de recevoir n'importe quel message doté d'une adresse IP. Vous pouvez dialoguer avec n'importe quelle autre extrémité dès que vous connaissez son adresse IP.

Protocole TCP

Le service (ou la couche) IP est donc le service de base qui sert à acheminer « quelque chose » vers n'importe quel ordinateur dans le monde. Dotés d'un moyen d'une telle puissance, les concepteurs d'IP furent tentés d'aller au delà, de définir, en s'appuyant sur cette infrastructure de communication, des protocoles capables de rendre des services bien plus élaborés que la simple transmission de l'information.

Citons par exemple le plus connu : le fameux protocole TCP, de TCP/IP. TCP (Transport Control Protocol) est, par certains côtés, comparable au service de transmission en recommandé. En effet, le schéma que nous venons de décrire souffre d'une lacune évidente : IP offre les mécanismes de transmission d'un message d'un ordinateur à un autre via des routeurs, mais rien dans ce protocole ne garantit que le message soit arrivé à bon port. Si un paquet IP se perd quelque part sur le réseau, ou s'il est endommagé au cours de son transfert, l'expéditeur n'en sera pas informé. IP n'offre pas de service fiable.

C'est là qu'intervient TCP : lorsque votre ordinateur désire envoyer un message, il peut très bien faire appel à ce protocole au lieu de se servir directement de IP. Avant d'émettre votre message, TCP contacte au préalable votre correspondant (en fait, le TCP de votre correspondant) afin de se

mettre d'accord avec lui sur le fait que vous allez échanger de l'information. Si les deux TCP sont d'accord pour communiquer, ils négocient ensemble les meilleurs paramètres possibles pour optimiser la transmission de cet échange ; votre TCP ouvre en quelque sorte avec celui de votre correspondant un chemin virtuel temporaire qui relie les deux ordinateurs comme s'ils disposaient d'une ligne dédiée pour faciliter les futurs échanges.

Bien sûr, TCP se sert de IP au cours de cette phase préalable d'établissement de session : dans ce cas précis, IP est utilisé par TCP non pas pour échanger de l'information utilisateur, mais pour acheminer des paramètres « d'administration ». Une fois que les deux extrémités se sont mises d'accord, les échanges d'information utilisateur peuvent commencer. Toutefois, la grande différence avec IP, c'est que votre TCP entretient un dialogue constant avec le TCP distant, afin de contrôler le bon déroulement des échanges : il s'assure que les messages arrivent bien à destination, dans le bon ordre (car un message peut être découpé en plusieurs paquets IP), et ne subissent pas d'altération durant leur transfert. TCP est chargé de demander à votre ordinateur de réexpédier les éventuels paquets perdus. Grâce à ce protocole, vous êtes sûr que l'information arrive à bon port, et sans erreur.

Couches fonctionnelles : modèle OSI

Comme vous le constatez, TCP se préoccupe de la qualité du transport de l'information de bout en bout ; il utilise pour cela un autre logiciel comme moyen d'acheminement de l'information sur un réseau, un logiciel de « plus bas niveau » : IP. TCP est donc une couche logicielle située « au dessus » de la couche IP. C'est la raison pour laquelle on a coutume de représenter les concepts de télécommunications sous la forme d'un empilement de couches fonctionnelles, appelé modèle de référence OSI. Pour mieux situer les services réseau et comprendre plus facilement la mécanique compliquée des échanges – et des attaques – sur Internet, évoquons quelques instants ce modèle.

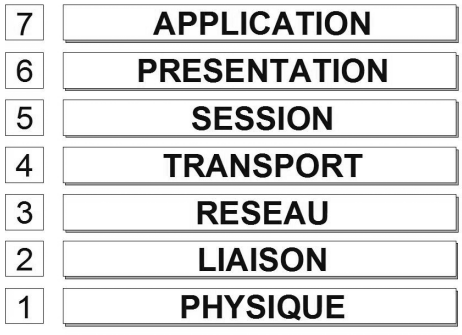


Figure 4–1
Modèle de référence OSI

Le modèle OSI définit une architecture générique censée décrire les principes de fonctionnement d'un système de communication (par exemple, une session entre votre ordinateur et un serveur sur Internet). Même si cette vision a quelque peu vieilli (elle fut proposée bien avant l'adoption généralisée des protocoles de communication utilisés à l'heure actuelle), bon nombre de concepts demeurent toujours valables. En observant la figure 4-1, vous constatez que ce modèle est constitué d'une superposition de sept couches fonctionnelles, chacune jouant un rôle bien précis dans le processus global de communication. Pourquoi adopter spécialement un modèle en « couches » ? Pour décrire ce qui se passe dans la réalité, tout simplement : l'expérience montre qu'une communication est bâtie en fait sur une série de processus disjoints et complémentaires s'appuyant les uns sur les autres. Voyons à quoi correspondent, dans le monde Internet, ces couches mystérieuses du modèle OSI.

Couches 1 (physique) et 2 (liaison)

Nous ne parlerons pas beaucoup des couches 1 et 2, le niveau « physique » et le niveau « liaison ». Elles sont matérialisées physiquement par deux éléments :

- votre carte ethernet ou votre carte modem, grâce à laquelle l'ordinateur peut se raccorder avec le médium physique du réseau ;
- son pilote, logiciel permettant à cette carte d'envoyer et de recevoir des trames sur ce médium physique, en un mot de communiquer avec d'autres cartes raccordées au même réseau.

Lorsque vous achetez votre ordinateur et que celui-ci comporte une carte réseau, vous disposez, sans le savoir, des deux premières couches du modèle OSI.

Couche 3 (réseau)

La couche 3 s'appuie sur la capacité à émettre et à recevoir des trames (couches 1 et 2), pour acheminer des paquets d'information sur le réseau, jusqu'à l'utilisateur final – d'où son nom, couche « réseau ».

Dans le monde Internet, le niveau 3 est universellement couvert par la couche IP. Cette dernière est implantée bien sûr sur votre poste (car lorsque vous achetez un ordinateur muni d'une carte ethernet, il y a de fortes chances pour que celui-ci soit livré avec la pile IP), mais aussi partout sur le réseau, à commencer par les routeurs, les serveurs distants et toute machine censée communiquer sur le réseau. La couche IP est transversale ; c'est en quelque sorte le dénominateur commun, la « plateforme » universelle, le ciment qui lie toutes les machines entre elles sur Internet.

Couche 4 (transport)

Vous saurez de même trouver la place de la couche TCP : elle se situe au dessus de IP, donc au niveau de la couche 4, la couche « transport ». C'est logique : TCP se soucie principalement de la façon dont les informations sont transportées de bout en bout entre l'expéditeur et le destinataire. Beaucoup d'applications se servent de TCP. Par exemple, les messageries SMTP utilisent les services présumés fiables de TCP (elles sont associées par exemple au port TCP 25). Un autre protocole bien connu d'Internet utilise TCP : le protocole HTTP. Il est associé généralement au port TCP 80.

Couche 7 (application)

Tout comme TCP se sert de IP, il existe d'autres protocoles de plus haut niveau qui, au lieu de s'appuyer directement sur la couche IP, préfèrent utiliser les services fiables de TCP pour communiquer. Autrement dit, il existe des protocoles situés « au dessus » de TCP dans l'empilement des couches. Nous sommes au cœur du modèle OSI : prenez l'exemple du navigateur Internet que vous connaissez bien. Vous êtes habitué à le manier pour accéder, entre autres, à des pages HTML sur un serveur web ; pour vous, ce navigateur est perçu comme une application, au même titre que la messagerie, le traitement de texte ou le simulateur de vol. Toutefois, pour rendre le service que vous attendez, ce navigateur doit dialoguer avec le serveur web distant, ce qui s'effectue dans un langage particulier. Il s'agit là encore d'un protocole de communication, à ceci près que celui-ci manipule des concepts de niveau applicatif : des URL, des images, des scripts, etc. C'est donc un protocole « applicatif », de niveau 7 dans le modèle OSI. Bien sûr, vous l'avez deviné, nous sommes en train de parler de HTTP (ou de HTTPS lorsque les échanges ont lieu dans un mode sécurisé).

Modèle simplifié TCP/IP

Si l'on considère l'empilement des différentes couches protocolaires intervenant dans le cadre du Web, nous avons au sommet l'application matérialisée sur votre poste de travail par le navigateur. Ce dernier s'appuie sur le protocole de niveau 7 HTTP (ou HTTPS), lequel s'appuie sur TCP, lui-même adossé à IP qui, à son tour, utilise les ressources de la carte réseau (couches 1 et 2). Voici donc exposée de manière simplifiée, la pile complète des protocoles mis en œuvre lorsque vous surfez sur Internet.

