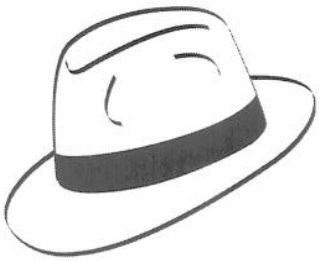
the HACKADEMY SCHOOL



Polycopié de cours

Cours Newbie

Une publication The Hackademy School

Une publication **The Hackademy School**

Bienvenue dans ce premier volet des cours par correspondance de The Hackademy School

NOUS Y ÉTUDIERONS :

Une publication **The Hackademy School**

IMPORTANT:

Ce polycopié de cours de The Hackademy School a pour objectif unique de contribuer à une meilleure compréhension des risques de sécurité liés à l'usage de l'outil informatique, et par là de permettre de s'en protéger plus efficacement. Il sera utile aux administrateurs système et réseau, aux développeurs, et plus généralement à toute personne utilisant Internet chez elle ou au travail. Si vous êtes soucieux de comprendre comment un pirate pourrait tenter de vous attaquer afin d'être à même de déjouer ses tentatives, ce cours est fait pour vous. Cependant, aucune garantie n'est donnée que ce contenu va vous permettre de vous protéger efficacement ou de manière "ultime", car ce n'est pas le cas et ça ne le sera jamais. De plus, le contenu de ce cours de niveau "débutant" est loin de couvrir le sujet de manière exhaustive: nous vous détaillons des méthodes d'attaque courantes, et nous vous fournissons des pistes pour vous en protéger. Nous vous donnons les bases nécessaires, à vous d'approfondir les points qui vous concernent directement, soit grâce à The Hackademy School, soit en faisant des recherches sur Internet.
Ce cours peut présenter des erreurs ou omissions susceptibles de vous porter préjudice. The Hackademy et DMP ne sauraient être tenus pour responsables des dommages éventuels causés par une application des méthodes présentées ici sur un système. Merci de nous prévenir si vous constatez de telles erreurs.
Il est formellement interdit par la loi d'appliquer les techniques d'attaque présentées dans ce cours sur un système que vous ne possédez pas. Vous pouvez cependant les appliquer sur vos systèmes informatiques à des fins de tests de vulnérabilité, en gardant à l'esprit que cela présente toujours des risques que vous assumerez seul.

Loi N° 88-19 du 5 Janvier 1988 relative à la fraude informatique. Extraits donnés pour illustration.

Accès ou maintien frauduleux dans un système informatique :
2 mois à 1 an de prison,
2 000 à 50 000 francs d'amende.

Accès ou maintien frauduleux dans un système informatique avec dommages involontaires : modification ou suppression de données, altération du fonctionnement du système
2 mois à 2 ans de prison,
10 000 à 100 000 francs d'amende.

Entrave volontaire au fonctionnement d'un système informatique :
3 mois à 3 ans de prison,
10 000 à 100 000 francs d'amende.

Introduction, suppression, modification intentionnelles de données :
3 mois à 3 ans de prison,
2 000 à 500 000 francs d'amende.

Suppression, modification intentionnelles du mode de traitement, des transmissions de données :
3 mois à 3 ans de prison,
2 000 à 500 000 francs d'amende.

Falsification de document informatique, usage de document falsifié :
1 an à 5 ans de prison,
20 000 à 2 000 000 francs d'amende.

Avertissement

Certaines techniques présentées dans ce cours sont usuellement utilisées par un pirate qui chercherait à s'introduire dans un réseau sur lequel il ne possède pas d'accès. Il est bien sûr interdit de mettre en application ces techniques sur un réseau que vous ne possédez pas, ou sans l'accord écrit et certifié de son propriétaire.
Il est essentiel de comprendre que si ces méthodes sont ici présentées, c'est avant tout dans une optique de compréhension générale de la sécurité et des moyens mis en œuvre par les pirates, et ce dans le seul et unique but, de pouvoir lutter contre ce danger.

De plus, ces méthodes de protection s'appliquent autant aux entreprises qu'aux particuliers. En effet, en dehors du nombre de documents privés que vous possédez sur votre ordinateur et que vous ne voudriez probablement pas voir être volés, un éventuel pirate pourrait vouloir se servir de votre système comme d'une passerelle dans le but de ne pas être retrouvé. Dans ce cas, ce serait à vous, en tant que personne physique ou morale (c'est-à-dire vous ou votre entreprise) de prouver votre innocence. De plus, une politique convenable de sécurité est de réinstaller entièrement votre système en cas de piratage, avec la perte et de temps et de finances que cela implique. Vous serez donc sans doute d'accord pour dire qu'il est essentiel d'assurer une sécurité optimale de votre système dès sa mise en place.
La structure générale de ce document se présentera sous la forme :
- description de l'attaque.
- moyens à mettre en œuvre pour éviter d'en être victime.

De plus, dans le cas malheureux où vous seriez victime d'un piratage, il est primordial de le détecter, et tout aussi important de localiser son origine, d'établir la liste des actions qui ont été exécutées sur votre réseau, estimer les dommages causés... Ces méthodologies seront également étudiées plus tard dans ce cours.

Introduction aux Réseaux TCP/IP

Un peu d'histoire

Lorsque les systèmes multi-utilisateurs ont connu une stabilité satisfaisante, les recherches se sont orientées vers un protocole de communication de ces systèmes, entraînant diverses expérimentations dans le monde. C'est l'armée américaine qui accélèrera ce processus, avec le financement de programmes de recherches universitaires pour le développement de voies de télécommunications redondantes (ARPANet). En cas de conflit militaire, la bonne circulation de l'information et sa confidentialité sont majeures, et les liaisons de communication étaient les premières cibles militaires.

Notions réseaux

Le matériel

Toute communication demande un support. L'informatique n'échappe pas à cette règle, et il a donc été nécessaire de mettre au point des interfaces capables de traduire le langage binaire d'un système digital en signal adapté à un support (paire de cuivre, câble coaxial, fibre optique, etc.). Ces interfaces comportent des circuits électroniques permettant d'écouter ou d'émettre sur un support. Chaque adaptateur dispose d'une petite quantité de mémoire, qui peut être accédée par le système hôte (PC, etc.).

Une première phase de développement a donc consisté à mettre au point ces adaptateurs, ainsi que de fournir en vue de développements à venir une documentation précise sur les registres et adresses à utiliser pour exploiter les fonctions de communication.

Ces opérations forment la première couche du modèle de référence OSI. C'est la couche physique. Elle permet une communication entre un système (digital) et un support (analogique) de transmission (ondes, laser, cuivre, fibre optique, etc.).

Les cartes les plus répandues sont des cartes Ethernet 802.3 (RJ45, BNC, AUI) et peuvent supporter des débits de 10Mb/s ou 100Mb/s. Elles permettent de transcrire une donnée digitale (ex. 0011 0100) en une tension adaptée au support (amplitude, codage, etc.).

Mais les adaptateurs réseaux gèrent également les états du support, et savent détecter un certain nombre d'erreurs sur ce support. Cette partie est transparente aux développeurs, mais elle est toutefois assurée par chaque NIC (Network Interface Card).

Toutes les cartes Ethernet disposent d'une adresse physique unique. Cette adresse, également appelée adresse MAC (Media Access Control), est utilisée pour les dialogues entre deux cartes. Elle est codée sur 6 octets , dont les 3 premiers décrivent le constructeur (ex. 00:0a:24 désigne le constructeur 3COM). Les adresses MAC (format des adresses MAC) sont généralement représentées sous forme hexadécimale, chaque octet étant séparé par le symbole ':' (ex. 00:40:05:61:71:EC).

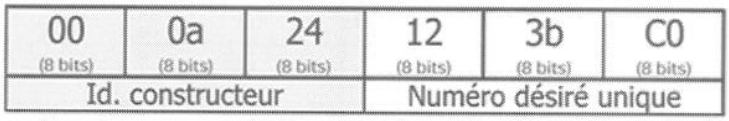


Figure 1

Sécurité des transmissions (fiabilité)

La couche réseau permet donc de joindre un destinataire relié au réseau (directement ou indirectement, d'où les fonctions de routage), mais prend en charge également des opérations de bases sur la gestion du service. Des trames ICMP peuvent être échangées entre les routeurs ou les stations pour signaliser un événement sur le réseau (perte de

paquets, filtrage, taille de trame trop grande et fragmentation IP nécessaire, etc.).

Mais il est nécessaire de disposer d'une partie logicielle capable d'assurer la bonne émission/réception des données. Lorsqu'un paquet (ou datagramme) ne parvient pas au destinataire, sans intervention logicielle, le paquet n'est pas arrivé, mais n'est jamais ré-émis automatiquement.

Deux protocoles viennent combler ce manque : UDP (User Datagramme Protocol) et TCP (Transmission Control Protocol).

L'UDP ne contrôle pas la perte des paquets, chaque paquet est émis sans numérotation vers le destinataire, et sans acquiescement. Le protocole TCP, quant à lui, assure un transfert plus fiable des données, en ouvrant une session de communication avant tout dialogue, puis en numérotant les paquets pour la reconstruction, en ré-émettant les paquets perdus ou erronés…

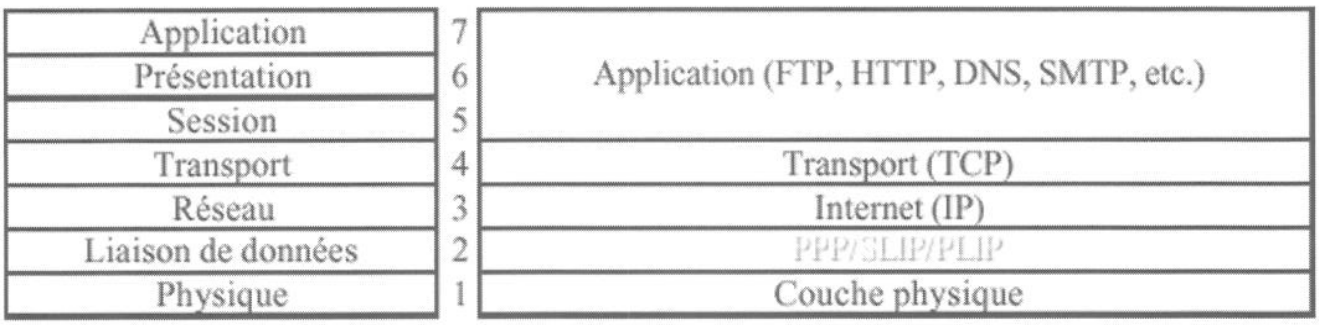
Les protocoles TCP et UDP se placent donc comme couche de transport dans la pile IP, car ce sont eux qui assurent la transmission des données d'un point à l'autre d'un réseau, en gérant les nécessaires ré-émissions (ou non) des paquets perdus ou altérés, etc.

Communications réseaux : les modèles OSI et TCP/IP

Les communications entre systèmes ne sont possibles que si chaque système comprend son destinataire (un français ne parle pas espagnol, et vice-versa). Il a donc été nécessaire de définir une norme pour permettre à chacun de communiquer avec un réseau existant.

C'est en cela que TCP/IP est appelé réseau ouvert. Les protocoles utilisés sont normalisés et disponibles pour le monde entier. Chacun peut donc adapter son système propriétaire pour communiquer en TCP/IP, en écrivant les différents composants logiciels répondant aux normalisations TCP/IP (la majorité des OS disposent aujourd'hui d'une implémentation TCP/IP).

L'Open Systems Interconnection Reference Model a donc normalisé un modèle de référence OSI-RM, utilisant 7 couches distinctes. TCP/IP s'inscrit dans ce modèle, mais n'utilise pas systématiquement l'ensemble des 7 couches.



Modèle de référence OSI *Modèle TCP/IP*

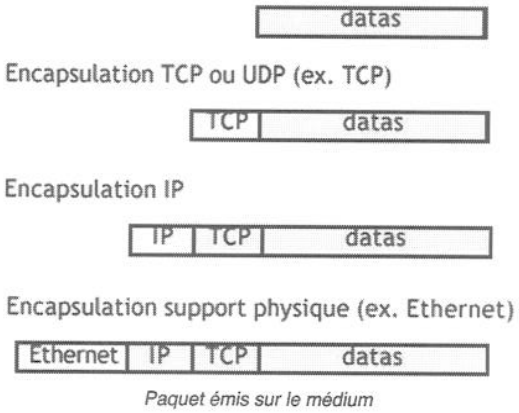
Le rôle de chaque couche est de permettre à la couche supérieure de lui passer des données qui seront émises, ainsi que de transmettre les données de la couche inférieure à la couche supérieure (données reçues).

On voit donc que pour une seule communication entre deux systèmes, il est nécessaire d'utiliser plusieurs protocoles.

Encapsulation

Seule la couche supérieure (Application) contient les données et uniquement les données à émettre ou reçues. Chaque couche ajoute ses propres entêtes, encapsulant les paquets de données dans de plus grands paquets, ou enlevant les entêtes dans le cas d'une réception.

Lorsqu'un paquet de données demande à être émis par une application, ces données vont donc recevoir plusieurs entêtes fonction des protocoles utilisés.



Paquet émis sur le médium

Dans le cas d'une réception, chaque couche prendra les informations nécessaires et retirera ensuite ses entêtes pour donner le bloc de données restant à la couche de niveau immédiatement supérieur.

Liaisons

Il existe certains cas d'utilisation qui demandent une couche supplémentaire. Dans le cas d'un accès par modem (donc par liaison série). Il n'y a pas d'adresse matérielle (adresse MAC) sur le modem. Cette adresse étant utilisée par les couches physiques et de réseau, il ne peut en théorie y avoir de communication. Le modem n'étant pas une interface réseau mais série (la communication se fait par un port COM), elle ne dispose pas en standard d'adresse matérielle, ni de ROM fournissant une interface de communication IP.

Il faut donc une couche logicielle supplémentaire, afin de simuler et fournir une alternative à l'utilisation des adresses MAC. Dans le cas d'une liaison TCP/IP avec un modem, on utilisera généralement le protocole PPP (Point to Point Protocol), qui se placera entre la couche réseau et la couche physique. Ce protocole fournira une solution logicielle aux communications IP nécessitant une adresse MAC.

Couches et protocoles utilisés

Chaque couche de la pile IP fait appel à un ou plusieurs protocoles pour remplir certaines fonctions (la couche transport utilise TCP ou UDP). Par cette méthode, les couches permettent de normaliser les flux de données entrants et sortants. Chaque couche (et donc chaque implémentation) est donc indépendante des couches supérieures et/ou inférieures.

- On appelle protocole un dialogue connu par les deux parties, entre deux couches de même niveau. Une couche de niveau (n) ne sera capable de dialoguer qu'avec une autre couche de même niveau qu'elle.
- On appelle service l'ensemble des fonctions que doit absolument remplir une couche, fournissant l'interface pour transmettre des données de la couche (n) à la couche (n+1) ou (n-1)

Address Resolution Protocol ou ARP

Lors de dialogue entre deux stations, il est nécessaire que les adaptateurs réseaux soient en mesure de prendre les

données qui leur sont adressées, sans traiter celles qui ne les concernent pas (d'où un gain de temps CPU et réseau). Certains réseaux fonctionnant sous forme de bus (Ethernet non switché, raccordement coaxiaux, etc.), toutes les données transitent sur le support, et donc tous les adaptateurs réseaux doivent analyser les trames pour ne prendre en compte que celles qui leurs sont destinées.

Les seules adresses disponibles et utilisables au niveau de l'interface physique (Couche 1 du modèle TCP/IP) sont les adresses MAC. Sans ces adresses, chaque adaptateur devrait décoder chaque trame jusqu'au niveau 3 (IP) pour savoir si cette donnée lui est adressée ou non.