Avec les autres applications, c'est exactement la même chose. Par exemple, votre client de messagerie – qui est une application – se sert des protocoles de niveau 7 SMTP, POP3 ou IMAP4 pour communiquer ;

AVANCÉ Modèle OSI et modèle TCP/IP

Dans le monde IP, les concepts définis initialement par l'OSI au niveau des couches 5 (Session) et 6 (Présentation) sont généralement implémentés au sein des protocoles de niveau 7 (voir figure 4-2), voire au niveau des applications.

ceux-ci s'appuient sur TCP, lequel utilise IP, etc... Si l'on représentait l'empilement de ces différentes couches protocolaires, le schéma obtenu donnerait une vision particulière du modèle de référence OSI appliquée au monde Internet (figure 4-2).

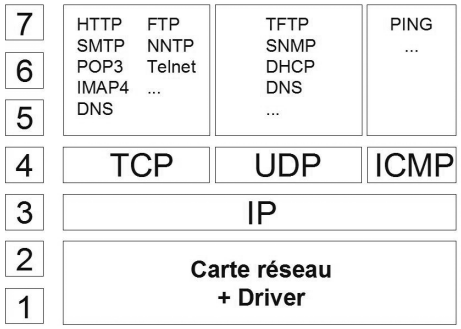


Figure 4–2
Modèle de référence OSI appliqué au monde IP

Il est important de conserver ce schéma en tête car cela vous aidera à comprendre la philosophie des attaques sur Internet, la diversité des mesures à prendre pour se protéger efficacement, ou les différences qui existent entre les pare-feux.

Protocoles UDP et ICMP

Avant de clore cette longue introduction, n'oublions pas d'évoquer les protocoles UDP et ICMP : IP, TCP, UDP et ICMP sont des protocoles fondamentaux d'Internet que nous aborderons sans cesse dans la suite de ce chapitre et au chapitre suivant.

Comme nous l'avons vu, TCP rend des services fort utiles sur le plan de la fiabilité des communications. Toutefois, il ne présente pas toujours que des avantages car, il ne faut pas l'oublier, la gestion d'une session a un coût en terme de performances : passer par TCP ralentit indiscutablement les échanges. C'est la raison pour laquelle, lorsque les contraintes de performances sont élevées, ce qui est souvent le cas pour les fonctions système ou proches du système, les développeurs optent pour une approche plus souple : au lieu de confier la gestion de la transmission à TCP, l'application ou le service se charge elle-même (ou lui-même) des paquets perdus, endommagés ou reçus dans le désordre et utilise un accès beaucoup plus direct à IP. Le service définit ainsi généralement une procédure de gestion beaucoup plus allégée – donc plus rapide – que les procédures luxueuses de TCP. Cet accès direct s'appelle UDP.

UDP (User Datagram Protocol) fournit une grande partie des services intéressants de TCP, comme le fait d'associer un numéro de port à un pro-

gramme. Toutefois, UDP n'est pas un service fiable, il n'est pas orienté connexion et ne garantit pas l'intégrité des données de bout en bout, ce qui oblige le protocole qui l'utilise à combler lui-même cette lacune. En revanche, UDP est idéal pour transmettre ou recevoir des datagrammes (c'est comme cela que l'on nomme les paquets IP avec UDP), spontanément, sans formule de politesse exaspérante susceptible de ralentir les échanges. De nombreux services réseau utilisent UDP, comme le protocole DHCP (attribution dynamique des adresses IP aux postes du réseau) ou SNMP (gestion de réseau). Notez que le protocole DNS utilise à la fois TCP et UDP (DNS est associé aux ports TCP 53 et UDP 53).

ICMP (Internet Control Message Protocol) est quant à lui entièrement dédié à la gestion des problèmes qui surviennent sur un réseau : c'est grâce à lui que les machines ou les passerelles peuvent rendre compte des anomalies de fonctionnement. Par exemple, pour vérifier si une machine distante connectée au réseau est bien « visible » de votre poste, un moyen simple consiste à effectuer un `ping` de cette machine à travers le réseau, c'est-à-dire à lancer la commande :

```
ping adresse_IP_machine_distance
```

`ping` fait ni plus ni moins appel au protocole ICMP et se contente tout simplement d'envoyer une trame ICMP `ECHO` à cette machine (en quelque sorte un « coucou es-tu là ? »), en attendant en retour une trame de type ICMP `REPLY` (« Oui, je suis là »). Si vous recevez effectivement cette trame ICMP `REPLY`, cela veut dire que les deux machines vont pouvoir communiquer.

Si d'aventure vous tentiez d'envoyer une requête vers une adresse qui n'existe pas, il y a de fortes chances pour que le réseau vous retourne un message ICMP de type `DESTINATION UNREACHABLE`, vous informant ainsi de la raison pour laquelle votre requête est restée sans réponse ; cette simple information peut en effet vous faire gagner un temps considérable.

Pour éviter les congestions du réseau, chaque paquet IP contient dans son en-tête une information « durée de vie », ou `TTL` en anglais (Time To Live). Initialisé à une valeur donnée (128 la plupart du temps), ce champ est décrémenté chaque fois qu'il passe au travers d'un nœud du réseau. Si ce paquet n'a pas atteint sa destination finale avant que son `TTL` soit égal à zéro, il est impitoyablement détruit par le nœud qui le voit transiter. Toutefois, dans sa grande bienveillance, le routeur vous informe de son sinistre forfait. Là encore, ICMP est mobilisé et le routeur vous envoie un message ICMP `TIME EXCEEDED`, qui contient toutes les références au paquet détruit ; vous pouvez ainsi prendre les mesures adéquates (pas vous bien sûr, mais le service émetteur), comme réémettre ce paquet.

ICMP renferme bien d'autres messages de contrôle, qu'il serait fastidieux de décrire dans cet ouvrage. Il s'agit d'un protocole essentiellement orienté administration, et votre intérêt pour ses activités, en tant qu'utilisateur, est somme toute assez limité. Toutefois, nous allons le voir un peu plus loin (et c'est pourquoi nous abordons ce sujet), ICMP est un protocole royal pour un pirate. Ayez quelques instants l'âme d'un tricheur et voyez comment tirer parti de tous ces protocoles de communication.

Comment l'attaquant perçoit-il un protocole de communication ?

Rentrons maintenant dans le vif du sujet. Pour un attaquant, sachez qu'un protocole de communication n'est rien d'autre qu'un moyen puissant grâce auquel il est possible de faire avaler à votre ordinateur les mensonges les plus énormes ; il suffit juste de lui parler poliment.

Si vous saisissez les implications de ce propos surprenant, vous comprendrez la philosophie des attaques informatiques et saurez mettre en œuvre les vraies mesures de protection.

À travers les quelques exemples suivants, nous allons voir comment leurrer les protocoles de communication.

Attaques perpétrées via les protocoles réseau

Derrière leur apparente innocence, les protocoles IP sont de redoutables vecteurs d'intrusion

Il y a au moins deux raisons à cela. La première tient au fait que TCP/IP et les protocoles qui lui sont associés ont été conçus vers la fin des années 1970. Ils étaient à l'origine destinés au département américain de la Défense (le DARPA) et visaient à permettre aux grands systèmes centraux de la Défense de communiquer entre eux. À l'époque, personne ne parlait d'Internet public. Bien que cette suite de protocoles ait été définie pour servir un domaine hautement stratégique, les concepteurs ont jugé – à juste titre d'ailleurs – qu'il n'était pas nécessaire de prévoir de mécanismes de sécurité particuliers, cette infrastructure évoluant en circuit fermé.

TCP/IP s'est ainsi développé au fil des ans jusqu'à former le groupe de protocoles robustes et efficaces (en terme de communication, cela

s'entend) que nous connaissons aujourd'hui. Bien entendu, il n'intégrait toujours pas les mécanismes de sécurité qui n'auraient pas manqué de voir le jour s'il avait été pensé pour des réseaux ouverts. Cependant, victime de son incroyable popularité, TCP/IP s'est progressivement répandu dans les entreprises au cours des années 1980, puis s'est retrouvé, en toute logique, propulsé en première ligne lorsqu'il a fallu acheminer le trafic public du monde entier. Voilà comment la communication sur Internet repose sur des protocoles non prévus au départ pour contrer les attaquants.

La deuxième raison est évidemment liée au fait que TCP/IP est présent sur tous les ordinateurs et équipements de communication du monde entier. Les spécifications, ainsi que le code source de nombreuses implémentations des couches protocolaires de TCP/IP, sont publics et accessibles à toute personne qui a suffisamment de courage pour se plonger dans les méandres des mécanismes complexes de son fonctionnement. Bien entendu, les pirates ne s'en privent pas. Ils prennent tout leur temps pour étudier dans ses moindres détails le fonctionnement de chaque service, de chaque fonction, qu'elle soit documentée ou non. Ils s'en donnent à cœur joie, rivalisent de subtilités, trouvent parfois des astuces étonnantes, et mettent au point des mécanismes, « bruyants » ou furtifs, exploitant les faiblesses de ces protocoles, contournant les pare-feux et pénétrant ensuite des infrastructures de millions de sites. Le balayage TCP, succinctement décrit plus loin, en est un exemple, mais il en existe des dizaines d'autres.