Dans le cas d'un dialogue entre deux stations 10.23.23.2 et 10.23.23.254, la première étape consiste donc à trouver l'adresse matérielle de la station destinatrice, de manière à envoyer les données à cette station (en précisant son adresse matérielle plutôt qu'IP). C'est là qu'intervient le protocole ARP (niveau 3, couche réseau). Ce protocole va permettre à une station de découvrir l'adresse matérielle d'une autre station.

Pour cela, si 10.23.23.2 cherche à contacter 10.23.23.254, la station va, avant tout dialogue, diffuser (broadcaster) à l'ensemble des stations du réseau une requête ARP. Chaque station va alors recevoir cette requête ARP, composée du message suivant :

Station 10.23.23.2 d'adresse matérielle xx:xx:xx:xx:xx:xx cherche l'adresse matérielle de la station 10.23.23.254.

Toutes les stations reliées à ce segment analysent alors cette demande, mais seule la station 10.23.23.254 va répondre à cette demande, en renvoyant le message suivant :

Station 10.23.23.254 a pour adresse matérielle yy:yy:yy:yy:yy:yy.

Les deux stations 10.23.23.2 et 10.23.23.254 stockeront alors le couple (adresse IP, adresse MAC) obtenu dans un cache (dit cache ARP, cf. Figure - exemple de table ARP) pour ne plus reposer cette question dans le cas d'une nouvelle communication dans un faible délai (quelques minutes avant que le cache ARP n'efface ce couple s'il n'est plus utilisé).

```
C:\WINDOWS\Bureau>arp -a

Interface : [redacted] on Interface 0x2
  Adresse Internet      Adresse physique      Type
  129.33.182.200        20-53-52-43-00-00     dynamique
  129.33.183.72         20-53-52-43-00-00     dynamique
  206.108.111.106       20-53-52-43-00-00     dynamique
  213.36.80.1           20-53-52-43-00-00     dynamique
  213.36.82.165         20-53-52-43-00-00     dynamique
  216.40.32.30          20-53-52-43-00-00     dynamique
```

On voit dans cette capture (émission et réponse d'une requête ARP sur un segment local) que la station 10.23.23.2 a demandé l'adresse matérielle associée à l'adresse IP 10.23.23.254. L'adresse MAC de destination est une adresse de broadcast (toutes les stations du réseau) : tous les bits de l'adresse MAC sont à 1, à savoir 0xFFFFFFFFFFFF. L'ensemble des stations connectées au réseau devront donc traiter cette trame. La trame suivante montre la réponse de la station 10.23.23.254 à cette demande. Cette fois, la réponse n'est envoyée qu'à la station émettrice (ce qui est indiqué comme adresse matérielle de réponse).

```
16:08:13.422549 eth0 > arp who-has 10.23.23.2 tell 10.23.23.34 (0:50:ba:c8:20:e1)
16:08:13.422915 eth0 < arp reply 10.23.23.2 is-at 0:40:5:36:53:3d (0:50:ba:c8:20:e1)
```

Internet Protocol (IP)

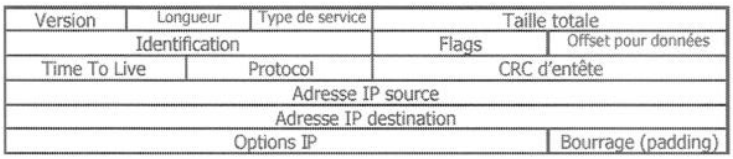
Sur un segment Ethernet, il n'est pas nécessaire d'utiliser une couche matérielle ou logicielle pour remplir les fonctions de liaison. Les protocoles de niveau 2 sont utilisés uniquement sur des liens séries ou parallèles, ou tout autre interface ou équipement ne disposant pas d'adresse MAC (ex. le PPP ou SLIP pour les accès IP via modem).

Chaque trame circulant sur le réseau possède, par le jeu des encapsulations successives, plusieurs entêtes. Une trame de données a donc au minimum une entête liée au média utilisé (généralement Ethernet). C'est le cas de l'ARP. Les trames utilisant les adresses IP auront en plus des informations d'entête IP.
Les informations contenues dans cette entête fixe de 20 octets (au minimum, voire plus si des options IP sont utilisées) renseignent sur la station émettrice (adresse IP), l'adresse du destinataire, le checksum (somme de contrôle), le protocole , la version, etc.

Il existe 3 sortes d'adresses IP :

- Unicast qui ne s'adressent qu'à une station particulière,
- Broadcast qui s'adressent à toutes les stations,
- Multicast qui s'adressent à un groupe Multicast (prédéfini).

Entête IP



Version : 4 bits Le champ Version renseigne sur le format de l'entête Internet. Ce document décrit le format de la version 4 du protocole.

Longueur d'En-Tête : 4 bits Le champ Longueur d'En-Tête (LET) code la longueur de l'en-tête Internet, l'unité étant le mot de 32 bits, et, de ce fait, marque le début des données. Notez que ce champ ne peut prendre une valeur en dessous de 5 pour être valide.

Type de Service : 8 bits Le Type de Service donne une indication sur la qualité de service souhaitée, qui reste cependant un paramètre "abstrait". Ce paramètre est utilisé pour "guider" le choix des paramètres des services actuels lorsqu'un datagramme transite dans un réseau particulier. Certains réseaux offrent un mécanisme de priorité, traitant préférentiellement un tel trafic par rapport à un trafic moins prioritaire (en général en acceptant seulement de véhiculer des paquets d'un niveau de priorité au dessus d'un certain seuil lors d'une surcharge momentanée). Principalement, le choix offert est une négociation entre les trois contraintes suivantes : faible retard, faible taux d'erreur, et haut débit.

Longueur Totale : 16 bits Le champ "Longueur Totale" est la longueur du datagramme entier, y compris en-tête et données, mesurée en octets. Ce champ ne permet de coder qu'une longueur de datagramme d'au plus 65,535 octets. Une telle longueur rendrait de toute façon les datagrammes impossibles à gérer pour la plus grande partie des réseaux. Les hôtes devront au moins pouvoir accepter des datagrammes d'une longueur jusqu'à 576 octets (qu'il s'agisse d'un datagramme unique ou d'un fragment). Il est de même recommandé que des hôtes ne décident d'envoyer des datagrammes de plus de 576 octets que dans la mesure où ils sont sûrs que la destination est capable de les accepter.

Identification : 16 bits. Une valeur d'identification assignée par l'émetteur pour identifier les fragments d'un même datagramme.

Flags : 3 bits Divers commutateurs de contrôle. Bit 0 : réservé, doit être laissé à zéro Bit 1: (AF) 0 = Fragmentation possible, 1 = Non fractionnable. Bit 2: (DF) 0 = Dernier fragment, 1 = Fragment intermédiaire.

Fragment Offset : 13 bits Ce champ indique le décalage du premier octet du fragment par rapport au datagramme complet. Cette position relative est mesurée en blocs de 8 octets (64 bits). Le décalage du premier fragment vaut zéro.

Durée de vie : 8 bits Ce champ permet de limiter le temps pendant lequel un datagramme reste dans le réseau. Si ce champ prend la valeur zéro, le datagramme doit être détruit. Ce champ est modifié pendant le traitement de l'entête Internet. Chaque module Internet (routeur) doit retirer au moins une unité de temps à ce champ lors du passage du paquet, même si le traitement complet du datagramme par le module est effectué en moins d'une seconde. De ce fait, cette durée de vie doit être interprétée comme la limite absolue maximale de temps pendant lequel un datagramme peut exister. Ce mécanisme est motivé par la nécessité de détruire les datagrammes qui n'ont pu être acheminés correctement sur le réseau.

Protocole : 8 bits Ce champ indique quel protocole de niveau supérieur est utilisé dans la section données du datagramme Internet. Les différentes valeurs admises pour divers protocoles sont listée dans la RFC "Assigned Numbers" [rfc1060].

Checksum d'entête : 16 bits Un Checksum calculé sur l'entête uniquement. Comme certains champs de l'entête sont modifiés (ex. durée de vie) pendant leur transit à travers le réseau, ce Checksum doit être recalculé et vérifié en chaque point du réseau où l'entête est réinterprétée.

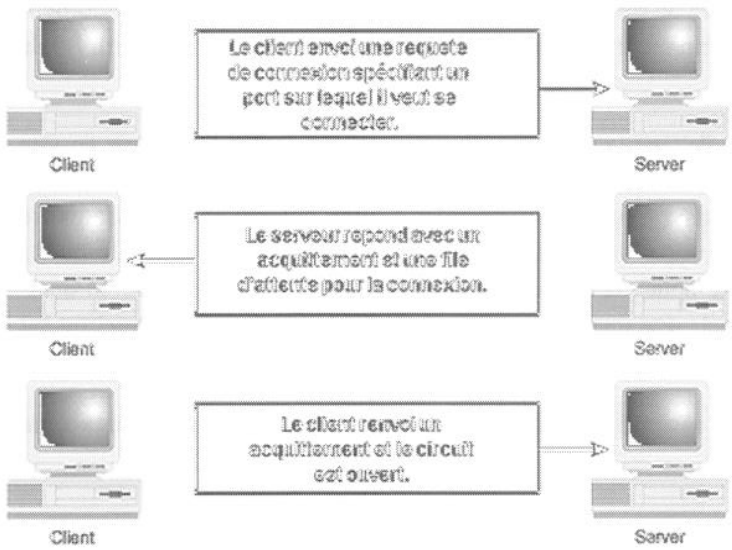
Adresse source : 32 bits L'adresse Internet de la source.

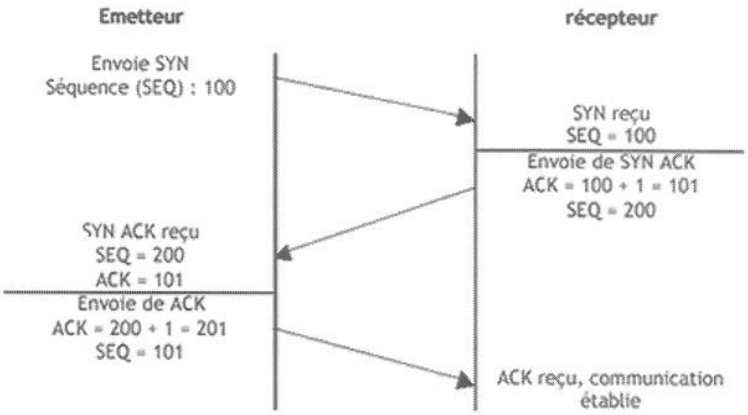
Adresse destination : 32 bits L'adresse Internet du destinataire.

Transmision Control Protocol : TCP

La couche de transport (couche n°4 dans la pile IP) assure le bon transfert des données. C'est cette couche qui, par exemple, va numéroter les trames TCP avant de les émettre sur le réseau, pour que le destinataire puisse reconstruire l'ensemble des données dans le bon ordre (ce n'est pas le cas d'UDP). Deux protocoles sont couramment utilisés dans un environnement TCP/IP. TCP et UDP.

TCP assure la numérotation des paquets, et le destinataire acquiesce chaque paquet. Il est donc nécessaire pour les deux parties d'établir une négociation du dialogue. C'est pour cela qu'une communication TCP débute toujours par une synchronisation des deux protagonistes. L'émetteur demande au récepteur si ce dernier est prêt à recevoir les données, ce dernier acquiesce donc la demande, que valide l'émetteur. Les transferts de données peuvent alors commencer. L'établissement d'une connection TCP se fait sur un "Three Way Handshake Connection".





Prenons par exemple une machine A et une machine B. La machine A est cliente, la machine B est serveur.

1. A --- SYN ---> B ; La machine cliente envoie un paquet TCP au serveur avec le flag SYN activé, ce qui veut dire : "puis-je établir une connection ? (SYN)".
2. A <--- SYN/ACK --- B ; La machine serveur répond par un paquet TCP avec les flags SYN et ACK activés, ce qui veut dire : "Oui, tu peux établir la connection (ACK), et moi ? Puis-je établir la connection ? (SYN)". Il est nécessaire d'envoyer un paquet avec le flag SYN, même en réponse, car une connection s'établit toujours à double-sens.
3. A --- ACK ---> B ; La machine cliente répond par un paquet TCP avec le flag ACK activé, ce qui veut dire "Oui, tu peux établir la connection (ACK)".

Si une machine refuse une connection, elle va répondre par un RST au SYN envoyé par le client.

Entête TCP

<table>
<tr><td colspan="6">Port source</td><td colspan="2">Port destination</td></tr>
<tr><td colspan="8">Numéro de séquence TCP</td></tr>
<tr><td colspan="8">Numéro d'acquiescement</td></tr>
<tr><td>offset</td><td>réservé</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Fenêtre</td></tr>
<tr><td colspan="6">Somme de contrôle</td><td colspan="2">Pointeur d'urgence</td></tr>
<tr><td colspan="6">Options</td><td colspan="2">Bourrage</td></tr>
<tr><td colspan="8">Données TCP</td></tr>
</table>

Port source : 16 bits Le numéro de port de la source.

Port Destinataire : 16 bits Le numéro de port du destinataire.

Numéro de séquence : 32 bits Le numéro du premier octet de données par rapport au début de la transmission (sauf si SYN est marqué). Si SYN est marqué, le numéro de séquence est le numéro de séquence initial (ISN) et le premier octet a pour numéro ISN+1.

Accusé de réception : 32 bits Si ACK est marqué, ce champ contient le numéro de séquence du prochain octet que le récepteur s'attend à recevoir. Une fois la connexion établie, ce champ est toujours renseigné.

Data Offset : 4 bits La taille de l'entête TCP en nombre de mots de 32 bits. Il indique là ou commencent les données. L'entête TCP, dans tous les cas, possède une taille correspondant à un nombre entier de mots de 32 bits.

Réservé : 6 bits Réservés pour usage futur. Doivent nécessairement être à 0.

Bits de contrôle : 6 bits (de gauche à droite): URG: Pointeur de données urgentes significatif ACK: Accusé de réception significatif PSH: Fonction Push RST: Réinitialisation de la connexion SYN : Synchronisation des numéros de séquence FIN: Fin de transmission

Fenêtre : 16 bits Le nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.

Checksum : 16 bits Le Checksum est constitué en calculant le complément à 1 sur 16 bits de la somme des compléments à 1 des octets de l'entête et des données prises deux par deux (mots de 16 bits). Si le message entier contient un nombre impair d'octets, un 0 est ajouté à la fin du message pour terminer le calcul du Checksum. Cet octet supplémentaire n'est pas transmis. Lors du calcul du Checksum, les positions des bits attribués à celui-ci sont marqués à 0. Le Checksum couvre de plus une pseudo entête de 96 bits préfixée à l'entête TCP. Cette pseudo entête comporte les adresses Internet source et destinataires, le type de protocole et la longueur du message TCP. Ceci protège TCP contre les erreurs de routage. Cette information sera véhiculée par IP, et est donnée comme argument par l'interface TCP/Réseau lors des appels d'IP par TCP.

Pointeur de données urgentes : 16 bits Communique la position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence. Le pointeur doit pointer sur l'octet suivant la donnée urgente. Ce champ n'est interprété que lorsque URG est marqué.

Options : variable Les champs d'option peuvent occuper un espace de taille variable à la fin de l'entête TCP. Ils formeront toujours un multiple de 8 bits. Toutes les options sont prises en compte par le Checksum. Un paramètre d'option commence toujours sur un nouvel octet. Il est défini deux formats types pour les options: Cas 1: Option mono-octet. Cas 2: Octet de type d'option, octet de longueur d'option, octets de valeurs d'option. La longueur d'option prend en compte l'octet de type, l'octet de longueur lui-même et tous les octets de valeur et est exprimée en octets. Notez que la liste d'option peut être plus courte que ce que l'offset de données pourrait le faire supposer. Un octet de remplissage (padding) devra être, dans ce cas, rajouté après le code de fin d'options. Ce octet est nécessairement à 0. TCP doit implémenter toutes les options. Actuellement, les options définies sont (type indiqué en octal) :

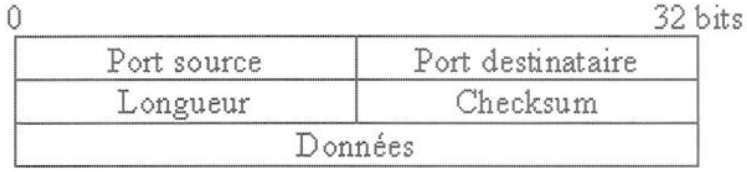
Donnée d'option : Taille maximale de segment : 16 bits Si cette option est présente, elle communique à l'émetteur la taille maximale des segments qu'il pourra envoyer. Ce champ doit être envoyé dans la requête de connexion initiale (avec SYN marqué). Si cette option est absente, le segment pourra être pris de n'importe quelle taille.

Bourrage (padding) : variable Les octets de bourrage terminent l'en-tête TCP: de sorte que le nombre d'octets de celle-ci soit toujours multiple de 4 (32 bits) de sorte que l'offset de données marqué dans l'en-tête correspond bien au début des données applicatives.

User Datagramme Protocol : UDP

UDP est plus tolérant, plus rapide, mais également moins fiable dans sa technique de transmission. Les données sont émises sans aucune assurance que l'émetteur puisse les recevoir. Chaque paquet est émis sur le réseau (sans numérotation), au maximum de la vitesse possible (fonction de la station et de l'état du média). Si des paquets sont perdus, il n'est pas possible pour l'émetteur de le détecter (ni pour le destinataire), de même que les données peuvent parvenir au destinataire dans un désordre complet suivant la complexité de la topologie du réseau.

En-tête UDP



Le Port Source est un champ optionnel. Lorsqu'il est significatif, il indique le numéro de port du processus émetteur, et l'on supposera, en l'absence d'informations complémentaires, que toute réponse devra y être dirigée. S'il n'est pas utilisé, ce champ conservera une valeur 0.

Le Port Destinataire a une signification dans le cadre d'adresses Internet particulières.

La Longueur compte le nombre d'octets dans le datagramme entier, y compris le présent en-tête (et par conséquent, la longueur minimale mentionnée dans ce champ vaut huit, si le datagramme ne transporte aucune donnée).

Le Checksum se calcule en prenant le complément à un de la somme sur 16 bits des compléments à un calculé sur un pseudo entête constitué de l'information typique d'une entête IP, l'entête UDP elle-même, et les données, le tout additionné d'un octet nul éventuel afin que le nombre total d'octets soit pair.

La pré-entête ajoutée avant l'entête UDP contient l'adresse IP source, l'adresse IP destinataire, le code de protocole, et la longueur du segment UDP. Cette information permet d'augmenter l'immunité du réseau aux erreurs de routage de datagrammes. La procédure de calcul du Checksum est la même que pour TCP.

Notions Ports TCP/UDP : Multiplexage/Démultiplexage

Une station peut émettre et recevoir simultanément plusieurs flux de données TCP et UDP. Pour cela, il est donc nécessaire que chaque extrémité (qui peuvent être différentes pour chaque communication établie) sachent à quel processus (système) rattacher une trame arrivant sur une interface. Pour cela, les protocoles TCP et UDP utilisent des numéros de ports. Ces numéros sont PRIMORDIAUX dans toute communication TCP ou UDP, et permettent d'associer une communication à un processus. Chaque donnée transitant sur le réseau s'est donc vu associer deux numéros de ports : le premier côté émetteur, le second côté récepteur. Chaque communication est donc caractérisée par deux couples (adresse IP, port utilisé) relatif à chaque extrêmité.

Les ports TCP et UDP sont totalement indépendants. Il est donc possible d'avoir simultanément une communication sur le port 25/TCP et le port 25/UDP.

Cette technique se rapporte au multiplexage/démultiplexage, par décodage du numéro de port dans la trame, la donnée est envoyée à l'un ou l'autre des processus du système. Par convention, les systèmes implémentent la logique suivante :

- Les numéros de ports inférieurs à 1024 ne peuvent être utilisés que par le super-utilisateur,
- Une application cliente utilisant TCP ou UDP utilisera un numéro de port supérieur à 1024 (même si l'utilisateur est le super utilisateur). Il existe toutefois certaines exceptions volontaires comme les r-services...

Une communication implique qu'un port soit ouvert sur la machine cliente et qu'un autre port soit ouvert sur la machine serveur. Il ne s'agit pas forcément des mêmes ports.

1. Une application serveur ouvre un port en permanence pour permettre l'attente de demandes de connection.
2. Une application cliente ouvre des ports au besoin. Elle n'attend pas de demande de connection, elle ne joue pas le rôle d'une application serveur et ne présente donc pas un point d'entrée sur un système.
3. Il existe 65535 ports, ni plus ni moins. La plupart d'entre eux sont réservés par des services précis (FTP : 21, telnet : 23, SMTP : 25, etc.)
4. Un port fermé est comme un mur en béton armé. Rien n'y entre, rien n'en sort.

Exemples :

1. Lorsque A envoie à B un paquet TCP avec le flag SYN activé, et que le port visé est fermé, la machine B renvoie un paquet TCP avec le flag RST activé. Certains firewalls ne renvoient pas de paquet TCP avec le flag RST actif (comme ZoneAlarm).
2. Lorsque A va vouloir se connecter sur le serveur HTTP de B, son application cliente (Internet Explorer) va ouvrir un port (1106, par exemple). L'application cliente va envoyer un paquet composé des entêtes IP, TCP, HTTP vers le port 80 de la machine B.

Quelques ports TCP couramment utilisés suivant leurs services

☑	13	Daytime => Time of day
☑	21	Ftp => File Transfer Protocol
☑	22	Ssh => Remote Login Protocol
☑	23	Telnet => Remote Login Protocol
☑	25	Smtp => Simple Mail Transfer Protocol
☐	42	NameServer => WINS Host Name Server
☑	53	Domain => Domain Name Server
☑	79	Finger
☑	80	Http => World Wide Web, HTTP
☐	98	linuxconf
☐	109	Pop2 => Post Office Protocol 2
☑	110	Pop3 => Post Office Protocol 3
☑	111	SunRPC => SUN Remote Procedure Call
☐	113	identd => Authentication Service
☐	118	SqlServ => SQL Services
☐	135	epmap => DCE endpoint resolution
☑	139	Netbios-ssn => NETBIOS Session Service

Si les paquets de données étaient transmis de façon anarchique, sans aucune règle concernant leurs constructions et leurs transmissions, les systèmes ne pourraient se comprendre de façon globale. Un système d'une entreprise A comprendraient les données des systèmes d'une autre entreprise A, mais pas ceux de l'entreprise Q. Pour que les systèmes puissent comprendre les données qu'ils s'inter-envoient, il faut standardiser la façon dont ces données sont construites et la façon dont elles sont envoyées. Cette standardisation s'effectue grâce à la mise en place des "protocoles". Chaque paquet va être constitué par des entêtes spécifiques à un protocole.

Sur Internet, le protocole le plus courant est TCP (Transmission Control Protocol). Lorsque vous allez sur un site Web, par exemple http://www.dmpfrance.com, les protocoles IP (Internet Protocol), TCP et HTTP (HyperText Transfer Protocol) seront utilisés pour envoyer et construire les paquets de données.

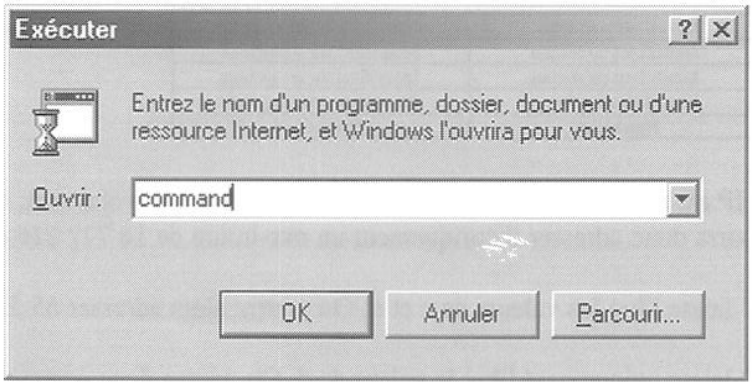
- IP va servir à définir tout ce qui concerne l'adressage des données ;
- TCP va définir le type de paquet envoyé ;
- HTTP va envoyer les données qui lui sont spécifiques, soit les pages Web.

IP va être utilisé dans l'adressage des paquets, permettant ainsi aux machines relais émettrices et réceptrices d'établir un chemin correct de transmission de données. TCP va définir le type de paquet, à savoir un paquet servant à établir la connection, à la fermer, etc. Ce sont réellement ces deux protocoles qui sont les plus importants sur Internet à un niveau global.

Utilisation de la commande Netstat

La commande "netstat'" est bien instructive, même si elle n'est pas toujours très lisible. Elle affiche les statistiques de protocole et les connexions réseau TCP/IP en cours d'utilisation sur la machine locale.

Lancer l'interface de commandes MS-DOS




```
C:\WINDOWS\Bureau>netstat -a

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    brotha:44334           BROTHA:0               LISTENING
  TCP    brotha:12345           BROTHA:0               LISTENING
  TCP    brotha:pop3            BROTHA:0               LISTENING
  TCP    brotha:nbsession       BROTHA:0               LISTENING
  UDP    brotha:44334           *:*
  UDP    brotha:4515            *:*
  UDP    brotha:nbname          *:*
  UDP    brotha:nbdatagram      *:*
```

La première colonne indique le protocole utilisé lors de la communication. La deuxième colonne indique l'adresse de votre machine, ou son nom. Après les deux points se situent le numéro de votre port utilisé dans la communication. La troisième colonne indique l'adresse de la machine distante. Après les deux points se situent le numéro du port utilisé dans la communication. La dernière colonne indique l'état de la connection, à savoir si elle est établie, en train de s'établir, en train de se terminer, etc.

Note : Si une application serveur comme un trojan monopolise un port, et qu'un intrus est connecté au trojan, vous le verrez grâce à netstat !

L'adressage IP

Chaque système souhaitant discuter sur le réseau mondial IP (Internet) doit disposer d'une adresse IP. Ces adresses, affectées par des organismes de régulation, sont classifiées et normalisées. Une station de l'Internet ne peut être localisée (joignable) que par son couple unique (Adresse IP, Masque de sous-réseau).

Les adresses IP

Une adresse IP est composée de deux champs : l'adresse réseau et l'adresse machine. L'adresse réseau est placée sur les bits de poids forts, alors que l'adresse de machine est calculée sur les bits de poids faible.

Il existe plusieurs classes d'adresses. On parle des classes A, B, C, D et E. Elles sont différenciées par les bits de poids forts qui les composent.

A	0000	Identifiant du réseau	Identifiant de la machine
B	1000	Identifiant du réseau	Identifiant de la machine
C	1100	Identifiant du réseau	Identifiant de la machine
D	1110	Identifiant du réseau	Identifiant de la machine
E	1111	Non utilisé	Non utilisé

Une adresse IP est toujours de la forme a.b.c.d. Dans le cas d'une classe A, on peut librement fixer les valeurs b, c et d. On pourra donc adresser théoriquement un maximum de 16 777 216 (2 3x8 =2^{24}) machines.

Une classe B laisse libre les valeurs de c et d. On pourra alors adresser 65 536 (2 2x8 =2^{16}) machines.

Une classe C laisse uniquement libre la valeur de d. On pourra donc adresser 256 (2^8) machines.

La classe D est une classe quelque peu différente, puisqu'elle est réservée à une utilisation particulière : le multi-casting (diffusion temps réel vers plusieurs destinations).

La classe E est, quant à elle, une classe non usitée à ce jour, et réservée à des utilisations à des fins expérimentales.

On dispose donc en théorie des plages d'adresses suivantes :

Classe	*Plage*	
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Il existe quelques adresses dites non routables. Ces adresses sont réservées à un usage interne, ou dans le cas de réseaux privés. Elles ne sont en théorie jamais routées sur l'Internet. Il existe 3 classes d'adresses IP :

- Classe A : 10.0.0.0
- Classe B : 172.16.0.0 à 172.31.0.0
- Classe C : 192.168.0.0 à 192.168.255.0

127.0.0.0 est aussi une classe A particulière, puisqu'elle ne sera jamais routée sur un réseau. Elle est réservée pour un usage interne. Elle correspond à l'interface loopback (interface de bouclage). Ainsi, l'adresse IP 127.0.0.1 désigne votre ordinateur.

S'informer sur un système cible

Se renseigner sur le système

On peut considérer généralement qu'une tentative d'intrusion de la part d'un pirate commençe toujours par une prise d'information sur le système qu'il cherche à attaquer. Il existe dans ce but toute une méthodologie à appliquer, mais il y a heureusement un ensemble de techniques pour s'en protéger.
Dans les explications qui vont suivre, nous verrons quelles sont ces techniques de renseignement sur un système, comment elles peuvent être utilisées, et bien sur comment se protéger.

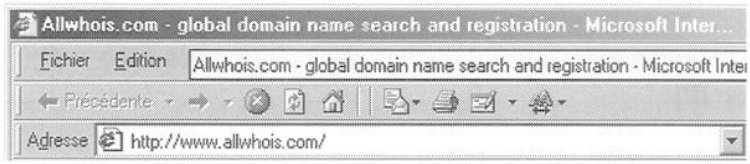
WHOIS

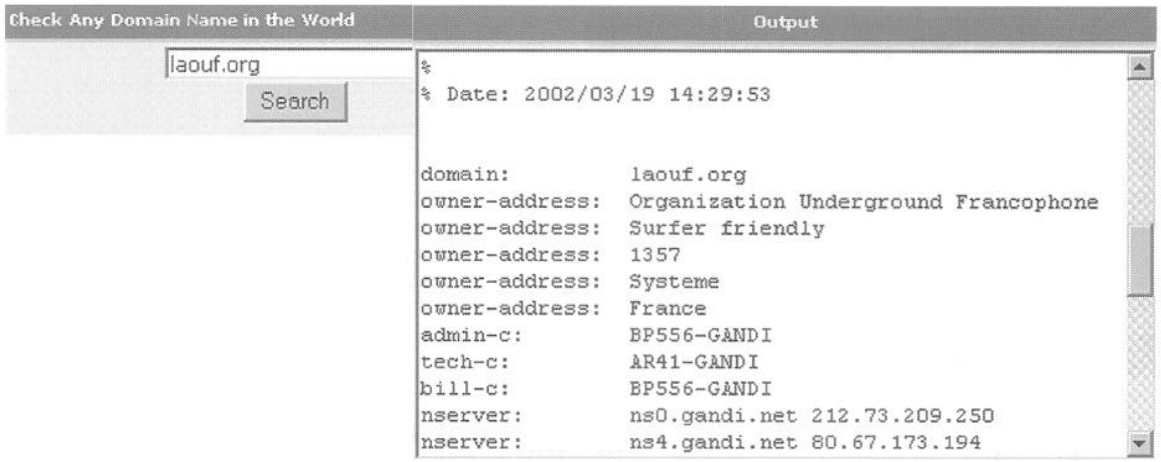
Lorsqu'un nom de domaine, "caramail.com", par exemple, est enregistré sur Internet, des informations comme l'identité du "registrant", c'est-à-dire celui qui enregistre le nom de domaine, ou encore l'identité du responsable technique, sont stockées dans les bases de données de prestataires de services appropriés. Les bases de ces pres-

tataires (ARIN, Internic, NetworksSolutions, Gandi, RIPE...) sont consultables gratuitement par l'intermédiaire de requêtes appelées "whois" (comprendre "Who is ?").