TCP, UDP ou ICMP : des protocoles bien utiles aux pirates pour analyser une installation à distance

Exploitation de ICMP

Nous avons vu précédemment à quoi pouvait servir la commande `ping`. Imaginez par exemple qu'un pirate décide de l'exploiter pour sonder automatiquement une plage d'adresses IP qui correspond justement à celle de votre réseau 192.168.0.x. Pour parler concrètement, imaginez qu'il lance à distance les commandes suivantes :

```
ping 192.168.0.1
ping 192.168.0.2
ping 192.168.0.3
ping 192.168.0.4
ping 192.168.0.5
…
ping 192.168.0.253
ping 192.168.0.254
```

En analysant les réponses reçues, l'attaquant saura, en très peu de temps, quels sont les systèmes individuels actifs sur votre réseau. En exploitant simplement les protocoles de communication, il peut déduire une cartographie complète et précise de votre installation ; commencez-vous à percevoir le danger inhérent à ce protocole ?

Vous apprendrez très vite à contrer cette attaque grossière au chapitre suivant, mais peut-être entrevoyez-vous déjà la nécessité de restreindre sérieusement, voire d'interdire le protocole ICMP au niveau du pare-feu.

Ouverture de session TCP

Bien qu'il existe des exceptions (curieusement, le pare-feu de Windows ne permet pas de bloquer les paquets ICMP `ECHO` et `REPLY`), partons du principe que le protocole ICMP est désormais systématiquement bloqué en entrée de site ou sur votre machine unique. Cela désarme-t-il le méchant pirate ? Disons que cela lui complique un peu la vie. Il existe en effet des attaques plus sournoises qui permettent de recueillir toutes sortes d'informations précieuses sur les machines et les services actifs.

Par exemple, détaillons quelques instants le schéma dit de la « poignée de main à trois états », la procédure standard d'ouverture d'une session TCP. Lorsque votre poste client décide d'ouvrir une session avec un serveur Web distant (donc via le protocole HTTP), TCP contacte ledit serveur et entame la petite négociation suivante :

- Votre poste : « Bonjour Monsieur le Serveur, je souhaiterais ouvrir une session avec vous ».
- Le serveur : « Bonjour Monsieur le Client. D'accord pour ouvrir cette session, je suis prêt ».
- Votre poste : « Merci Monsieur le Serveur, bien reçu, nous pouvons commencer ».

À compter de ce moment, la session est ouverte, sans autres fioritures. Notez au passage comme cette procédure est simple ! De façon générale, les protocoles IP sont bâtis sur des mécanismes simples et de bon sens (peut-être est-ce là le secret de leur succès ?).

Balayage de ports

Nous avons écrit plus haut que les communications ne pouvaient avoir lieu que si le port était ouvert. Dans le cas de notre serveur Web, les communications transiteront par le protocole HTTP, le protocole du Web. Traditionnellement, tout le monde considère que le port 80 d'un serveur Web est ouvert (port associé au protocole HTTP). Dans le cas de notre poignée de main, tous les échanges se font donc sur ce port (son numéro est un champ des en-têtes TCP et UDP). Si, au lieu d'utiliser le

port 80, votre poste avait engagé une poignée de main avec ce même serveur, mais cette fois sur le port 7 561 (très rarement ouvert), il est fort probable que celui-ci ne lui eût jamais répondu.

À ce stade, vous devinez peut-être comment un attaquant peut tirer parti de ce mécanisme. Alors, avez-vous l'âme d'un tricheur ?…

Peut-être pas encore suffisamment. Alors imaginez ceci : supposez que, connaissant l'adresse IP d'une de vos machines (192.168.0.12), l'attaquant initie avec celle-ci une poignée de main, en utilisant le port numéro 1. Si ce port est fermé, l'attaquant ne recevra aucune réponse. Supposez maintenant qu'il réitère cette tentative sur le port numéro 2, et ainsi de suite jusqu'au port numéro 65 535. Il y a de fortes chances pour que cet attaquant reçoive très peu de réponses positives, puisque tous vos ports sont fermés… Tous ? sauf ceux délibérément ouverts par vos applications pour communiquer sur Internet. Supposons que l'attaquant reçoive deux réponses : une sur le port 25, l'autre sur le port 80. 65 535 requêtes, pour 2 réponses… que d'énergie gaspillée ! Certes, mais peu importe, c'est l'ordinateur qui fait le travail, et très rapidement. Au bout du compte, le pirate sait maintenant que la machine située à l'adresse 192.168.0.12 a deux ports ouverts, d'où il peut déduire que cette machine héberge votre serveur de messagerie (traditionnellement associé au port 25) et votre serveur web (port 80). Désormais, il n'a plus qu'à concocter une belle attaque, exploitant de manière éhontée la cohorte de vulnérabilités de SMTP, de HTTP et des logiciels serveurs qui les exploitent.

Cette attaque est tout simplement ce que l'on appelle un balayage de ports. Ne vous y trompez pas, c'est une attaque élémentaire, qui ne nécessite aucune compétence (une multitude d'outils existent). Vous saurez la contrer très rapidement. Malgré tout, les balayages de ports continuent à être utilisés de plus en plus massivement et sont rarement gratuits. Il sont souvent suivis de stratégies d'attaques beaucoup plus précises (des attaques spécifiques dirigées contre les services actifs par exemple).

En examinant le résultat du balayage ci-après, un pirate sait par exemple qu'il pourra tenter d'infiltrer votre machine directement sur les ports ouverts (111, 512, 32772…), ou en exploitant les vulnérabilités des services actifs identifiés, comme Telnet, SMTP ou FTP (oui, ça y est, ils sont identifiés !). Le pirate expérimenté saura même déduire de tout ceci qu'il a affaire à une machine Unix et qu'il s'agit probablement de Solaris.

```
192.168.1.51   echo                7/tcp Echo [95,JBP]
192.168.1.51   discard              9/tcp Discard [94,JBP]
192.168.1.51   sunrpc             111/tcp rpcbind SUN RPC
192.168.1.51   daytime             13/tcp Daytime [93,JBP]
192.168.1.51   chargen             19/tcp ttytst source
```

Comparaison

Important trafic de balayage de ports

Le nombre d'entreprises pénalisées par les trafics de balayage est impressionnant. Retirer le trafic de balayage serait un peu comme rendre la rue de Rivoli fluide le samedi après-midi à l'approche de Noël.

```
192.168.1.51   ftp                21/tcp File Transfer
[Control] [96,JBP]
192.168.1.51   exec               512/tcp remote process
execution;
192.168.1.51   login              513/tcp remote login a la
telnet;
192.168.1.51   cmd                514/tcp shell like exec, but
automatic
192.168.1.51   ssh                 22/tcp Secure Shell
192.168.1.51   telnet              23/tcp Telnet [112,JBP]
192.168.1.51   smtp                25/tcp Simple Mail Transfer
[102,JBP]
192.168.1.51   nfs              2049/tcp networked file system
192.168.1.51   lockd            4045/tcp
192.168.1.51   unknown         32772/tcp unassigned
192.168.1.51   unknown         32773/tcp unassigned
192.168.1.51   unknown         32778/tcp unassigned
192.168.1.51   unknown         32799/tcp unassigned
192.168.1.51   unknown         32804/tcp unassigned
```

Évidemment, cela n'est qu'un début, mais détailler les opérations suivantes n'étant pas l'objectif de cet ouvrage, nous nous arrêterons là.

Exploitation du TTL

Avec un autre exemple, examinons comment un tricheur peut découvrir des données capitales sur votre installation. Il fera simplement appel aux riches fonctionnalités des protocoles, sans même chercher à les violenter.

Partons du principe que le pirate engage avec vous un dialogue insolite : il vous envoie un message constitué de plusieurs paquets, mais s'attache à régler la durée de vie du premier paquet (TTL, Time To Live) à 1, celle du deuxième à 2, et ainsi de suite pour les suivants. Rappelez-vous que le TTL d'un paquet est diminué de 1 chaque fois qu'il traverse un routeur. Lorsque le premier paquet traverse le premier routeur situé sur la route qui relie le pirate à votre machine, son TTL passe donc à 0 et le paquet est détruit. Comme les routeurs sont des tueurs polis, celui-ci vous informe et vous renvoie un paquet ICMP `TIME EXPIRED`, dans lequel se trouvent les références du paquet détruit, mais aussi les coordonnées du routeur impitoyable. Le pirate connaît donc l'existence et l'adresse de ce routeur. Lorsque le paquet suivant est détruit (TTL=2), le pirate reçoit un nouvel ICMP ; il a donc connaissance de l'existence et de l'adresse du routeur suivant. Et ainsi de suite jusqu'à votre poste, le pirate parvient à identifier tous les routeurs qui le séparent de votre machine. Il obtient ainsi l'adresse IP du dernier saut avant sa cible… c'est-à-dire, probablement, celle du routeur d'entrée de votre site ou de votre pare-feu, autrement dit le point de raccordement du réseau visé : le dispositif auquel les pirates sont susceptibles de s'intéresser en premier vient de dévoiler sa présence et son adresse IP ! Il faudra malheureusement peu de temps

avant qu'il ne dévoile à l'attaquant ses vulnérabilités et, si sa configuration est faible, il succombera certainement à ses coups de boutoirs. Percevez-vous maintenant l'intérêt de restreindre ICMP ?