De nombreux prestataires de ce service sont en ligne sur Internet, mais leur fiabilité à fouiller les bases de données peut varier. Ainsi, il n'est pas impossible d'avoir à mener des requêtes "whois" en passant par plusieurs prestataires.
Parmi ceux qui peuplent l'internet, on en retiendra au moins trois :

http://www.allwhois.com : Whois sur les noms de domaines de tous les pays du monde (.ch, .uk, .nl, etc.).
http://www.whois.net
http://www.betterwhois.com





Une foule de renseignements peuvent être obtenus par l'intermédiaire des ces requêtes :
- si l'entreprise est propriétaire d'une plage d'ip spécifique, le pirate la connaîtra, et pourra alors élargir son champ d'action.
- Les adresses et noms des serveurs DNS, dont l'exploitation est expliquée par la suite.
- Le nom, adresse, téléphone et email du propriétaire du nom de domaine. Ces informations peuvent être exploitées dans le cadre d'une attaque par social engeneering, comme cela est également expliqué par la suite, ou pour la découverte de mots de passe que vous auriez pu choisir et ayant un rapport avec les informations fournies.
Il est vital de donner le minimum de renseignements possibles vous concernant lors de votre enregistrement. Ne préciser que ce qui est obligatoire. Donner une adresse email spécialement conçue pour cet enregistrement et que vous n'utiliserez qu'à cette fin.

La commande ping

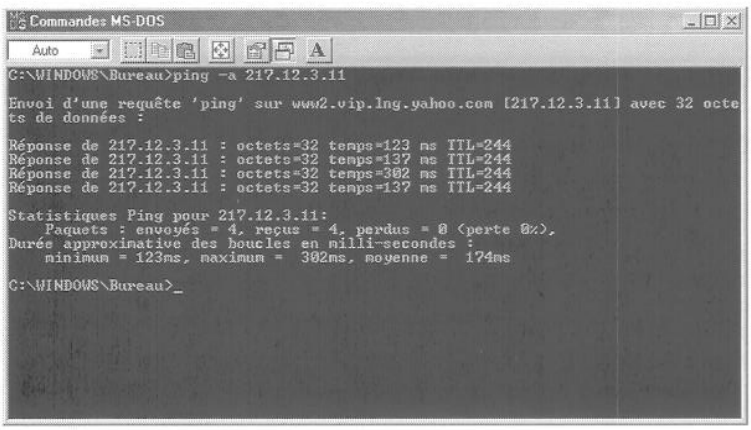
La toute première étape consistera toujours pour un pirate à obtenir l'adresse ip de votre système, afin naturellement de pouvoir communiquer avec lui. La fonction Ping peut alors être utilisée pour vérifier que le système est actif sur le réseau.
La machine qui envoie un "ping" vers une autre machine, attend un écho de son appel pour s'assurer que celle-ci est bien disponible. Le message de PING doit suivre le routage normal de IP à travers les passerelles et routeurs... Il utilise pour cela le protocole ICMP encapsulé dans la trame IP. Le retour d'un PING (echo reply = pong) donne généralement le temps mis par le message pour faire l'aller-retour (RTT = round trip time) jusqu'au destinataire.

Il existe plusieurs versions de PING plus ou moins évoluées. Le champ "CODE" du message ICMP peut donner

des informations sur le résultat du test : Réseau inaccessible... Machine inaccessible... Echec de routage... Etc.

Ping intègre diverses fonctionnalités. Afin de toutes les visualiser, tapez " ping " sous DOS. Parmi les différentes fonctions de ping, on retiendra :

1. L'option "-t", qui envoie des paquets ICMP_echo_request en boucle, jusqu'à interruption de la part de l'utilisateur par un "break" (CTRL+C). Exemple : ping -t [Adresse IP]
2. L'option "-a", qui sert à transposer une adresse IP en un nom d'hôte. Exemple : ping -a [Adresse IP]
3. L'option "-n", qui sert à envoyer un nombre de paquetsICMP_echo_request précis. Exemple : ping -n 8 [Adresse IP]
4. L'option "-l", qui permet de spécifier la taille de la requête à envoyer. Exemple : ping -l 64 [Adresse IP]
5. L'option "-i", qui permet d'imposer une durée de vie (TTL) de base, entre 1 et 255. Exemple : ping -i 145 [Adresse IP]
6. Et éventuellement l'option "-w" qui permet de spécifier un délai d'attente pour les trames echo_reply ("timeout"). Exemple : ping -w 999 [Adresse IP]



Savoir lire un compte-rendu de l'outil ping est très simple. Dans le champ réponse vous sont indiqués :

- en octets la taille du paquet que vous avez envoyé ;
- en millisecondes le temps de réponse du système ciblé ;
- et la valeur du TTL lorsque le paquet est arrivé à destination.

Quatre requêtes ICMP_echo_request sont envoyées lors d'une utilisation courante de Ping, afin de bien s'assurer des résultats.

La commande tracert

Tracer la route qu'emprunte un paquet de données pour aller d'un point A à un point B peut être utile afin de déterminer, par exemple, les différentes zones géographiques qu'il traverse, ou encore le dernier routeur emprunté pour l'acheminement des données. Pour effectuer ce processus, utilisez l'outil Tracert de votre système.

Tracert est l'abréviation de "Trace Route". L'objectif du logiciel est la mise en lumière du chemin emprunté par un paquet de données pour atteindre un point précis d'un réseau. Il peut être utilisé pour l'évaluation des performances d'un réseau, pour évaluer à quel niveau peuvent se situer des points de congestion ou localiser des problèmes d'infrastrucutres.

Le principe de "traceroute" est relativement simple :

Le logiciel crée un paquet avec les adresses source et destinataire, et une valeur de durée de vie TTL (nombre de passerelles traversées) égale à "1". Ce paquet va s'arrêter sur le premier routeur rencontré.

Celui-ci va envoyer un message d'erreur ICMP (time exceeded) avec son adresse comme "source" et l'adresse "source" de l'émetteur, comme destination. Le logiciel "traceroute" va enregistrer cette information, et créer un nouveau paquet comme le premier, mais avec un TTL de "2". La traversée du premier routeur va mettre le TTL à "1". Le paquet va donc mourir sur le deuxième routeur. Comme précédemment, le routeur N°2 va envoyer une message d'erreur ICMP avec son adresse, qui sera mémorisée par "traceroute"... et ainsi de suite jusqu'au destinataire.

Pour effectuer ce processus, utilisez l'outil Tracert de votre système.

1. Allez sous MS-DOS.
2. Tapez tracert.
3. S'affichent alors les options de paramétrage, tout comme pour Ping.
4. On ne les utilisera pas dans l'absolu, donc tapez simplement tracert [Adresse IP]

```
C:\WINDOWS\Bureau>tracert www.tucows.com

Détermination de l'itinéraire vers www.tucows.com [216.40.32.30]
avec un maximum de 30 sauts :

  1   110 ms    96 ms    96 ms
]
  2    96 ms   110 ms   110 ms
  3    96 ms    96 ms   110 ms

  4   206 ms   206 ms   220 ms

  5   123 ms   110 ms   110 ms
  6   110 ms    96 ms   110 ms  if-10-0-0.bb1.Paris.Teleglobe.net [195.219.32.81
]
  7   138 ms   109 ms   110 ms  if-0-0.core1.Paris.Teleglobe.net [195.219.14.129
]
  8   123 ms    97 ms   123 ms  if-8-0.core1.Frankfurt2.teleglobe.net [195.219.1
5.206]
  9   192 ms   193 ms   192 ms  if-10-0.core3.NewYork.Teleglobe.net [66.110.8.15
4]
 10   192 ms   193 ms   192 ms  if-10-0.bb8.Newyork.Teleglobe.net [207.45.223.11
0]
 11   206 ms   206 ms   206 ms  if-1-0.core1.Toronto3.Teleglobe.net [207.45.220.
54]
 12   234 ms   220 ms   220 ms  ix-8-0.core1.Toronto3.Teleglobe.net [216.6.0.146
]
 13   234 ms   233 ms   220 ms  core3-toronto12-pos6-2.in.bellnexxia.net [206.10
8.107.229]
 14   234 ms   233 ms   220 ms  core1-toronto12-pos5-0.in.bellnexxia.net [64.230
.242.193]
 15   220 ms   234 ms   219 ms  dis1-toronto12-pos6-0.in.bellnexxia.net [206.108
.97.70]
 16   234 ms   219 ms   234 ms  206.108.111.106
 17   288 ms   206 ms   234 ms  129.33.182.200
 18   220 ms   234 ms   219 ms  129.33.183.72
 19     *        *        *     Délai d'attente de la demande dépassé.
 20     *        *        *     Délai d'attente de la demande dépassé.
 21   261 ms   220 ms   233 ms  radware1-39.tucows.com [216.40.39.80]
 22   206 ms   233 ms   220 ms  www.tucows.com [216.40.32.30]

Itinéraire déterminé.

C:\WINDOWS\Bureau>
```

Tracert intègre diverses fonctionnalités. Afin de toutes les visualiser, tapez " tracert " sous DOS. Il y en a peu, certes, mais trois d'entre elles peuvent s'avérer essentielles.

1. L'option "-d" empêche la conversion des adresses IP des machines qui effectuent le relais en noms d'hôtes. Exemple : tracert -d [Adresse IP]
2. L'option "-h" permet de spécifier un nombre de "sauts" maximum, c'est-à-dire le nombre maximum de points de relais résolu. Par défaut, ce nombre est 30 ("avec un maximum de 30 sauts"). Exemple : tracert -h 45 [Adresse IP]
3. L'option "-w" qui permet de spécifier un timeout, un temps d'attente, après quoi, le processus est avorté, précis pour la résolution de chaque hôte. Exemple : tracert -w 999 [Adresse IP]

Savoir lire un compte-rendu de l'outil tracert est très simple. Dans le tableau des résultats, vous avez un classement des systèmes relais de données. Les délais en millisecondes indiquent des résultats sur le temps qu'il a fallu pour contacter chaque système de relais, sachant que cette tentative se fait par trois fois. Dans la dernière colonne se trouvent les noms d'hôtes des systèmes de relais, avec leurs translations en adresses IP. Entraînez-vous à repérer les informations que contiennent les noms d'hôtes, et celles que fournissent un traceroute.

Recherche d'informations sur la personne ou la société

Une personne

Peut être êtes-vous un habitué des forums, ou des newsgroups, ou possédez-vous une page web. Un pirate qui vous aurait pris pour cible pourrait se lancer dans la recherche de votre présence sur le web afin d'acquérir des informations supplémentaires.
- Concernant les newsgroups, il suffit pour le pirate d'utiliser des moteurs de recherche spécifiques aux news, tel que http://groups.google.com
- Pour les forums et sites web, une simple recherche par l'intermédiaire d'un moteur de recherche tel que Google (http://www.google.com) est suffisante.
Le principal danger de ce type de référencement est que vous pouvez y divulguer des renseignements non destinés au public. Imaginez que vous ayez un probleme d'installation d'un serveur particulier sur un systeme d'exploitation donné, le pirate connaîtra alors sans peine le nom et la version de votre serveur et de votre système d'exploitation. Evitez donc à tout prix de divulguer les informations qui ne sont pas essentielles sur un endroit aussi peu securisé que le web.
- L'assaillant peut également glaner des informations auprès de vos proches, en essayant de s'imiscer dans votre vie privée ou professionelle. N'oubliez pas également qu'il peut s'agir d'une personne que vous connaissez, et qu'elle peut avoir des informations privées vous concernant. Afin d'éviter toute mauvaise surprise, n'utilisez jamais de mots de passe se raportant à votre date de naissance, aux noms de votre femme, enfant ou chien, ou en rapport avec quelques renseignements vous concernant et qui pourraient être connus.

- Une autre méthode que nous avons déja évoquée est celle dite du social engeneering, qui a tendance a ne pas être jugée à sa juste valeur. Il s'agit de se faire passer par un quelquonque moyen de communication (téléphonique, mail,...) ou même physiquement, pour quelqu'un que l'on n'est pas afin d'obtenir des informations confidentielles. Une technique courante sur les webmail consiste, par exemple, à envoyer un mail semblant provenir de son administrateur et prétextant une panne du serveur pour vous demander de vous réenregistrer en demandant login et mot de passe, qui seront alors renvoyés au pirate. Partez donc du principe qu'en aucun cas, un organisme ou une société chez qui vous avez un compte ne vous demandera votre mot de passe, tout au mieux votre login.

Une société

Votre entreprise est, peut-être pour des raisons promotionelles évidentes, présentes sur le web. Cela peut être, si vous ne filtrez pas l'information qui y est diffusée, une source de renseignements supplémentaires pour l'attaquant. Le statut de votre entreprise, le nom des employés et leurs adresses emails, le nom et adresse du webmaster dans les codes sources de vos pages web, des liens non securisés vers des parties non destinées au public... Voilà autant d'éléments supplémentaires que votre pirate se fera une joie de récupérer.
De plus, on voit souvent des cas ou les paires logins/mots de passe des utilisateurs du réseau de l'entreprise correspondent à des couples nom-prénom. Si ces informations sont présentes sur le site, notre pirate pourrait essayer l'ensemble des combinaisons possibles en construisant une liste de login/password probables obtenus sur le site. Nous ne le répèterons donc jamais assez, mais il est impératif de filtrer totalement l'information fournie.

Après avoir récupéré un certain nombre de renseignements sur le système cible, le pirate va passer à des opérations plus techniques, qui doivent être effectuées sur le système, afin de pouvoir procéder par la suite à l'élaboration d'une stratégie d'attaque.

Evaluation des caractéristiques d'un système

Le scan de ports ou "à la recherche d'applications serveurs actives"

Il faut avant tout préciser ce qu'on entend par "système". Au niveau de ce cours ne seront expliqués que les procédés utilisées lors de la réalisation d'attaques sur un ordinateur, et non pas un réseau. C'est-à-dire que l'on va voir quelles stratégies et méthodes adoptent les pirates lorsqu'ils souhaitent s'attaquer à un système précis. Nous vous conseillons d'appliquer l'ensemble des techniques présentées ici de façon individuelle à chacune de vos machines, afin de savoir savoir ce qu'un pirate pourrait détecter. A la fin de cette session seront présentés des outils permettant d'empêcher un éventuel pirate d'exploiter ces faiblesses.

Ce petit éclaircissement posé, abordons le plus essentiel des processus : le "scan de ports".

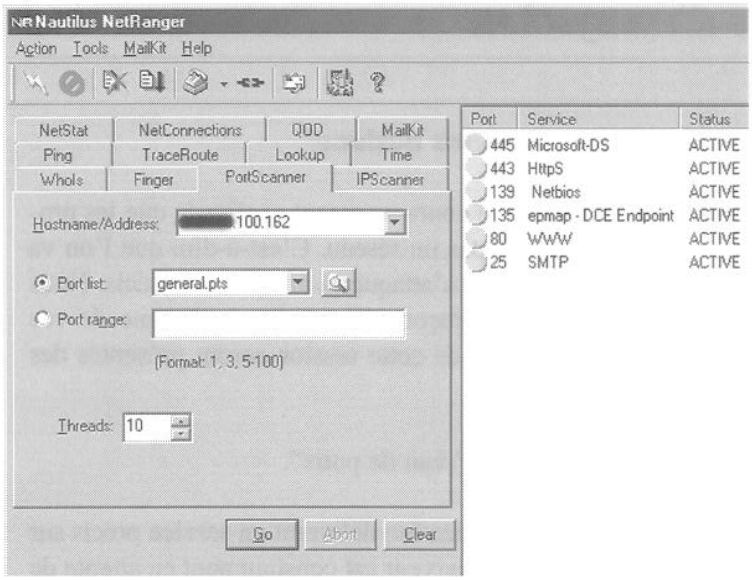
Rappelez-vous le début de ce cours. Une application serveur, c'est une application délivrant un service précis sur la requête d'un client, dans le cadre d'une configuration adaptée. Donc, un serveur est constamment en attente de connections, et pour ce faire, il monopolise un port précis, entre 1 et 65535, qui lui ouvre un canal de communication. C'est un peu schématique par rapport aux données techniques complexes qui régissent le processus, mais l'essentiel est là.