Telnet, FTP, TFTP et SNMP, facteurs de risque

Une attaque correspond à une procédure précise. La plupart du temps, elle exploite la fonction boguée d'un logiciel d'une version donnée, tournant sur un système d'exploitation particulier (une attaque dirigée contre Outlook sur Windows Me peut être inopérante contre Outlook sous XP). Pour cela, la connaissance du système d'exploitation, des logiciels que vous utilisez, de leur version, du fabriquant ou de l'éditeur (particulièrement dans le cas des piles IP) représente pour le pirate un élément stratégique majeur sans lequel il ne saura poursuivre son action.

Telnet

Imaginez que vous hébergiez un serveur web sur l'une de vos machines et que le service Telnet soit actif (rappelez vous la sortie de balayage précédente). Qui empêche le pirate, maintenant parfaitement informé de la chose, de lancer la commande `telnet www.votreSiteWeb.com 80` ? Personne. Il lui suffit juste de saisir ensuite n'importe quoi et de presser la touche *Enter* pour recevoir une réponse ressemblant à peu près à ceci :

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Mon, 12 Sept 2005 10:36:26 GMT
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is
incorrect. </body></html>
```

Bien sûr, la commande a échoué, mais quelle importance ? En l'espace de quelques secondes il connaît le nom et la version du logiciel de votre serveur web. À partir de cet instant, faites confiance au pirate averti ; il possède certainement les outils capables d'exploiter à merveille les vulnérabilités spécifiques de IIS 5.0. Il est déjà en train de mitonner une belle attaque sur mesure et si, par malheur, votre logiciel n'est pas à jour, considérez que vous avez désormais perdu le contrôle de votre serveur !

IMPORTANT **Intérêt du pare-feu applicatif**

Notez au passage que si un grand spécialiste de Telnet avait analysé à la volée le contenu sémantique de l'information transmise par le pirate, il se serait vite aperçu de la supercherie et aurait bloqué son transfert, avant même qu'elle atteigne le serveur web. En conséquence, le pirate n'aurait pas eu accès à cette information capitale « Microsoft IIS/5.0 », en tous cas pas par ce biais-là. Vous vous doutez évidemment que le mystérieux grand spécialiste est le pare-feu. Pourquoi cette remarque ? Simplement pour que vous perceviez mieux l'intérêt des pare-feux applicatifs (nous en débattrons au chapitre suivant) : il ne suffit pas qu'un pare-feu sache seulement autoriser ou bloquer un service (c'est-à-dire autoriser ou bloquer un port), il est très important qu'il sache aussi analyser le contenu sémantique des informations véhiculées à l'intérieur de ce protocole. Un pare-feu qui se respecte doit absolument être capable d'effectuer une analyse dans les couches hautes du modèle OSI (notez par exemple à la figure 4-2 que Telnet est un protocole de niveau 7). Considérez qu'un pare-feu matériel qui se cantonne à un niveau 4 (autorisation/blocage des ports TCP/UDP) est une passoire.

TFTP

TFTP (Trivial File Transfer Protocol) est un autre boulevard assidûment fréquenté par les pirates. Vous n'avez peut-être jamais entendu parler de ce protocole étant donné que peu d'utilisateurs y ont recours. Cependant, pratiquement tous les routeurs – dont peut-être le vôtre – prennent en charge TFTP, employé par les administrateurs pour sauvegarder et restaurer, entre autres, les fichiers de configuration. Malheureusement, dire que TFTP est un protocole mal sécurisé est un euphémisme : ses informations circulent en clair sur le réseau, il n'utilise aucun mécanisme d'authentification et offre parfois un accès direct aux systèmes de fichiers. Après avoir effectué une reconnaissance préliminaire de votre réseau, un pirate peut très bien se connecter à votre installation par TFTP et, avec la simple commande :

```
> get configFichier.cfg
```

accéder à – ou modifier – des informations sensibles comme les noms de communautés SNMP, ainsi que les listes de contrôle d'accès. Muni de ce sésame, le pirate envisage des attaques de plus grande envergure par le truchement de SNMP et des protocoles de routage. Il peut notamment modifier les tables de routage de vos équipements afin d'intercepter vos sessions et de vous amener ainsi à lui fournir des informations précieuses. Ces dernières seront utilisées pour compromettre la sécurité de l'ensemble de votre système ainsi que l'intégrité de vos données.

SNMP

Nous ne parlerons pas beaucoup de SNMP (Simple Network Management Protocol), étant donné qu'il s'agit d'un protocole de gestion utilisé essentiellement dans les grands systèmes pour effectuer la supervision d'équipements et de matériels informatiques. Cependant, SNMP est tellement répandu et si peu sécurisé qu'il représente un vecteur d'intrusion ahurissant ; à ce titre, il mérite d'être mentionné.

Beaucoup d'administrateurs réseau, pourtant très au fait des possibilités offertes par SNMP, ignorent qu'en autorisant, même partiellement, un tel service, ils ouvrent toute grande une porte à travers laquelle les loups auront tôt fait de s'engouffrer ! À l'heure où de plus en plus de protocoles traditionnels (comme Telnet) cèdent la place à des homologues sécurisés (c'est le cas par exemple de SSH), SNMP ne chiffre ni les mots de passe, ni les contenus. Par ailleurs, contrairement à ce que beaucoup d'administrateurs croient, il ne suffit pas de restreindre de manière significative les possibilités d'utilisation de SNMP pour que la configuration soit sécurisée. SNMP reste vulnérable à de nombreuses attaques par débordement de tampon. Pour un pirate, SNMP est un moyen efficace pour accéder au répertoire racine d'une machine avec les droits administrateur : c'est un protocole vraiment dangereux. Les experts en sécurité sont unanimes et préconisent la désactivation pure et simple de ce service dès que cela est possible.

À RETENIR SNMP n'est pas sécurisé

De mauvaises langues prétendent que SNMP signifie « Security is Not My Problem ».

CONSEIL Évitez Telnet, TFTP ou SNMP

De façon générale, les actions à mener sont simples : il faut interdire totalement les services comme Telnet, TFTP ou SNMP sur votre installation, soit en les désactivant au niveau de vos équipements, soit en les bloquant au niveau de votre pare-feu.

Les protocoles NetBIOS : une pièce maîtresse de Windows très apréciée des pirates

Dans le monde Windows, le service NetBIOS mérite une attention particulière sur le plan de la sécurité.

NetBIOS est un pilier de l'édifice de Microsoft : il s'agit d'une suite de protocoles applicatifs (donc situés au niveau 7 du modèle OSI) accessibles à travers une interface logicielle et des outils intégrés au système d'exploitation. NetBIOS est très puissant et est l'une des chevilles ouvrières de la communication entre ordinateurs sous Windows. Il est omniprésent sur toutes les machines qui fonctionnent avec un système d'exploitation Microsoft. NetBIOS vous concerne tous.

Or, ce service est très mal sécurisé, voire pas du tout. Il réunit donc à lui tout seul les trois éléments d'un cocktail détonnant : large diffusion, puissant, non sécurisé.

Aussi, vous ne serez pas surpris d'apprendre que NetBIOS est très prisé par la communauté des hackers, qui l'utilisent comme cheval de Troie, agent efficace pour la collecte d'informations et l'infiltration rapprochée.

B.A.-BA NetBIOS

Ce service a en charge la gestion du partage des ressources en réseau et de tous les problèmes qui s'y rapportent. Par exemple, lorsque vous accédez à une imprimante partagée, c'est grâce à NetBIOS. Lorsque vous établissez une connexion directe à un lecteur réseau (lecteur de type H:\, M:\, Z:\…), c'est encore NetBIOS qui le gère. Lorsque vous obtenez des informations sur les noms, les machines, les domaines et les groupes de travail de votre réseau, c'est encore à NetBIOS que vous le devez.

Prenons un exemple : le service de nommage NBNS (NetBIOS Name Service), fonctionnant sur le port UDP 137, est capable, en deux commandes d'une simplicité désarmante, de dresser la liste des domaines du réseau et des machines rattachées à chaque domaine. Pire, il fournit une liste valide de noms d'utilisateurs pour un domaine donné. Voyons plutôt :

```
H:\>net view /domain
Domain
-------------------------------------------------------
FINANCE
PROJET
DEV_DOMAIN
The command completed successfully.
```

En réitérant la même commande, mais en focalisant cette fois sur le domaine `FINANCE`, cela donne :