Scanner les ports va donc permettre à un pirate de repérer les applications serveurs actives. Chaque port ouvert peut ainsi être considéré comme un point d'entrée au système, une éventuelle source de vulnérabilités.

Note : Scanner les ports, c'est simplement envoyer, grâce à un logiciel, des paquets TCP avec le flag SYN activé, aux ports du système distant.

Effectuer un scan de ports sur une de vos machines est très simple. Moult logiciels hantent l'internet à cet effet. Dans nos pratiques, nous utiliserons Nautilus NetRanger, qui est très efficace et très rapide. Vous le trouverez sur http://www.download.com, ou encore sur le site des développeurs (http://www.nautidigital.com).

1. Ouvrez le logiciel.
2. Cliquez sur l'onglet PortScanner.
3. Dans la zone "Hostname/Address" indiquez une adresse IP ou un nom d'hôte.
4. Dans la zone "Port range", indiquez une plage de port ou un port spécifique à vérifier. Une plage de ports c'est un ensemble de ports compris dans une intervalle. Dans le cas de Nautilus, spécifier une intervalle de port de type [3000 ; 6000] se fait selon la syntaxe suivante : "3000-6000". Vous pouvez aussi n'indiquer qu'un seul numéro, cela reviendrait à ne vérifier qu'un seul port. Notez toutefois quelques petites choses. Un bon scan se fait sur une intervalle de 1 à 65535, c'est-à-dire sur l'intégralité des ports. En effet, il se peut que des applications serveurs se terrent dans des ports éloignés. C'est aussi pourquoi nous vous déconseillons l'utilisation de l'option "Port list", qui ne permet de vérifier que certains ports spécifiques.
5. L'option Threads définit le nombre de requêtes de scans de ports à envoyer en même temps. Au lieu de scanner les ports un par un, vous pouvez multiplier ainsi votre activité par plus de 30 fois ! Indiquez une valeur de 30 à 60 dans "Threads", qui est fonction de votre vitesse de connection. Evitez de mettre une valeur trop grande, cela risquerait de faire bugguer l'application. De même, n'ouvrez pas deux fois Nautilus NetRanger, utilisez une, et une seule, session d'application. Sinon, là aussi, le logiciel risquerait de patauger.
6. Lancez le scan, en cliquant sur "Go".



7. Au niveau des résultats, ne vous préoccupez pas de la couleur des pastilles. Seul les ports indiqués comme actifs ("ACTIVE") nous intéressent.

La liste des ports indiqués comme actifs révèle généralement la présence d'applications serveurs actives délivrant des services bien spécifiques. Afin de résoudre l'identité de ces serveurs, et des services qu'ils délivrent, les pirates peuvent émettre des hypothèses, mais se doivent, dans la mesure du possible, de confirmer ou d'infirmer. Il va donc être nécessaire de supposer à quoi correspond un port ouvert. Pour cela, l'utilisation de fiches textuelles, comme une liste de ports, peut être très utile. Ce genre de liste se trouve partout sur Internet (recherchez "Ports numbers" sur http://www.google.com, par exemple). Après avoir évalué par quel service est, probablement, monopolisé un port, le pirate doit parvenir à la certitude qu'il se trouve bien en face de ce qu'il suppose être.

Partir à la recherche d'informations sur le système d'exploitation

La chose la plus simple et la plus directe qu'un pirate puisse faire pour obtenir des informations sur un système, c'est de s'y connecter.

Utilisation de Telnet

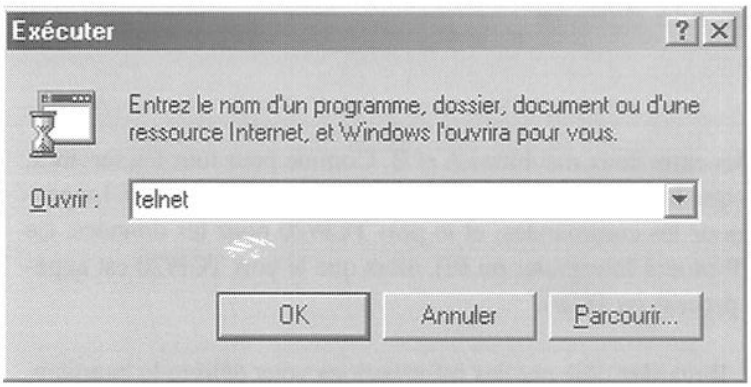
Telnet (Telecommunications Network) permet à une machine client de se connecter sur un serveur, et ce, quelles que soient leurs localisations dans le monde, pour peu que ces deux machines sont raccordées à l'Internet. Les clients telnet existent sur la quasi-totalité des plates-formes (Windows, Unix, MacOS, BeOS…). Il permet la connexion TCP sur n'importe quel port d'un machine distante.

Il y a deux façons d'utiliser correctement Telnet :

- En utilisant l'interface graphique
- En indiquant des options au programme au moment de le lancer

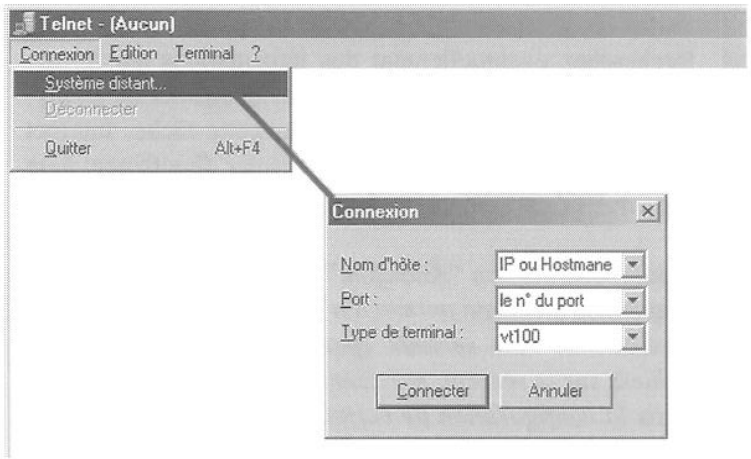
Pour la première solution, ouvrez telnet :

1. Cliquez sur "Démarrer",
2. Puis sur "Executer".
3. Tapez "telnet" et validez.
4. Cliquez sur "Connexion", puis sur "Système distant".
5. Dans la fenêtre, indiquez un nom d'hôte ou une adresse IP pour permettre la connection au système distant. Entrez ensuite un numéro de port. Attention ! Pour les services les plus courants (SMTP, FTP, HTTP, etc.) vous pouvez entrer comme indication non pas le numéro de port mais le service qu'il désigne. Par exemple, au lieu d'indiquer "80", vous pouvez indiquer "HTTP". Cette pratique vous est déconseillée pour au moins les motifs qui suivants :
   - Cela ne marche pas pour tous les services ;
   - Vous pourrez être amené à travailler sur un autre système où cette fonctionnalité ne sera pas présente ;
   - Implicitement, vous n'apprendrez pas la désignation numérique des différents ports ;



Pour accéder plus rapidement à des connections distantes, préférez la deuxième solution.

1. Cliquez sur Démarrer,
2. Puis cliquez sur Exécuter.
3. Tapez "telnet [IP] [PORT]", ce qui donne pour le site dmpfrance.com, par exemple, "telnet dmpfrance.com 80", ce qui vous connectera sur le service HTTP du site dmpfrance.com.



En vous connectant sur les différentes applications serveurs qu'exécute un système vous pouvez être à même de trouver bon nombre d'informations sur le système. L'annexe suivante décrit succintement par quel biais vous pouvez récupérer des informations sur les services sus-nommés :

- FTP
- SMTP
- HTTP
- SNMP
- Telnet

Repérer des informations sur un système est une tâche très facile, les systèmes ayant une grande facilité à s'auto-présenter, à travers ce qu'on appelle des "bannières". L'immense majorité des systèmes ne disposent pas d'une configuration adéquate. Mais malgré les différentes tentatives (désespérées ?) que peuvent émettre les administrateurs systèmes concernant leurs configurations, certaines informations ne manqueront pas d'alerter un pirate averti. Avec un peu de pratique, il s'avèrera que ce processus de récupération d'informations sera de plus en plus simple. Après un rapide coup d'œil sur le type et la version du serveur HTTP, par exemple, un pirate pourra déterminer sous quel système d'exploitation tourne une machine-serveur (Windows NT 4, 2000, Unix...).

Une petite note au sujet de ce chapitre et des informations obtenues par rapport aux scans de ports. La mise en lumière de l'activité de certains ports peut révéler des informations sur le type de système distant comme les ports 135 à 140 (service NetBIOS de Windows), 111 (SunRPC sur des stations SUN)... Pour identifier le service qui tourne derrière un port, le pirate se réfère à sa liste de ports, puis il se connecte, et enfin il recherche des informations sur le service concerné via Internet. Il est tout à fait possible que vos systèmes fassent tourner des applications serveurs développées uniquement sous Windows ou sous Unix. Le fait de connaître le système d'exploitation d'une machine distante permettra alors au pirate de cibler la façon dont il pourra l'approcher.

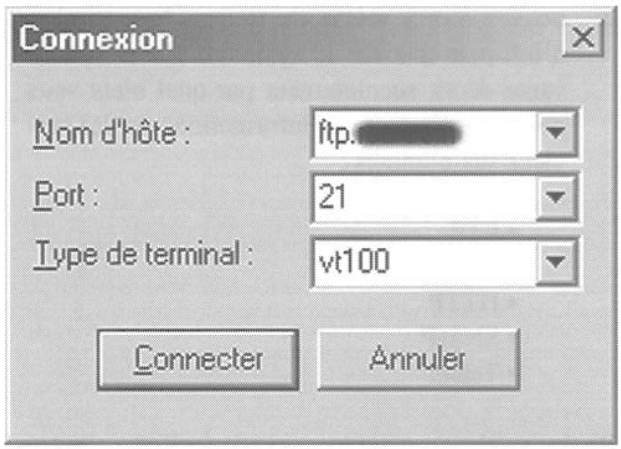
***Note** : Lorsque A envoie une requête à la machine B, celle-ci est à l'écoute permanente des requêtes présentées sur le port TCP (23 par défaut). B répond alors par une demande d'authentification, à laquelle A doit répondre (login + password). Lorsque cette phase est réussie, l'entrée standard est redirigée sur le clavier de A, et la sortie standard est redirigée sur l'écran de A. Tout se passe comme si l'utilisateur de A était devant la machine B, alors que des milliers de kilomètres peuvent les séparer.*

Récupérer des informations sur des services donnés

FTP : Files Transfert Protocol

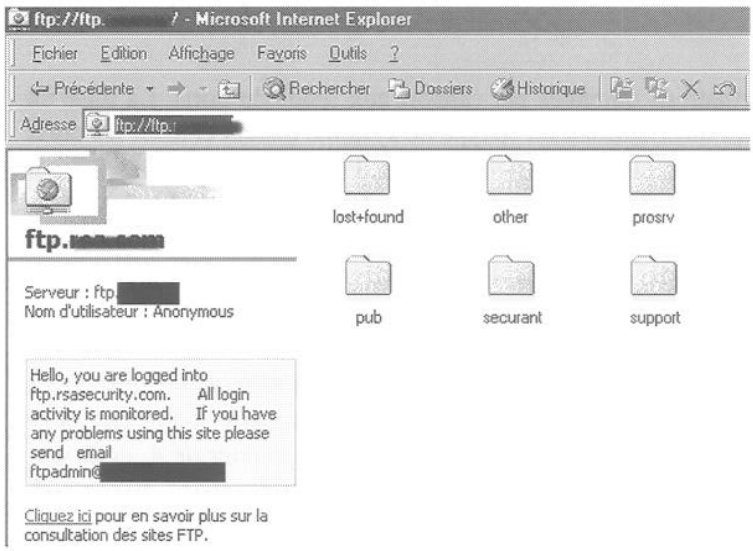
FTP est utile dès qu'il s'agit de transférer des données entre deux machines A et B. Comme pour tous les services, la machine A doit être équipée d'un client ftp, alors que la machine B est, elle, équipée d'un serveur FTP. Le protocole TCP utilise par convention le port TCP/21 pour les commandes, et le port TCP/20 pour les données. Le port TCP/21 est appelé l'interpréteur de protocole (Protocol Interpreter ou PI), alors que le port TCP/20 est appelé processus de transfert de données (data transfert process ou DTP).

Connectez-vous au service FTP visé, via le port 21. Regardez déjà quelles informations vous délivre la bannière, s'il y en a.



Recherchez éventuellement des informations sur le serveur mentionné. Puis tentez de vous connecter en anonyme. Préférez votre navigateur pour cette tâche. Internet Explorer vous permet de vous connecter directement à un service FTP, par défaut en Anonyme.

Note : Une session "Anonyme" est une session gérée par l'administrateur qui permet à n'importe qui de profiter du service FTP du serveur (pour le téléchargement de fichiers sur le serveur, par exemple).
Mais la configuration de certains services FTP, qui laissent la possibilité d'accès à des sessions anonymes, est parfois désastreuse au point que certains sites laissent traîner l'accès au fichier "passwd" (d'arborescence "/etc/passwd", sous un système linux, ce fichier contient tous les logins actifs sur la machine), ou encore l'arborescence complète du site, voire même des répertoires avec des accès écriture (où tout le monde peut envoyer des fichiers généralement).



Depuis Internet Ecplorer le "browsing" (un affichage) des répertoires révèle des répertoires typiques de systèmes de type UNIX. Il s'agit de vérifier si c'est véritablement le cas. Ouvrez une session FTP via telnet et connectez-vous en Anonyme.

Note : N'hésitez pas à consulter les différents répertoires accessibles afin de vous faire une idée sur le système.

Généralement, sous FTP, les commandes ne varient pas selon les serveurs. Ainsi, pour vous connecter il vous faudra utiliser la syntaxe suivante :

1. USER Anonymous [pour rentrer en Anonyme]
2. PASS machin@chose.com [généralement, vous aurez à indiquer votre adresse e-mail comme mot de passe]

Ensuite, vous vous retrouverez à l'aveugle, surtout si vous ne connaissez pas le système. Les commandes qu'il vous est possible d'enregistrer sont généralement listables par la commande "help" ou "?".

Sur l'exemple ci-dessous, les commandes du service FTP ont été utilisées (sur un autre système) pour mettre en lumière le type de système d'exploitation utilisé. Ici, les informations délivrées sont d'une importance mineure. Ceci dit, certains systèmes vont jusqu'à révéler la version du système d'exploitation, ce qui est manifestement plus grave.

```
USER Anonymous
331 Guest login ok, send your complete e-mail address as password.
PASS ojjojjjgcfhb@uhgFdhFvbopo.con
230-You are user #1 of 50 simultaneous users allowed.
230-
230 Logged in anonymously.
help
214-The following commands are recognized (* => unimplemented, + => extension).
214-    ABOR    CWD     MKD     OPTS+   REIN    SITE    STRU*
214-    ACCT*   DELE    MLSD+   PASS    REST    SIZE    SYST
214-    ALLO*   FEAT+   MLST+   PASV    RETR    SMNT*   TYPE
214-    APPE    HELP    MODE    PORT    RMD     STAT    USER
214-    CDUP    LIST    NLST    PWD     RNFR    STOR
214-    CLNT+   MDTM    NOOP    QUIT    RNTO    STOU
214-
214 Send comments to ovh@ovh.net.
MLST
250-Begin
 type=dir;modify=20001027233524;UNIX.mode=0755 /
250 End.
FEAT
211-Extensions supported:
 CLNT
 MDTM
 MLST type*;size*;modify*;UNIX.mode*;UNIX.owner;UNIX.uid;UNIX.group;UNIX.gid;uni
que
 PASV
 REST STREAM
 SIZE
 TVFS
 Compliance Level: 19981201 (IETF mlst-05)
211 End.
```

SMTP : Simple Mail Transfert Protocol

Le protocole SMTP est certainement un des protocoles le plus utilisé sur l'Internet. Son but est de permettre le transfert des courriers électroniques. Il est similaire au protocole FTP, de part son langage de commande. Il est généralement implémenté sur le port TCP/25.

Comme pour tous les autres services, un service SMTP peut révéler, par sa bannière, des informations. Mais le plus intéressant, c'est l'intégration, non nécessaire, de deux commandes spécifiques au service SMTP. Ces deux commandes sont "vrfy" et "expn". Pour vérifier si elles sont accessibles, tapez "help".

- Vrfy : cette commande a pour but de vérifier si une adresse e-mail existe à l'adresse du serveur questionné. Ce qui veut dire que si vous vous connectez à un système d'adresse "betetruc.com", que vous tapez "vrfy admin", et que le système vous répond positivement, c'est qu'il existe une adresse "admin@betetruc.com", et donc certainement un compte de login "admin" sur le système. Il est donc possible de récupérer des logins sur le système concerné.
- Expn : cette commande permet de vérifier l'existence d'alias au sein d'un système pour un compte donné. Un alias permet à une personne physique d'avoir plusieurs adresses e-mails. Cela peut être une bonne source d'informations.

```
Connexion  Edition  Terminal  ?
220 [redacted] ESMTP Sendmail 8.9.3/8.9.3/FDN; Thu, 31 Jan 2002 01:59:29 +0100
help
214-This is Sendmail version 8.9.3
214-Topics:
214-    HELO    EHLO    MAIL    RCPT    DATA
214-    RSET    NOOP    QUIT    HELP    VRFY
214-    EXPN    VERB    ETRN    DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation send email to
214-    sendmail-bugs@sendmail.org.
214-For local information send email to Postmaster at your site.
214 End of HELP info
vrfy root
250 <root@jab      .fr>
expn root
250-<antoine@or        .fr>
250-<xavier@bab        .fr>
250-<pj@gizmo     .fr>
250-<lulu@ro          fr>
250 <bureau@e         .fr>
vrfy antoine
250 Antoine Hulin <antoine@ja        .fr>
```

Dans l'exemple ci-dessus, le pirate a réussi à avoir des informations sur l'identité d'une personne, et sur les alias tournant pour "root" (certainement des adresses correspondant à d'autres administrateurs systèmes).

HTTP

Pour vous connecter à un système via HTTP, utilisez le port 80. Après quoi, il vous est possible d'envoyer différentes commandes au système, celles-ci pouvant avoir des conséquences différentes. Le procédé consiste à envoyer d'abord une commande valide, puis à rappuyer sur ENTER afin de renvoyer une validation.

Prenons un exemple concret :

1. Connectez-vous sur www.microsoft.com (telnet www.microsoft.com 80)
2. Entrez comme commande : OPTIONS / HTTP/1.0
3. Validez en appuyant sur ENTER, et revalidez à nouveau.
4. Les informations contenues dans P3P ("Platform for Privacy Preferences") désignent les informations collectées sur les utilisateurs. Référez-vous à http://www.w3.org/TR/P3P/ pour en savoir plus sur le système P3P.


```
OPTIONS / HTTP/1.0
—
HTTP/1.1 404
Server: Microsoft-IIS/5.0
Date: Thu, 21 Mar 2002 23:06:53 GMT
P3P: CP='ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR S
AMo CNT COM INT NAV ONL PHY PRE PUR UNI'
Pragma: no-cache
cache-control: no-store
Connection: Keep-Alive
Content-Length: 20049
Content-Type: text/html
Expires: Thu, 21 Mar 2002 23:06:53 GMT
Cache-control: private
```

Il est aussi possible d'utiliser la commande GET et OPTIONS sur un même serveur, ceci permettant de révéler un certain nombre d'informations intéressantes de façon complémentaire.

```
GET / HTTP/1.0
—
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
P3P: CP='ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR S
AMo CNT COM INT NAV ONL PHY PRE PUR UNI'
Content-Location: http://tkmsftwbw09/default.htm
Date: Thu, 21 Mar 2002 23:10:30 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 20 Mar 2002 01:48:51 GMT
ETag: "90e1c362b1cfc11:886"
Content-Length: 26668
```

Un autre exemple ! IP : XXX.XXX.XXX.XXX : 80 - Service HTTP. Ici, le serveur révèle sa version ainsi que les commandes autorisées.

```
OPTIONS / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 21 Mar 2002 23:40:32 GMT
MS-Author-Via: MS-FP/4.0,DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PR
OPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Cache-Control: private

GET / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 21 Mar 2002 23:41:47 GMT
Connection: Keep-Alive
Content-Length: 1275
Content-Type: text/html
Set-Cookie: ASPSESSIONIDGGQGQSDC=KENDJHDBAKFGGDCIOEPBHJLJ; path=/
Cache-control: private
```

Mis à part la version du serveur et les modules qui tournent dessus, les informations récoltées ne sont pas toutes cruciales mais peuvent vous amener à mieux situer la configuration du système cible. Notez que vous serez normalement déconnecté du système, il s'agit de lire les informations sans quitter la session telnet (sans confirmer la déconnection). Par ailleurs, il se peut tout à fait qu'un service HTTP ne délivre qu'un nombre minimal d'informations, et ceci en raison de la configuration adaptée du serveur. Que ce soit sur les serveurs IIS ou Apache, vous pouvez contrôler et modifier les informations fournies par votre serveur, et donner de fausses pistes au pirate !

***Note concernant HTTP** : autant un serveur HTTP tel que IIS est soumis à de nombreuses failles, autant sur Apache, le nombre de failles est quasi-inexistant. Apache est une application serveur pour différents systèmes d'exploitations, y compris Windows. Il est entièrement gratuit et a forte tendance à concurrencer le serveur IIS en raison de sa qualité et de sa fiabilité. Il s'octroie d'ailleurs une plus grande part de marché que ce dernier. Mais ne vous fiez pas à ce modèle de sécurité : des erreurs de configuration inhérentes à la distraction de l'administrateur peuvent avoir de lourdes conséquences. Apache.org en a fait les frais en 99.*

SNMP : Simple Network Management Protocol

SNMP est un protocole de gestion d'équipement réseau qui permet à l'administrateur d'interroger ses équipements afin d'en récupérer des informations. Dans notre exemple, nous avons trouvé quatre équipements sur notre réseau qui figuraient dans le community string "public", c'est-à-dire que n'importe qui peut avoir accès aux informations que les équipements renvoient.

Vous pouvez trouver sur internet des outils qui permettent d'automatiser les requêtes. http://www.solarwinds.net/

Note : le community string "public" est, généralement, la valeur par défaut attribuée à une machine faisant tourner un agent SNMP. C'est à l'administrateur d'en modifier la configuration. Le contraire d'un string public est le string "private", qui, lui, n'autorise à ne délivrer aucune information au grand public.

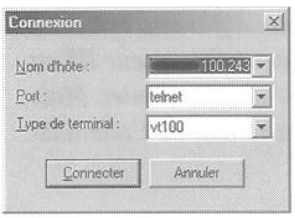
TELNET

Pas de miracle pour Telnet. Ce service est généralement restreint par une identification obligatoire par login et mot de passe. La bannière qu'affiche le système peut en revanche être utile. Utilisez telnet pour vous connecter. Par défaut, vous vous connectez sur le port 23, donc, il n'est pas nécessaire de spécifier de port.

```
Connexion  Edition  Terminal  ?

Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.17 on an i686
login:
```

Dans notre exemple, la version complète du système d'exploitation est dévoilée. Mais, et c'est tout aussi grave, la version du noyau (Kernel 2.2.17) l'est aussi. Avec de telles informations, ce type de système risque de ne pas tenir deux secondes face à un pirate de niveau moyen.

Pour l'imprimante réseau HP IP=XXX.XXX.100.243:23 (trouvée avec le scan SNMP ci-dessus), il semble que cela ne soit pas le cas.



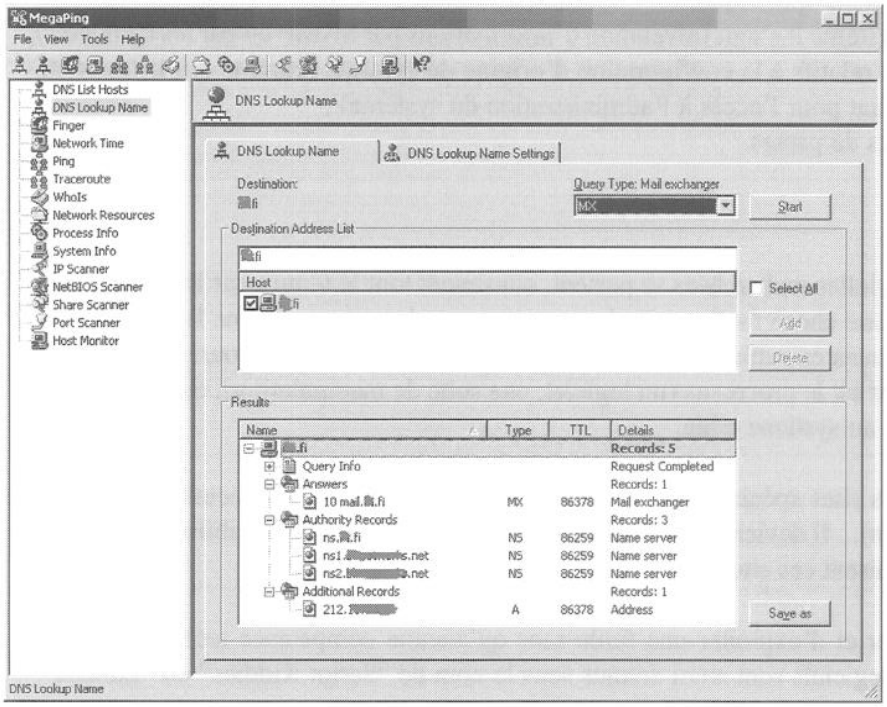

```
HP JetDirect

Please type "?" for HELP, or "/" for current settings
> ?

        To Change/Configure Parameters Enter:
        Parameter-name: value <Carriage Return>

        Parameter-name  Type of value
        ip:             IP-address in dotted notation
        subnet-mask:    address in dotted notation
        default-gw:     address in dotted notation
        syslog-svr:     address in dotted notation
        idle-timeout:   seconds in integers
        set-cmnty-name: alpha-numeric string (32 chars max)
        host-name:      alpha-numeric string (upper case only, 32 chars max
)
        dhcp-config:    0 to disable, 1 to enable
        ipx/spx:        0 to disable, 1 to enable
        dlc/llc:        0 to disable, 1 to enable
        ethertalk:      0 to disable, 1 to enable
        banner:         0 to disable, 1 to enable

        Type passwd to change the password.

 Type "?" for HELP, "/" for current settings or "quit" to save-and-exit.
 Or type "exit" to exit without saving configuration parameter entries
```

Le transfert de zone DNS

Si vous possédez un réseau ouvert sur le monde, ainsi que plusieurs ip sur le net, il est fort probable que vous possédiez un serveur DNS, ou serveur de noms de domaines. Son rôle est de fournir aux visiteurs l'adresse ip correspondant au nom du système demandé par l'utilisateur. Expliquons brièvement son fonctionnement sur lequel nous reviendrons dans le cours suivant.
Vous souhaitez vous connecter au site de www.dmpfrance.com

Vous allez alors envoyer une requête DNS au serveur DNS de votre fournisseur d'accès afin qu'il transforme www.dmpfrance.com en adresse ip à joindre. Cependant, cette adresse ip peut être, dans le cas d'un réseau important que vous possederiez, l'adresse ip d'un serveur DNS propre à l'entreprise et appartenant à son domaine, que vous interrogerez à son tour, afin d'obtenir l'adresse ip de www.dmpfrance.com. Les adresses ip de ces serveurs DNS peuvent être obtenues comme vous avez pu le voir par l'intermédiaire des banques de données whois.
Le serveur DNS, pour être en mesure de savoir quel ip correspond à quel nom d'hôte, maintient à jour une table de correspondance. A quoi sert donc ce transfert de zone ? Simplement à mettre à jour cette table de correspondance auprès d'autres serveurs DNS, généralement un serveur DNS de sauvegarde.
Malheureusement pour nous, si votre serveur est mal configuré, il peut autoriser la consultation de cette table à n'importe qui. Le pirate aura alors accès aux adresses ip et aux noms de toutes les machines composant le réseau, noms qui sont souvent très révélateurs de leur rôle dans le réseau.
Une fois l'ensemble de ces informations obtenues, le pirate cherchera laquelle semble la plus vulnérable, profitant de cette faiblesse pour s'introduire dans votre réseau.

Ces informations peuvent être obtenues grâce à l'utilitaire MegaPing
(http://www.softpile.com/Internet/Utilities/Download_08678_1.html).



Il est toutefois possible de limiter ce transfert de zone, qui sous windows est autorisé par défault vers n'importe quel serveur. Pour ce faire, lancer l'utilitaire MMC sous \Services et Applications\DNS\[serveur]\Forward Lookup Zone\[Nom de Zone] | Propriété, cochez l'option Only to the following servers, et donner l'adresse ip de votre serveur de sauvegarde. Il est également possible de désactiver totalement ce transfert de zone si vous estimez ne pas en avoir besoin, en décochant l'option "Allow transfert zone".

Les différents types d'attaques

La configuration du système

Si un système s'avère mal configuré, le pirate peut tenter d'exploiter des erreurs de configuration, compromettant la sécurité du système. Ces erreurs de configuration nécessitent de bien connaître le fonctionnement du système ciblé car le principe de leur exploitation n'est pas le même que pour les failles. Elles sont variables, spécifiques à certains environnements, ce qui rend la facilité de leur exploitation, ainsi que les processus qui permettent de les exploiter, quasi-aléatoires.

Configuration par défaut : la faiblesse première d'un système.

En guise d'exemple de problème de configuration, on pourrait parler des systèmes dont la configuration d'origine n'a pas été retouchée. Les routeurs sont potentiellement les premières victimes de ces problèmes.

1. Le pirate va s'attaquer à un système spécifique;
2. Il va regarder de quel type de système il s'agit (révélation d'informations par SNMP ou par les bannières);
3. Il va rechercher des documents relatifs à la configuration d'origine du système (comme des listes contenant les mots de passes par défaut pour l'accès à l'administration du système) ;
4. Il va tester ces logins et/ou mots de passes.

Failles logicielles et exploits

Au niveau des serveurs, les failles logicielles recherchées se portent, quasiment tout le temps, sur les applications serveurs. Trouver des failles n'est pas une chose facile, et il n'est pas rare que les pirates, même les plus expérimentés, exploitent des failles déjà connues et publiques. Cette exploitation de failles se fait couramment par ce qu'on appelle des "exploits". Un exploit est le processus (un logiciel, une suite de manipulations, etc.) qui permet d'utiliser une faille pour porter atteinte au système cible.

Failles et exploits sont recensés sur des sites spécialisés comme SecurityFocus (http://www.securityfocus.com), Securiteam (http://www.securiteam.com)... Il devient donc facile de tester d'éventuelles vulnérabilités sur un système à l'aide des informations que diffusent ces sites.

Certains logiciels permettent de repérer et d'exploiter une faille sans qu'aucune compétence technique ne soit requise. Les utilisateurs de ce type de logiciels sont aussi connus sous le nom de "Script Kiddies" ou "Lamers".