```
H:\>net view /domain:FINANCE
Server Name             Remark
-------------------------------------------------------
\\MSG_PARIS             Serveur messagerie interne
\\DELL_CATHY            Catherine DUPONT
\\SECRETARIAT           Corinne MARTIN
\\SIT                   Stéphane DURAND
The command completed successfully.
```

Imaginez de telles informations entre les mains d'un pirate. À ce stade, il pourrait presque se connecter directement au système avec les droits d'un utilisateur authentifié (combien d'entre vous se reconnaîtront dans le cas de Corinne Martin : login « martin », mot de passe « corinne » ?).

Maintenant, si vous croyez que le pirate va s'arrêter en si bon chemin, c'est que vous ignorez les formidables capacités de NetBIOS. Le service SMB (Server Message Block), autre service NetBIOS fonctionnant sur le port TCP 139 ou 445, permet d'établir le plus simplement du monde et sans authentification aucune, une session SMB avec un partage situé sur n'importe quel ordinateur qui figure dans la liste précédente. Vous direz, à juste titre, que le pirate n'est pas supposé connaître le nom de ces partages. La belle affaire : Windows ouvre par défaut sur toutes les machines des partages masqués, comme `IPC$`, `C$` ou `Admin$`. Vous ne saviez pas que vous aviez des partages ouverts sur votre machine, autres que ceux que vous aviez définis explicitement ? Quel dommage ! car le pirate, lui, le sait. En lançant la simple commande :

```
net use \\DELL_CATHY\IPC$ "" /u:""
```

il se connecte directement à votre ordinateur, sans authentification, il établit ce que l'on appelle dans le jargon une connexion nulle.

Connexion nulle

Qu'est-ce qu'une connexion nulle pour un pirate ? C'est tout simplement un lien privilégié qui relie désormais sa machine à la vôtre. À partir du moment où une connexion nulle existe, votre machine devient subitement intarissable sur des sujets divers, comme celui des paramètres système ou réseau.

Le pirate sera capable de recenser les partages ouverts sur votre machine (les vôtres, les vrais, ceux que vous avez définis), de s'y connecter, de visualiser et d'accéder à votre arborescence de fichiers comme s'il se trouvait physiquement présent sur votre poste ! Si le partage se trouve au niveau de la racine, le pirate accède à tous les fichiers, y compris ceux de login/mots de passe du système, de votre messagerie, de votre site FTP, ou de vos bases de données. Même si ces mots de passe sont stockés chiffrés, partez du principe que le pirate saura les décrypter en très peu de temps, surtout lorsqu'ils figurent dans le dictionnaire !

À RETENIR **Sécuriser NetBIOS**

Une politique laxiste vis-à-vis des accès NetBIOS, et c'est la sécurité de tout le site qui s'écroule. Nous verrons au chapitre suivant qu'il est possible de se protéger de ce genre d'assaut. Globalement, il faut impérativement :

- ne jamais partager de dossier à la légère ;
- rester vigilant par rapport aux autorisations associées aux partages, définir des mots de passe robustes ;
- filtrer soigneusement les protocoles NetBIOS : autoriser à la rigueur sur votre réseau local les ports associés à ses services (ports UDP 137 – NetBIOS Name Service, TCP 139 – NetBIOS Session Service, ou 445 – service SMB directement sur TCP/IP), mais les interdire impérativement sur les réseaux non sûrs.

Attaques perpétrées via les protocoles applicatifs

En quoi HTTP, le protocole du Web est-il dangereux ?

Hormis les réseaux à caractère vraiment sensible (sièges d'entreprises, partis politiques, Défense…) – et encore ! – existe-t-il un pare-feu dans le monde qui interdise le protocole HTTP ? Pratiquement pas. Quelles que soient les politiques de filtrage mises en œuvre par ces produits (même quand elles sont des plus restrictives), ils ont à peu près tous le même point commun : celui de laisser passer HTTP, protocole universel d'Internet. S'il paraît en effet inconcevable de supprimer aux utilisateurs l'accès au Web, un protocole mondialement autorisé, pour un pirate, c'est ce qui s'appelle une aubaine : vaincre HTTP signifie faire main basse sur les réseaux du monde entier. Alors vous imaginez l'énergie déployée depuis des années par les cyber-voyous de tous bords pour y parvenir ! Résultat, HTTP (et, dans une moindre mesure, son petit frère HTTPS) constitue un véritable boulevard pour les intrusions. Examinons quelques exemples.

À RETENIR **Encapsulation de protocole**

Bien entendu, cette technique reste valable avec n'importe quel protocole autorisé sur la plupart des pare-feux, comme DNS, FTP ou SMTP (pour ne citer que ceux-là).

Encapsulation de protocole

Beaucoup pensent que, disposant d'un pare-feu quelque part sur le réseau, le problème de la sécurité est réglé. Alors pour fixer les idées, supposons que vous êtes protégé avec un pare-feu interdisant tout, sauf les connexions sortantes sur le port 80. Que peut bien tenter le pirate ? Une chose est certaine : si une trame HTTP venue de l'extérieur semble répondre à la requête d'un utilisateur situé à l'intérieur de la zone de protection du pare-feu, elle passera. Le pirate jouit donc d'une possibilité incontestable, celle qui consiste à détourner l'usage normal du protocole : en faisant l'hypothèse que votre machine a été préalablement infiltrée, qui pourrait bien empêcher un processus malveillant installé sur votre poste d'initier sans votre consentement une connexion arbitraire avec la machine du pirate ? Le pare-feu peut-être ? Non, puisqu'il autorise justement ce type de flux. Malgré sa présence, votre machine et le pirate peuvent communiquer tout à fait librement, à condition bien sûr d'enfermer les bribes de leur conversation à l'intérieur d'innocentes trames HTTP, autrement dit de se « déguiser » en HTTP. En d'autres termes, le pirate utilise HTTP comme protocole de transport pour acheminer un autre protocole, le sien, dont le contenu n'a probablement pas grand chose à voir avec des pages web. Ce protocole encapsulé peut contenir tout et n'importe quoi, y compris des commandes que seul le code malveillant installé sur votre poste saura interpréter. À partir de là, via un canal de communication établi au travers du pare-feu, avec la bénédiction totale de celui-ci et la complicité involontaire de HTTP, le pirate peut inonder le réseau avec des trames inutiles (attaque par déni de service), collecter et rapatrier vos données confidentielles, détruire des fichiers, installer à distance d'autres codes malveillants, etc. Voici donc un premier risque majeur, l'encapsulation d'un protocole arbitraire à l'intérieur d'un protocole autorisé.

Téléchargement de codes mobiles

Une caractéristique importante du protocole HTTP, nous le verrons plus en détail au chapitre 6, est sa capacité à transmettre les codes mobiles (contrôles ActiveX, scripts, applets Java, etc.), c'est-à-dire à télécharger sur votre poste en même temps que les pages web, de façon transparente et totalement à votre insu, des codes exécutables de toutes sortes, dont des codes malveillants. Qui donc peut bien empêcher ces téléchargements malheureux ? Pour que le pare-feu puisse faire quelque chose, encore faut-il :

- qu'il soit capable d'analyser le contenu des données véhiculées par HTTP (les pare-feux se limitant à une simple analyse de niveau 4, c'est-à-dire effectuant un filtrage basé sur les numéros de ports, sont donc complètement hors course) ;

À RETENIR **Danger de l'encapsulation de protocole**

Vous comprendrez aisément l'effet inattendu – et dévastateur en ce qui concerne la sécurité – produit par l'acceptation généralisée de HTTP et de HTTPS : la tendance actuelle des applications est de se servir de HTTP comme protocole de transport pour véhiculer les protocoles d'applications P2P, comme KaZaA, Emule, Bittorrent ou Overnet. Cela veut dire que HTTP ne sert plus seulement à transporter les objets du Web, il est utilisé par les éditeurs comme support universel pour transporter… des protocoles de plus haut niveau qui se révèlent souvent spécifiques, complexes et sujets à de nombreux changements. Or, ceci pose un problème évident en matière de sécurité, car, à l'heure actuelle, aucun outil de filtrage ne sait analyser de façon fiable le contenu de ces protocoles et il n'est pas sûr que ce genre de produit voie le jour, tant la tâche est ardue. Qui n'a jamais expérimenté l'infection par un virus ou l'installation d'un cheval de Troie par ce canal ? Hélas, à cause de HTTP, l'injection de codes malveillents devient courante, sans que ce protocole ne soit jamais violé.

- qu'il dispose d'une base de référence à jour répertoriant les « bons » codes et les mauvais.

Aujourd'hui, de tels pare-feux n'existent pas et il semble pour le moment illusoire d'espérer voir apparaître des produits efficaces dans un proche avenir.

CONSEIL **Mesures contre les codes mobiles**

Nous incitons fortement le lecteur à consulter le chapitre 6, dans lequel quelques mesures pour remédier à ce problème délicat sont proposées.

Détournement des flux chiffrés

L'utilisation croissante des flux chiffrés, qui transitent par exemple via les protocoles VPN-SSL et HTTPS, constitue paradoxalement une autre source d'infiltration : le trafic étant chiffré de bout en bout entre le poste utilisateur et le serveur distant, le pare-feu ne peut examiner son contenu et n'a d'autre choix que de laisser passer ce flux en bloc (ou de le bloquer complètement mais, dans ce cas, aucun trafic via un protocole sécurisé ne circulera). Si donc ce type de flux est autorisé et faisant l'hypothèse que votre poste a été infiltré, un processus malveillant peut très bien établir un tunnel chiffré avec l'ordinateur d'un pirate distant ; ce canal établi, le pirate pourra faire tout ce qu'il veut, télécharger des codes arbitraires, lancer des commandes à distance, collecter des informations… au nez et à la barbe du pare-feu qui reste aveugle.

Piratage par courrier électronique

Nous avons déjà abordé les problèmes classiques de contamination virale due à la réception de messages contenant une pièce jointe infectée. Ce type d'attaque est bien connu, au point d'ailleurs de faire presque oublier

qu'il existe d'autres moyens d'accès à votre espace informatique par la messagerie – moyens qui se révèlent pourtant d'une efficacité redoutable. Si vous n'êtes protégé par aucun pare-feu, ou si votre pare-feu laisse passer les protocoles usuels de la messagerie (SMTP, POP3, IMAP4), ce qui est fort prévisible, un pirate habile peut tout à fait jouer sur les mécanismes des protocoles de la messagerie, voire des forums de discussion sur Internet, pour transformer un canal de transmission « officiel » en un véritable boulevard d'intrusion.

Avez-vous déjà réfléchi à ce qu'est un client de messagerie ? Disons grossièrement qu'il s'agit d'un enrobage convivial destiné à vous faciliter la saisie des paramètres nécessaires à l'élaboration des messages (enveloppe et contenu), et à traiter ensuite ces messages. Une fois que vous avez entré les éléments caractéristiques du message (destinataire, corps du message), le client de messagerie fait appel à un moteur interne chargé de traduire ces paramètres en un langage particulier, que le serveur de messagerie saura interpréter. Ce langage est ce que l'on appelle SMTP, le protocole universel de la messagerie. Évidemment, exposé comme cela, parler de SMTP peut sembler tout à fait barbare. En réalité, il s'agit d'un langage de haut niveau, simple et de bon sens, à tel point que vous pourriez presque saisir directement, dans une fenêtre MS-DOS, des commandes SMTP vous permettant d'envoyer un message. Par exemple, si vous envoyez à un serveur de messagerie les commandes suivantes :

```
mail from:<addr_source>
rcpt to:<addr_desti>
```

en renseignant les champs d'adresses électroniques source et destination avec de bonnes valeurs, celui-ci enverra le message. Certes, il faut entrer d'autres commandes pour que le message soit complet, mais le principe est celui-là. Bien sûr, il faut aussi ranger les commandes SMTP, ainsi que les paramètres que vous fournissez, dans le bon ordre à l'intérieur de trames IP pour que celles-ci parviennent jusqu'au serveur (empilement de la couche SMTP au dessus de TCP/IP selon le modèle OSI – voir figure 4-2). Et évidemment, il ne faut pas se tromper dans la syntaxe des commandes, car sinon le serveur risque de considérer le message comme invalide. Tout ceci est un peu pénible ; c'est pourquoi nous utilisons tous un client de messagerie, qui a le mérite de nous débarrasser de ces problèmes de syntaxe et de rendre ces opérations automatiques.

Cependant, la tentation du pirate de se passer du client de messagerie est grande, car en élaborant ses messages directement en ligne de commande, il peut agir à sa guise sur chaque paramètre.

Supposez par exemple qu'il entre la séquence suivante :.

```
ehlo
mail from: <utilisateur.usurpé@domaine1>
rcpt to: <victime@domaine2>
data
subject: Panne de serveur e-mail
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
<HTML>
Suite à l'opération de maintenance ayant eu lieu récemment sur
le serveur mail de votre fournisseur d'accès, veuillez vous
connecter au site suivant et ressaisir vos identifiants afin de
valider votre compte :
http://www.asep-maintce.fr/comptesMail/
</HTML>
.
quit
```

Doté d'un outil adéquat, le pirate peut déjà envoyer un message qui semble provenir d'un autre utilisateur à l'adresse victime@domaine2. Jusque là, il n'y a encore rien de bien méchant, sauf si l'utilisateur victime tombe dans le piège, car dans ce cas précis, il s'agit d'un exemple simple de phishing.

Seulement, en enrichissant quelque peu ce squelette, le pirate peut tout à fait lancer des attaques extrêmement préjudiciables. Sachez par exemple qu'en ajoutant ne serait-ce que trois lignes bien choisies entre les deux balises <HTML> et </HTML>, le pirate peut activer l'exécution d'un programme sur votre machine : le code malveillant établissant une connexion HTTP avec le pirate.

Bien entendu, ces techniques datent un peu et sont actuellement fort heureusement déjouées par les programmes antivirus ou par les correctifs des clients de messageries. Cependant, de nouvelles vulnérabilités apparaissent tous les jours et n'oubliez jamais que la messagerie est un vecteur de piratage potentiel.

RENVOI **Phishing**

Les différents types d'attaques cités dans cet ouvrage sont définis à l'annexe B.

Risques liés aux applications sur Internet

Applications sur Internet : des vecteurs potentiels d'intrusion

Nous faisons ici allusion aux applications qui dialoguent sur Internet, qui reposent donc sur la pile des protocoles présentés schématiquement à la figure 4-2 ; nous nous situons donc maintenant en haut du modèle

OSI. Parmi les plus connues, citons notamment les navigateurs web (HTTP, HTTPS), les messageries (SMTP, POP3, IMAP4), les agents de gestion de réseaux ou d'équipements (SNMP), ou les applications poste à poste (P2P), basées sur des protocoles encapsulés (Kazaa, Emule, etc.). Cependant, il y en a bien d'autres.

Pour fixer les idées, prenons l'exemple du Web et de la messagerie électronique et partons du principe, pour continuer à ébranler les idées reçues, que vous êtes protégé avec un pare-feu. Qui plus est, votre pare-feu délivre à vos yeux une politique restrictive : il est configuré de manière à ce que tous les ports soient fermés, à l'exception bien sûr de ceux du Web, car vous hébergez un serveur web, ou de ceux de la messagerie ; les seuls protocoles autorisés à traverser le pare-feu sont donc HTTP (sur le port 80), HTTPS (HTTP sur SSL, sur le port 443), SMTP (sur le port 25) et POP3 (sur le port 110).

Malgré le caractère obsolète de cet exemple (peu de serveurs web sont encore vulnérables à cette attaque très ancienne), voyez comment il est facile à un pirate de récupérer à distance des données confidentielles : les premières versions du serveur web Apache était vulnérables à l'attaque dite PHF. Il n'était pas capable d'analyser, ni de valider correctement les entrées qu'il recevait. Le script PHF acceptait notamment le caractère de nouvelle ligne (`%0a`), interprétait la chaîne qui suivait comme une commande qu'il s'empressait d'exécuter avec les droits associés au processus du serveur web (c'est-à-dire, le plus souvent, les droits administrateur). Pour parler concrètement, lorsque le serveur web recevait la commande suivante :

```
/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

il renvoyait tout bonnement au pirate le fichier contenant la liste des identifiants utilisateurs et des mots de passe chiffrés (pour le pirate averti, retrouver ensuite les mots de passe en clair n'était pas très compliqué).

Vous trouvez peut-être que cet exemple n'est pas assez spectaculaire ? Qu'à cela ne tienne. Imaginez qu'à la place de la commande `/bin/cat /etc/passwd`, le pirate lance à distance un espion installé à l'avance ou, pourquoi pas, la commande `telnet`. Sur une fenêtre de son ordinateur, il récupère ainsi un interpréteur de commandes, grâce auquel il peut lancer sur sa machine, de façon interactive, des commandes qui s'exécute sur la vôtre ! Et le tout, bien sûr, avec la bénédiction de votre pare-feu. À ce niveau là, ce n'est plus une brèche…

Ceci n'est qu'un exemple, certes dépassé (notre but n'est pas de vous apprendre à pirater les systèmes !), mais il en existe des dizaines d'autres qui, eux, sont parfaitement opérationnels.

RAPPEL Applications boguées

N'oubliez jamais que tout logiciel vous apporte sa petite ration de bogues, qui, exploités « à bon escient », offrent aux pirates un moyen d'entrer au cœur de votre système (voir à ce sujet les quelques exemples présentés aux chapitres 3 et 6). Si la découverte d'un bogue et l'écriture du programme qui l'exploite demandent une haute expertise et un réel talent, l'utilisation de l'outil prêt à l'emploi qui en résulte, généralement publié sur Internet, est à la portée de n'importe quel « cyber-plouc ».