Le "bruteforce"

Le BruteForce est une technique qui consiste à tester, pour un nom d'utilisateur donné, des séries de mots de passes. Cette technique est efficace sur les systèmes ne mettant pas de limite aux nombres d'essais de saisies de mots de passes. Référez-vous à l'article de HackerZ Voice n° 6, en ligne sur www.dmpfrance.com, pour en savoir plus sur les méthodes et processus d'identification.

Comme il est possible de le constater, l'attaque est ce qu'il y a de plus court à faire, car c'est blanc ou noir. L'attaque marche ou ne marche pas. Certes, certaines attaques peuvent être longues, d'autres très brèves, d'autres compliquées... Des faiblesses peuvent apparaître lors de la recherche d'informations sur le système, permettant de réaliser une attaque sur l'instant.

Protéger votre système

Avoir une bonne politique de mot de passe

Vous l'aurez constaté au cours de ces différents chapitres, des mots de passe faibles, c'est-à-dire faciles à deviner, ou ayant un quelconque rapport avec un élément de votre vie personnelle sont une faille béante que n'hésiteront pas à employer certains pirates qui n'ont pas peur du manque de discrétion. Il faut cependant savoir que ce sont ces mots de passe dits faibles qui sont à l'origine de la majorité des intrusions. En effet, les pirates disposent de dictionnaires de mots de passe qui peuvent faire plusieurs dizaines de mégabits, et dans lesquels sont listés les mots les plus farfelus que vous pourriez utiliser. N'ayez donc pas uniquement confiance dans la longueur de vos mots de passes.
Qu'est-ce qu'un bon mot de passe alors ? Considérez qu'il doit faire au moins huit caractères de long, et alternez caractères de type numérique et alphanumérique, par exemple :
r2Hm8jK10n
Evidemment, un intrus potentiel pourrait essayer toutes les combinaisons possibles, mais le temps que cela prendrait pour trouver un tel mot de passe rend cette option inenvisagable.

Faire disparaître ses bannières

Comme vous l'avez constaté, une personne recherchant des informations sur vos serveurs et sur votre système d'exploitation serait ravie de voir que vous laissez à sa disposition cette mine d'informations que sont les bannières. Il suffit donc d'en changer le contenu, et pourquoi pas même d'y insérer de fausses informations, qui induiront le pirate en erreur. Sous linux, pour changer la bannière du serveur telnet, il suffit de se rendre dans le fichier /etc/issue.net.. Pour les autres serveurs, les bannières se changent directement dans les fichiers de configuration qui leur sont propres.

La mise en place d'un firewall

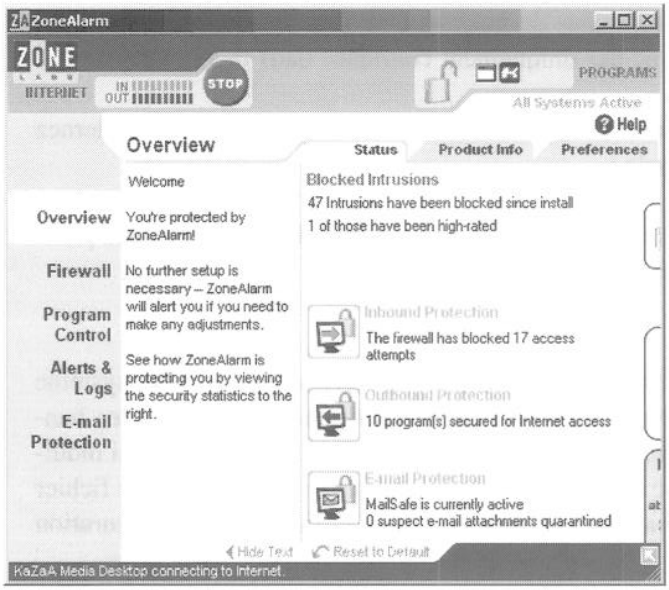
Un firewall a pour tâche d'empêcher toutes connections non désirées, et surtout non autorisées à l'un de vos serveurs. Il interdit donc toutes connections sur l'ensemble des ports 1-65535, si celles-ci n'ont pas été spécifiées comme étant autorisées. Il existe deux poliques différentes de règles à appliquer, l'une bonne, l'autre mauvaise :
- on interdit tout, puis on explicite spécifiquement ce qui est autorisé, il s'agit naturellement de la bonne politique
- on autorise tout, puis on explicite spécifiquement ce qui est interdit, il s'agit de la mauvaise politique

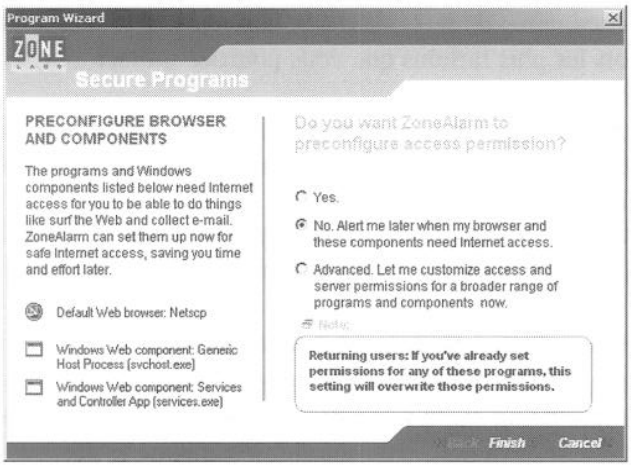
Pourquoi donc un administrateur utiliserait cette deuxième politique alors qu'il est évident qu'elle n'est pas souhaitable : parce que certaines applications et certains serveurs nécessitent de créer plusieurs canaux de communication, et cela demande une configuration plus délicate des règles de filtrage au niveau du firewall pour permettre à celles-ci de fonctionner correctement. Cependant, cette négligence peut avoir des conséquences désastreuses en ce qui concerne l'intégrité de votre système.

Il est une autre notion à expliquer concernant les firewalls qui n'est pas forcément évidente au premier abord. Quand on parle de firewall, on pense toujours au fait de bloquer les connexions entrantes, c'est-à-dire celles qui sont destinées à vos serveurs. Ceci est vrai mais pas complet. Un firewall peut également empêcher les connexions sortantes. Pourquoi donc utiliser une telle option ? Il y a d'abord les cas où vous voudriez empêcher les utilisateurs de votre système de perpétrer des actes de piratage, ou d'accéder à certains services, mais ce point ne sera abordé que plus tard. Il existe un autre cas où le pirate, conscient du fait que votre firewall lui interdise toutes connexions à votre serveur, vous fasse exécuter un programme à votre insu qui se chargerait de se connecter à son ordinateur, établissant une connexion sortante, et à l'aide d'une autre technique qui ne sera pas expliquée ici, lui permettra de prendre possession de votre système, malgré son impossibilité à se connecter à celui-ci.
Il existe pour cela un excellent freeware du nom de Zone Alarm (www.zonealarm.com), très simple d'utilisation, mais qui a le désavantage de n'être réellement efficace que sur un poste mono-utilisateur. Il a cependant l'avantage d'avoir un système de mise en place de règles extrêmement simple. Par défault, et dès la fin de son installation, il interdit toutes connexions, qu'elles soient entrantes ou sortantes. Puis, à chaque fois qu'une connexion extérieure cherchera à accéder à l'un de vos serveurs, il vous demandera l'autorisation. De plus, pour chaque application sortante, c'est-à-dire qui cherche à se connecter au web, il vous demandera également l'autorisation de laisser cette

connexion s'établir. Vous aurez la possibilité bien sûr de rendre cette autorisation permanente en cochant la case adéquate lors de l'affichage du menu d'avertissement. Enfin, ce firewall bloquera et enregistrera (vous donnant l'ip de l'assaillant) les attaques lancées contre votre système, ainsi que les requêtes icmp_echo_request (ping) et les scans de ports et, bien entendu, chaque tentative de connexion.

Voici le panneau de commande général de zonealarm:





Et les tentatives d'accès depuis/jusqu'à votre ordinateur sont affichées dans des fenêtres différentes:

Dans ce cas, zonealarm a bloqué une demande de connection provenant de l'adresse 192.168.2.20 en de notre serveur netbios.

Dans ce cas, zonalarm demande s'il a l'autorisation de laisser le programme ping.exe aller sur internet. Si vous n'avez lancé aucun programme qui devrait aller sur le net, vous devriez refuser sa sortie. Il peut s'agir d'une application installée par un pirate dans votre système pour le contrôler à distance, ou pour vous voler des informations.

La recherche de données sur Internet

Qu'elle soit informaticienne, pirate ou novice, une personne doit être à même de mettre à sa contribution toutes les ressources à portée de sa main. La première zone d'information qu'ait une personne dans ce domaine n'est plus la littérature. C'est Internet.

Savoir mener des recherches efficaces sur Internet est la clef de la réussite. Personne n'a la science infuse, mais le rassemblement des masses de données sur un seul et même réseau permet à n'importe qui d'avoir accès à n'importe quel savoir.

Les sources d'informations sur le piratage ne sont pas aussi rares qu'on pourrait le croire. Certes, les sites illégaux diffusant moult "cracks" ou tutoriaux illégaux sont difficilement repérables. En revanche, les sites légaux et sur le thème du piratage sont aussi nombreux que leurs sujets sont diversifiés.

Les sites sur la sécurité informatique sont de bien meilleures sources d'informations que des pages personnelles sur le piratage. En effet, ce sont en général des personnes qualifiées qui adminisitrent ces sites, et non pas des personnes en carence de savoir. Par conséquent, on ne saurait trop vous recommander ces sites. Ils fournissent une documentation généralement riches en information et offrent de nombreux points d'accès vers des tutoriaux qui s'adressent aussi bien aux débutants qu'à des personnes qualifiées.

Les sites sur les vulnérabilités sont des mines d'or en matière de sécurité. Ils servent aussi bien aux administrateurs réseaux soucieux d'établir des stratégies de sécurité planifiées qu'aux pirates. Ce sont souvent de véritables bases de données en matière de failles, de bugs et de problèmes relatifs à la sécurité informatique. Ainsi, n'importe qui peut évaluer la sécurité de son système à partir des failles connues et recensées par ces sites.

Les moteurs de recherche sont également de puissants alliés. Permettant de rechercher des sites en tout genres sur le sujet, ils sont toutefois à mettre dans des catégories à part. Les liens vers les nombreux sites qu'ils créent ne sont parfois pas de bonnes références. En revanche, avec un peu d'habitude, vous apprendrez rapidement à mener des recherches efficaces. Les mots clefs à taper sont par exemple :

- sécurité + n (où n représente l'objet sur lequel vous portez vos recherches)
- "sécurité des n" (où n représente cette fois plusieurs objets tels que "serveurs" "routeurs" "ordinateurs", etc.)

Vous pouvez également rechercher de la documentation plus généralisée sur des dispositifs de sécurité en ne tapant que des mots clefs comme "firewalls".

Les rebonds de sites en sites s'effectuent grâce aux sections de liens que mettent en place les webmasters. D'un lien sur un site vous passez à un autre. Cette solution de recherche a un double côté. D'une part, vous tomberez souvent sur des sites rarement visités, car mal représentés, et qui sont pourtant d'excellentes sources d'informations. D'autre part, vous tomberez souvent sur des liens morts ou des sites non mis à jour. C'est une chasse au trésor, en moins fastidieux : on voit du paysage !

***Remarque** : vous noterez que l'on n'aborde dans nos sujets de recherche qu'un angle de vue sur la sécurité informatique. En effet, le piratage peut amener à mieux comprendre la sécurité, et le contraire est tout aussi vérifiable. Pouvoir effectuer ce chemin en double-sens est un atout.*

Espionnage de systèmes informatiques

Il existe un ensemble conséquent d'outils, de surcroît très simples d'utilisation qui peuvent être utilisés par un pirate dans le but de s'introduire dans votre système, puis dans garder l'accès tout en vous espionnant. Nous parlerons notamment des troyens dont vous pourriez être la victime, qui donnent à un pirate un accès sans intrusion préalable. Et ce n'est pas le seul outil qui peut être utilisé : nous parlerons également des keyloggers qui espionnent vos frappes claviers, des méthodes pour effacer sa présence de votre système. Pour chacune de ces attaques, il existe heureusement des moyens de s'en protéger, à la condition naturellement de porter un minimun d'attention à la sécurité de son système. Cette section portera uniquement sur windows, les techniques sur des systèmes de type unix étant similaires.

Keylogging

Le Keylogger (traduction littérale : "enregistreur de clefs") est un dispositif en apparence simple, dont le concept est de se placer, à un niveau logiciel, entre l'utilisateur et le traitement des données qu'il effectue par le clavier. En clair, cela veut dire que tout traitement, toute frappe, fait au clavier sera enregistré par le logiciel et stocké sous forme d'un fichier consultable par la suite. Ainsi, le Keylogger s'avère être un système de surveillance fiable qui permet d'enregistrer de nombreuses choses comme des saisies de mots de passes, des saisies d'adresses, de rédactions de textes, etc. Pratiquer le Keylogging n'est pas une chose illégale en soi, à condition qu'il soit effectué sur votre machine, ou, si ça n'est pas le cas, que la personne surveillée ne le soit pas à son insu.

La plupart des Keyloggers sont invisibles. C'est-à-dire qu'ils fonctionnent en arrière-plan de toutes les applications Windows, de façon cachée, et qu'un utilisateur non averti ne s'apercevra nullement de la présence d'un tel outil d'espionnage.

Il existe foule d'applications de ce type, plus ou moins performantes, et dont le prix varie du "tout gratuit" au "tout payant" en passant par les versions d'évaluations et les sharewares.

Nous ne saurions trop vous recommander de tester en premier lieu les versions gratuites afin de trouver chaussure à votre pied. Faites par exemple un petit tour sur www.download.com en tapant comme mot clef pour votre recherche "keyloggers".

Avant de vous en présenter quelques-uns, sachez qu'un bon keylogger, qui est parfaitement invisible, ne va :

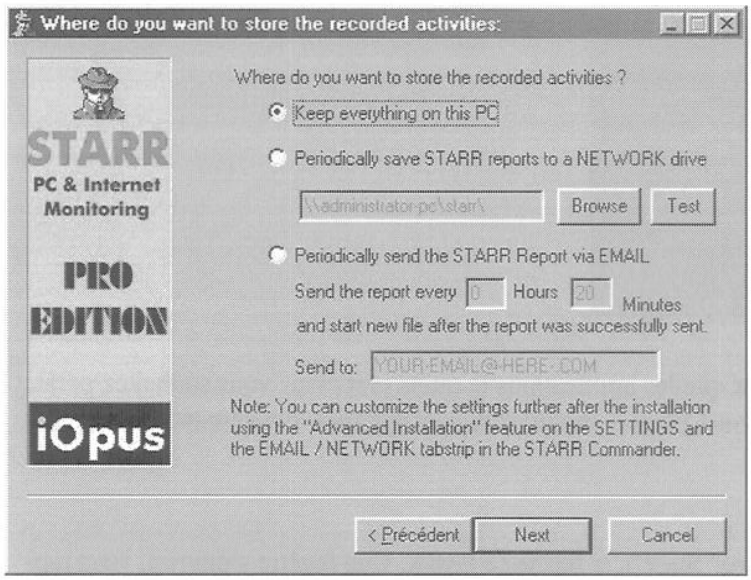
- manifester sa présence à aucun moment que ce soit ;
- être visible ni depuis la barre des tâches ni depuis le gestionnaire d'applications (CTRL+ALT+DEL).

Pour illustrer le propos, prenons un très bon exemple : iOpus STARR PC.