Le virus Netsky.P doit notamment sa brillante carrière au bogue d'Internet Explorer, lorsque celui-ci se trouve en présence d'un courrier infecté et dont l'en-tête MIME est incorrect (voir chapitre 3). Si vous utilisiez une version d'IE vulnérable à cette attaque (c'est-à-dire un IE que vous n'aviez pas remis à jour), la simple réception d'un message mal formaté provoquait l'exécution automatique de la pièce jointe, et vous étiez contaminé. Voyez encore comme il est aisé d'abuser un pare-feu effectuant un simple filtrage basé sur le numéro de port (agissant donc aux niveaux 3 et 4 du modèle OSI), alors que l'attaque se situe aux niveaux plus élevés des couches de protocoles. Si votre pare-feu laisse les ports 25 et 110 ouverts (donc autorise les protocoles SMTP et POP3), il n'a aucune raison d'intervenir…

À RETENIR **Nécessité d'un pare-feu « applicatif »**

Il n'est pas dans notre intention d'évoquer les dizaines et les dizaines de possibilités qui existent aujourd'hui pour entrer au cœur de votre système ; vous trouverez quelques exemples épars un peu partout dans cet ouvrage et plusieurs livres sont entièrement consacrés à ce sujet. Nous espérons au moins qu'à la lumière de ces exemples, vous commencez à comprendre à quel point tout objet communiquant est un ennemi en puissance et, surtout, pourquoi une protection efficace passe obligatoirement par un pare-feu « applicatif », capable d'analyser le contenu véhiculé à l'intérieur d'un protocole. Nous verrons ces points en détail au chapitre 5.

Se protéger des attaques dirigées contre les applications

Une protection efficace contre ce type d'attaque résulte inévitablement d'un faisceau de mesures qui se complètent.

La première consiste évidemment à mettre régulièrement à jour vos logiciels ; si vous installez les correctifs publiés chez les éditeurs, vous augmentez vos chances de colmater les failles connues et diminuez ainsi les risques d'attaque par cette voie.

La deuxième mesure est liée à la manière dont vous faites usage d'Internet. Pour la plupart d'entre vous, l'informatique n'est pas votre métier. Néanmoins, il est vraiment important que vous preniez définitivement conscience des pièges qui se cachent derrière une application. Vous constatez à quel point une application « honnête » est potentiellement exploitée par les pirates, alors, surtout, ne prêtez pas le flanc aux attaques en téléchargeant tout et n'importe quoi, de préférence des applications douteuses. Dites-vous bien que chaque code exécutable est un cheval de Troie en puissance, surtout s'il est gratuit, et encore plus s'il sert à échanger des fichiers piratés !

Ensuite, vous percevez sans doute qu'il y a urgence à installer un pare-feu. Ce problème sera traité au prochain chapitre mais, nous n'insisterons jamais assez, si un pare-feu limite son action à filtrer les protocoles sur la base des numéros de ports… il n'y voit que du feu ! De toutes façons, mettre en place un pare-feu, quel qu'il soit, est utile au moins pour interdire les protocoles, ou pour filtrer les applications dans le cas d'un pare-feu personnel. Cependant, sachez que, en ce qui concerne les protocoles autorisés, sa capacité de filtrage sera tout à fait partielle si c'est un pare-feu de niveau 4. Dans certains cas, en entreprise par exemple, il faut faire appel à un pare-feu applicatif.

Enfin, il faut aussi vous doter d'un bon antivirus pour contrer les attaques qui se situent dans les hautes sphères du modèle OSI.

ANTIVIRUS OU PARE-FEU **Jamais l'un sans l'autre**

Nous ne le répéterons jamais assez : pas de pare-feu sans antivirus, pas d'antivirus sans pare-feu.

Mention spéciale pour le Wi-Fi

Avec le Wi-Fi, nous entrons dans le monde fascinant des réseaux sans fil. Quand nous disons fascinant, nous pensons bien sûr aux utilisateurs qui y trouvent l'intérêt que l'on sait, mais aussi, et surtout, aux pirates. En effet, du point de vue de l'intrusion, les réseaux Wi-Fi offrent une voie royale ! Ces technologies nouvelles sont encore mal maîtrisées en ce qui concerne la sécurité, et sont aujourd'hui perçues par les attaquants comme le moyen le plus efficace pour contourner la sécurité d'un site, généralement affectée aux réseaux filaires.

Qu'est-ce que le Wi-Fi

Le Wi-Fi (*Wireless Fidelity*) est un label de certification désignant des équipements de communication radio et infrarouge qui satisfont à des critères techniques bien spécifiques : notamment une portée comprise entre 10 et 100 mètres, un débit de l'ordre de la dizaine de Mbits/s, voire plus dans le futur, et des exigences d'interopérabilité. Il s'agit donc d'un profil tout à fait adapté à la problématique du réseau local. Munis de la technologie Wi-Fi, les terminaux échangent de l'information et interagissent en réseau, comme s'ils étaient reliés par un câble Ethernet.

Si votre matériel est un terminal natif Wi-Fi (caméra, PDA, etc.), ou si vous équipez votre PC d'une carte réseau 802.11, il vous est possible de joindre un réseau sans fil. Il existe deux manières de se raccorder à un réseau Wi-Fi : via l'établissement d'un accès direct avec les autres terminaux Wi-Fi situés dans la zone accessible par votre carte (mode ad-hoc), ou bien à travers un point d'accès qui assure en général la passerelle vers le réseau Internet (mode infrastructure). Sitôt votre terminal allumé et quel que soit l'endroit où vous vous trouvez, à supposer bien sûr qu'il bénéficie d'une couverture suffisante, vous pouvez, sans formalité préalable, accéder à Internet, lire votre courrier électronique, accéder à distance aux données de votre entreprise ou communiquer avec vos interlocuteurs habituels en utilisant vos applications préférées.

JARGON **IEEE 802.11**

IEEE 802.11 représente la famille de normes qui définit les protocoles du Wi-Fi.

Risques liés au Wi-Fi

N'hésitons pas à rappeler une règle fondamentale en sécurité : plus une technologie devient populaire, plus elle est attaquée. Et comme, de surcroît, la sécurité n'a jamais été la préoccupation majeure des concepteurs du Wi-Fi, tirez-en vous-même les conclusions…

Commençons par le plus facile : il est très simple pour un pirate d'écouter ce que vous envoyez et ce que vous recevez. Comme ces informations sont transmises par voie radio, n'importe quel terminal Wi-Fi situé à la portée du point d'accès peut les capter. Certes, il reste au pirate un petit travail pour décrypter ces données, mais, comme nous allons le voir, ceci n'est pas bien méchant.

CONSEIL **Rien d'important par Wi-Fi**

Attention, avec le Wi-Fi, votre petite sœur saura lire votre courrier galant. Alors évitez ce canal pour envoyer à votre patron la dernière mouture de la proposition commerciale du contrat stratégique à venir.

Ce que nous venons d'évoquer pourrait être qualifié d'attaque passive pour pirate pantouflard. En étant un peu plus actif, on peut faire bien pire. À travers le réseau Wi-Fi, un pirate accède directement à votre poste. Il peut lire votre messagerie, accéder à des données financières, récupérer les fichiers sensibles, les mots de passe, les clés privées servant à déchiffrer ces mêmes fichiers...

Si, par malheur, le poste Wi-Fi est raccordé à un réseau d'entreprise, le pirate peut entrer directement au cœur de ce réseau, visiter les autres ordinateurs, les serveurs. Il accède ainsi à toutes les données commerciales ou financières, aux documents stratégiques, au nez et à la barbe des pare-feux ou de tout autre type de filtres.

À RETENIR **Wi-Fi = Danger**

Les risques liés au Wi-Fi sont majeurs. L'introduction de terminaux Wi-Fi dans un réseau filaire sécurisé est comparable à une ville fortifiée vaincue suite à l'invasion discrète et nocturne de parachutistes.

Localisation des points d'accès

Avec le Wi-Fi, les pirates ont remis au goût du jour une technique désuète utilisée au cours de la seconde guerre mondiale pour pister les opérateurs radio, le concept de *wardriving*. La détection et la prise d'empreinte de réseaux sans fil consiste à arpenter dans un véhicule (à la vitesse normale de la circulation) une zone d'activité, un centre-ville ou un dédale de rues, dans le but de localiser les points d'accès. Munis de dispositifs disponibles dans le commerce, c'est-à-dire un ordinateur portable, une carte réseau sans fil, une antenne et un récepteur GPS, ainsi que de quelques logiciels spécifiques, les pirates établissent tranquillement une cartographie très précise des points d'accès de votre région. Cette détection peut très bien se faire d'une manière tout à fait passive (il suffit d'écouter les trames balises émises par les points d'accès).

Parfois, il n'est même pas nécessaire de se fatiguer à faire ce travail. Des pirates, probablement soucieux d'économiser l'énergie des autres membres de leur confrérie, ont établi de magnifiques cartographies… que l'on trouve très facilement sur Internet !

Bien entendu, ces outils performants de *wardriving* ne se limitent pas à la simple détection des points d'accès. Ils fournissent aussi les précieux identifiants sans lesquel il est impossible de joindre le réseau, le fameux SSID (Service Set IDentifier), les adresses MAC des cartes référencées sur chaque point d'accès (ayez confiance, le pirate saura régler la sienne à une « bonne » valeur), et le mode de chiffrement du trafic.

Intrusion au cœur de votre système

Une fois que le pirate a localisé et identifié les points d'accès du secteur, il se sert de son analyseur de réseau pour classer les données interceptées, par point d'accès, puis par client. Il cherche ensuite à en savoir plus sur le mode de chiffrement (si les données sont chiffrées), notamment si elles sont chiffrées par SSL (c'est-à-dire par vous), ou si elle sont chiffrées par une implémentation de WEP (c'est-à-dire par l'infrastructure du Wi-Fi). Bien entendu, le pirate préfère le WEP, nous allons tout de suite voir pourquoi.

WEP (Wired Equivalent Privacy) est un algorithme cryptologique à clés secrètes destiné à protéger les trames émises sur un réseau sans fil. Les clés sont partagées entre le terminal et le point d'accès au réseau, et si le système ignore cette clé secrète partagée, il ne peut, en théorie du moins, faire partie du réseau. Seulement il y a un hic ! Contrairement à ce que pensent de nombreux utilisateurs, WEP n'a jamais eu la vocation d'offrir une sécurisation fiable du réseau ; WEP a été conçu dans un seul but : protéger le trafic d'un réseau WLAN contre les espions passifs et

involontaires. Les implémentations du WEP vous protègent en quelque sorte de votre petite sœur.

Le pirate n'a donc pas beaucoup de difficultés à casser cette clé. Dans la réalité, il y parvient… en trois secondes (parce que c'est un bon pirate, rassurez-vous ; un mauvais mettrait au moins dix secondes pour y arriver).

Dès lors, l'édifice s'écroule ; avec de bons outils et un peu de métier, tout est permis au pirate, ou presque. Il accède au contenu de votre machine et au réseau auquel elle est raccordée. Franchement, avec le développement des réseaux comme le Wi-Fi, pourquoi se fatiguer à contourner les équipements de sécurité périmétriques, comme les pare-feux ?

Mesures de protection

Après avoir brossé un tel tableau, faut-il abandonner le Wi-Fi ? Avant d'en venir à de telles extrémités, laissons à l'avocat de la défense le soin de présenter de nouvelles perspectives en matière de protection des réseaux sans fil. En effet, le constat alarmiste exposé précédemment reflète plutôt le mode d'utilisation actuel du Wi-Fi, et non la réalité de cette technologie, dotée des avancées récentes en matière de sécurité. Il faut savoir que depuis quelques années, les constructeurs se sont mobilisés pour développer des mécanismes (plus) fiables de sécurité. Malheureusement, si ces mécanismes sont pour la plupart intégrés aux produits Wi-Fi de nouvelle génération, les utilisateurs n'ont pas encore le réflexe de les employer. Essayons donc d'attirer votre attention sur ces points et de dresser une liste de mesures qui rehaussera indiscutablement le niveau de sécurité de votre infrastructure Wi-Fi.

Installez un pare-feu personnel

Si la carte Wi-Fi est installée sur le PC, il faut systématiquement installer un pare-feu personnel sur le poste. En effet, celui-ci réduira les risques d'intrusion par ce canal, et fera barrage à toute application qui tenterait d'établir à votre insu une connexion sortante vers Internet. Ce sujet sera examiné en détail au chapitre 5.

Utilisez WPA, voire WPA2

Comme nous venons de l'évoquer, disposer d'une liaison Wi-Fi non chiffrée est absolument suicidaire et les liaisons protégées avec un chiffre WEP ne valent guère mieux.

À la fin de l'année 2003, la Wi-Fi Alliance a lancé le concept de Wi-Fi sécurisé de nouvelle génération, en s'appuyant notamment sur un nouvel algorithme cryptologique, le WPA (Wi-Fi Protected Access), conçu

cette fois dans le but réel de sécuriser le trafic radio. WPA garantit un niveau de confidentialité plus élevé et l'intégrité du trafic échangé entre le terminal (votre poste) et le point d'accès ; il fournit en outre un service d'authentification forte du terminal, basé sur des mécanismes compatibles avec les protocoles d'authentification RADIUS.

En septembre 2004, une nouvelle évolution de WPA était disponible. WPA2 utilise l'algorithme AES, conçu par les cryptologues belges Vincent Rijmen et Joan Daemen (Rijndael), reconnu aujourd'hui dans le monde entier et massivement utilisé au sein des produits de sécurité actuels.

Ces deux algorithmes ont été spécifiés pour combler les vulnérabilités de WEP. Il est donc fortement recommandé d'abandonner WEP au profit de WPA, voire de WPA2.

Attention, vous ne pouvez utiliser ces algorithmes que si votre carte d'interface Wi-Fi et le point d'accès les acceptent mutuellement. En toute logique, les points d'accès fournis par les opérateurs doivent au moins proposer le WPA. Sachez en outre que la mise à niveau vers le WPA est réalisable sans changer d'équipement si ce dernier est certifié Wi-Fi. La mise à jour WPA2 risque en revanche de nécessiter l'installation d'un nouveau matériel.

Activez la traduction d'adresse (NAT)

Si vous disposez de votre propre routeur Wi-Fi et si celui-ci gère physiquement votre accès au réseau public, activez la traduction d'adresse (voir chapitre 5) : l'adresse privée de votre machine, ou le plan d'adressage interne de votre réseau, restera ainsi invisible du monde extérieur. Les pirates ne pourront donc pas joindre votre machine directement.

Masquez le SSID

Le nom du réseau sans fil (SSID) étant fort utile aux pirates, désactivez l'option de diffusion du SSID si votre équipement le permet. Si vous ne le faites pas, le SSID est émis continuellement sur les ondes à l'intérieur des trames balises, et c'est un jeu d'enfant d'intercepter cette information.

Ayez recours aux tunnels VPN

Si vous utilisez les réseaux Wi-Fi dans votre activité professionnelle, notamment pour accéder à distance aux ressources de votre entreprise ou pour échanger avec vos collègues des documents confidentiels, il est impératif de vous faire établir un tunnel privé de type VPN (*Virtual Private Network*) entre votre poste nomade et un serveur VPN installé dans l'entreprise. Le trafic sera ainsi chiffré de bout en bout entre votre poste et le serveur, qui plus est (si vous choisissez un bon produit – voir

chapitre suivant) avec un chiffre robuste. Ce trafic sera bien entendu surchiffré par le système Wi-Fi sur le tronçon radio.

Désactivez le Wi-Fi lorsque vous vous raccordez au réseau filaire

Pour les professionnels, si l'utilisation du Wi-Fi se justifie lors de vos déplacements, vous ne devriez en toute logique pas vous en servir, sauf cas particuliers, lorsque vous êtes de retour et lorsque votre poste est à nouveau raccordé au réseau filaire de l'entreprise.

Ne prêtez pas le flan aux attaques. Configurez votre poste de manière à activer manuellement votre liaison Wi-Fi à la demande, et veillez à ce qu'elle soit désactivée dès que vous vous branchez sur le réseau filaire.

Récapitulatif

L'objectif de ce chapitre n'était pas de vous présenter toutes les techniques qui existent à l'heure actuelle pour infiltrer les machines et en prendre possession : plusieurs ouvrages ne suffiraient pas pour décrire ne serait-ce que les attaques les plus connues.

En revanche, nous espérons vous avoir fait prendre conscience qu'à partir du moment où existe le plus petit canal ouvert entre le monde extérieur et votre informatique, un pirate peut s'en servir pour entrer et vous attaquer (en détournant le protocole de communication, en exploitant une vulnérabilité du protocole ou de l'application, en encapsulant un protocole de plus haut niveau, une donnée ou un programme malveillant, ou en utilisant une quantité d'autres astuces). Dès qu'un moyen de communication, quel qu'il soit, est ouvert entre vous et le monde extérieur, vous êtes potentiellement vulnérable. Sachez que, dans l'esprit du pirate chevronné, l'accès à une machine et l'obtention des droits administrateur sur cette machine ou sur un autre équipement (routeur) est une formalité. Le vrai travail commence après… Aujourd'hui, l'enjeu pour les pirates se situe beaucoup plus au niveau des couches hautes du modèle OSI, à savoir les protocoles applicatifs (HTTP, SMTP, DNS, etc.), les protocoles encapsulés à l'intérieur de HTTP (P2P, VoIP, H323, etc.) et les applications, c'est-à-dire une zone où le pare-feu devient de moins en moins pertinent. Contrairement à l'idée reçue, un pare-feu ne constitue pas la panacée : il ne fait que restreindre considérablement les « occurrences » possibles, et nous verrons dans quelle mesure au chapitre suivant, mais le risque subsiste toujours. Une protection efficace résulte d'un faisceau de mesures.