Installation

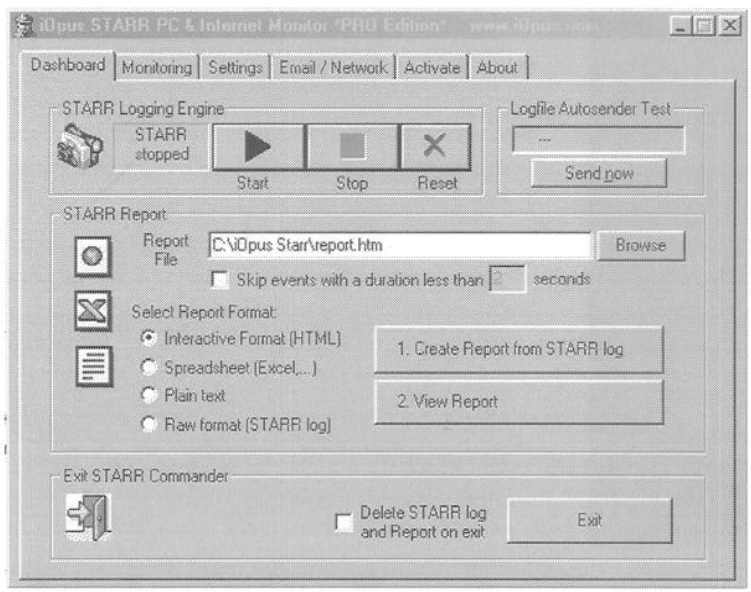
L'installation ne devrait poser aucun problème, même au moins initié. Sur la fenêtre de sélection de la zone d'enregistrement des "fichiers de log" (comprenez les fichiers où sont stockées les informations qu'a enregistrées le logiciel), vous avez trois possibilités :

- Garder les logs sur l'ordinateur où est installé le logiciel (par défaut, nous l'avons installé avec cette option). Si l'installation se fait avec cette option, cela veut dire que vous êtes obligés d'avoir un accès à la machine où STARR est installé ;
- d'enregistrer les fichiers de log sur un autre ordinateur du réseau local, sur un répertoire en partage.
- d'envoyer, par e-mail les fichiers de log.

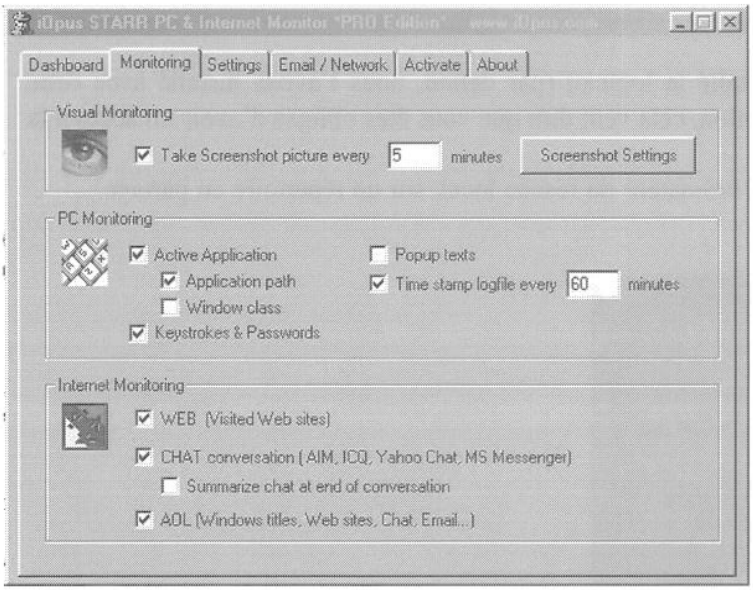


A la fin de l'installation, le logiciel s'ouvre, vous présentant sa fenêtre de gestion. Parmi les différents onglets à disposition seuls "Dashboard" et "Monitoring" sont susceptibles de nous intéresser. Le logiciel est entièrement en anglais mais n'en reste pas moins très facile d'utilisation.

Utilisation

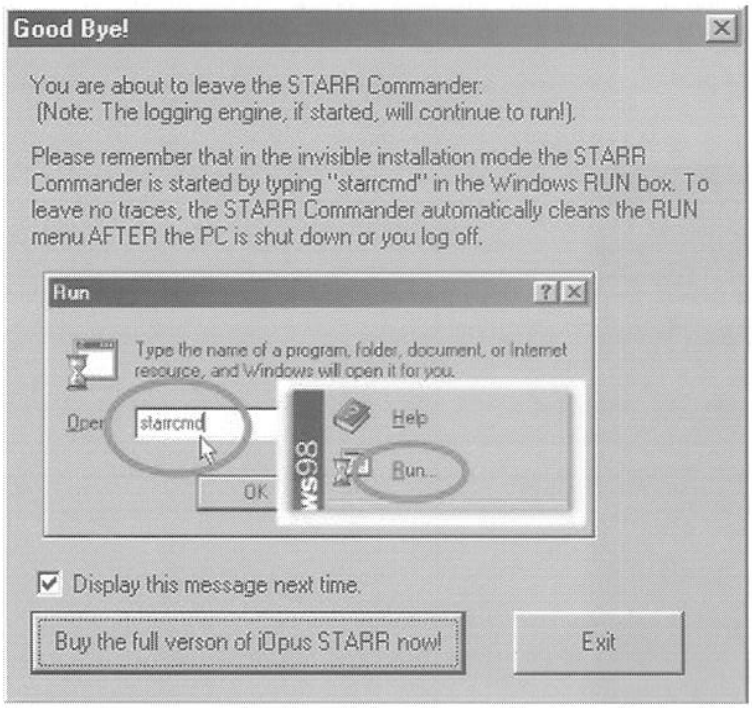


Le lancement d'une session de capture d'informations s'effectue par la touche "Start". Vous pouvez spécifier l'endroit où vous désirez placer le fichier de log, et aussi le format sous lequel vous désirez l'enregistrer, le format par défaut étant HTML. Nous vous conseillons de garder un format des fichiers de log en HTML, cette option permettant une lecture pratique et esthétique de l'activité enregistrée de l'ordinateur.



Par l'onglet "Monitoring" vous pouvez spécifier sur quelles applications et quels processus vous souhaitez porter votre surveillance. De même, en haut de l'écran, vous pouvez moduler la configuration concernant les captures d'écran ("screenshot") à votre guise.

1. Lancez une séance de capture (touche lecture/"Start"), et fermez STARR. Une fenêtre s'ouvrira, vous rappelant comment réouvrir STARR au besoin. Celle-ci indique qu'il vous faut passer par "Démarrer" "Exécuter" puis taper starrcmd.



2. Pour tester le logiciel, menez vos activités comme vous le faites couramment, et au bout d'une dizaine de

minutes par exemple, relancez STARR.

3. Pour afficher le résultat de l'enregistrement des données, cliquez d'abord sur le bouton "Creat Report from STARR log". Cette étape est obligatoire, sinon le logiciel ne créera pas le fichier log.

4. Ensuite cliquez sur View Report, ce qui vous ouvrira l'éditeur de texte ou de page approprié selon l'option d'enregistrement que vous avez choisi. Si vous avez gardé l'option d'un fichier log au format HTML. Ce sera alors votre navigateur web qui s'ouvrira.

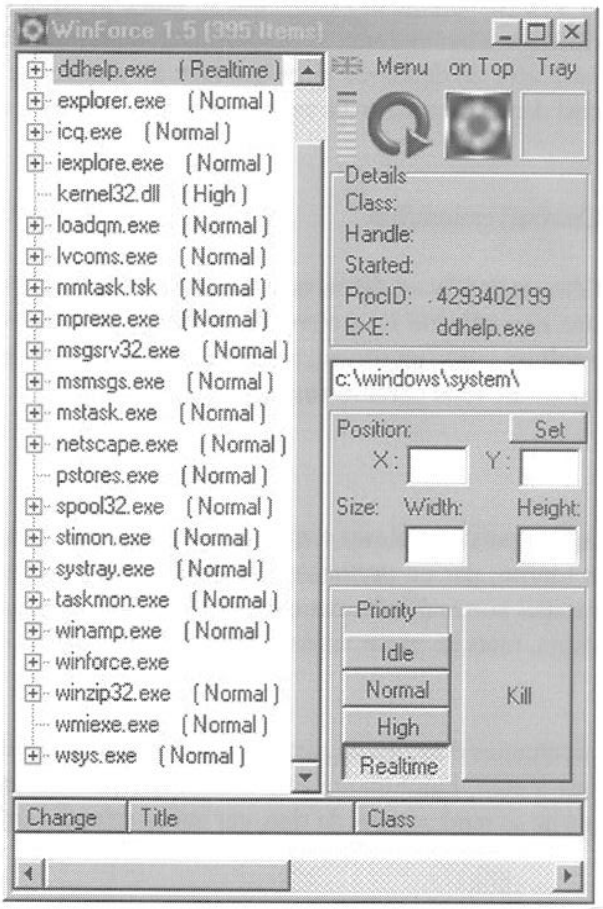
La magie de l'espionnage a fait son chemin, vous voici maintenant en possession d'un fichier de log complet, structuré et détaillé de toute l'activité de votre PC. Quelles protections à cette technique ?

Protection contre le Keylogging et les applications cachées

Si vous avez pris le temps de le faire, vous constaterez que STARR n'est visible ni par le gestionnaire de tâches ni dans la barre de tâches. A ce problème, pas de solution miracles. Il faut faire appel à un logiciel adapté. Nous en avons pris un, qui recense tous les processus actifs sur votre machine (comprenez toutes les applications qui tournent).

Winforce est un utilitaire gratuit, léger et très simple d'utilisation. Vous pourrez le trouver sur http://www.download.com. La fenêtre de gestionnaires d'applications de WinForce comporte deux fonctions essentielles :

- Actualiser ;
- Tuer.



La fonction Actualiser s'obtient par le bouton bleu en forme de flèche. Sélectionnez l'application à fermer et appuyez sur "Kill". L'application se fermera de force.

Autrement, des séries de symptômes peuvent être indices qu'un logiciel inconnu tourne en tâche de fond :

- La protection antivirus du BIOS vous informe d'un accès à la zone d'amorçage du disque dur.
- Lorsque vous lancez votre ordinateur, un message vous indique qu'il ne peut pas démarrer à partir du disque dur.
- Windows refuse de charger les pilotes de disque dur 32 bits.
- Au lancement de Windows, un message vous informe qu'un programme TSR force le démarrage en mode compatible MS-DOS.
- ScanDisk détecte des fichiers à liaison croisées ou d'autres problèmes.
- ScanDisk indique des secteurs défectueux sur les disques durs ou les disquettes.
- La taille des fichiers exécutables augmente subitement.
- La date de création ou de modification des fichiers comporte des valeurs erronées.
- Vous constatez que l'ordinateur se bloque fréquemment alors que vous n'avez ajouté aucun nouveau composant logiciel ou matériel.
- L'ordinateur se bloque et indique une erreur de parité.
- L'ordinateur semble être plus lent sans raisons apparentes.
- Le clavier et la souris ne fonctionnent plus de manière fiable, même après un nettoyage.
- Des fichiers ou des dossiers disparaissent de votre ordinateur de façon inexpliquée.
- Dans vos documents, des mots disparaissent ou s'ajoutent subitement.
- Votre ordinateur a des réactions imprévues, voire devient incontrôlable.

Ces symptômes sont plus globalement liés à l'activité de virus, mais certains d'entre eux sont récurrents pour divers types d'applications malicieuses. C'est le cas des ralentissements ou des dysfonctionnements.

On peut également considérer qu'il existe un point commun à l'ensemble de ces outils que le pirate pourrait installer chez vous : ils doivent être lancés au démarrage de windows. Pour ce faire, le programme, la première fois qu'il sera exécuté, devra créer une clé dans la base de registre afin de démarrer le programme au démarrage de windows. Nous étudierons la base de registre un peu plus tard dans ce cours, mais sachez que dans le cas où une telle clé serait créée, elle le serait dans la section :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Cette section regroupe l'ensemble des programmes devant être exécutés au démarrage. Il serait souhaitable que vous la consultiez après l'installation de votre système. Si une nouvelle clé s'y trouve répertoriée, alors que vous n'avez installé aucun programme, il est fort probable que ce soit un virus, un troyen, ou un keylogger. Soyez donc vigilant aux nouvelles clés qui apparaissent et dont le nom pourrait vous paraître suspect.

Le sniffing

Le sniffing, d'un point de vue théorique, est une méthode qui consiste à relever toutes les informations composantes d'un paquet réseau. Quel que soit le type de paquet (défini, par un protocole), le sniffer peut l'analyser. Ainsi, le sniffing devient une méthode efficace pour relever toutes sortes d'informations dans le champ de la zone de données d'un paquet. Tout peut y passer : noms d'utilisateurs, mots de passe, informations confidentielles, discussions, etc.

De plus, le sniffing est invisible. En effet, les informations contenues dans les paquets réseaux ne sont que subtilisées, et les paquets continuent de circuler comme si de rien n'était. Faire du sniffing n'implique pas même de perte de temps au niveau du transfert des données : la victime ne se rend compte de rien, car aucun ralentissement ne vient l'alerter.

Le sniffing est plutôt pratiqué dans des réseaux locaux, munis de hub ou sur des machines individuelles à l'aide de trojans, par exemple.

Ainsi définirons-nous le sniffing comme une méthode qui consiste à subtiliser des informations qui circulent sur un réseau à l'insu des utilisateurs concernés. Référez-vous aux explications détaillées et pratiques sur le Sniffing dans votre cours Newbie + pour en savoir davantage.

Espionnage à distance et prises de contrôles

Le meilleur système d'espionnage à distance qui ait jamais été conçu reste le trojan. Un trojan est une application de type dit "cheval de troie". Car, tout comme le cheval de Troie, il s'installe discrètement sur une machine à l'insu de l'utilisateur.

Comment marche un trojan ?

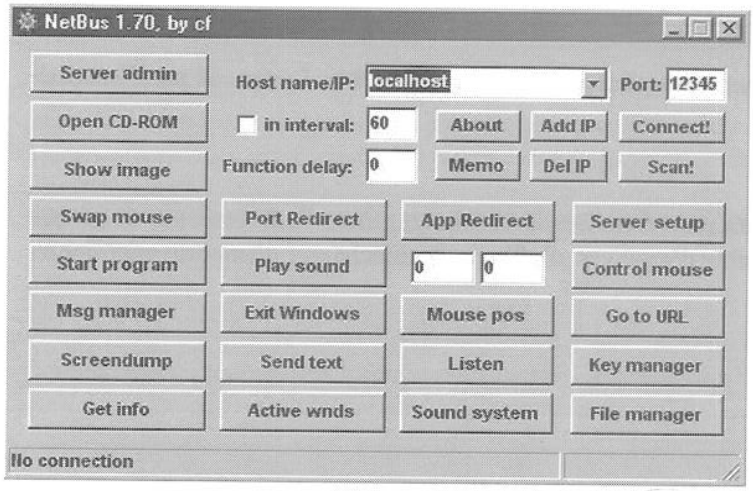
L'immense majorité des trojans se dissimulent dans des applications exécutables au format ".exe". Ces fichiers n'ont l'air de rien lorsqu'ils s'exécutent : des petits jeux, des animations, des faux messages d'erreurs... Mais ils installent en arrière-plan, sur la machine qui a exécuté le logiciel, une application serveur invisible. "Invisible" car l'utilisateur n'a jamais eu connaissance ni de son installation ni de son fonctionnement. Ce serveur va ouvrir un port, et attendre passivement des demandes de connections de la part d'un client adapté.

Le pirate, lui, dispose de l'application client, qui est la seule à pouvoir communiquer avec le serveur. Une fois connecté, il va pouvoir interragir avec la machine de la victime, ce qui va lui permettre de faire tout ce que le trojan lui permet. Ainsi, deux trojans différents ne permettront pas forcément à un pirate de faire les mêmes choses. Au fur et à mesure que les années se sont écoulées, les troyens ("trojan" au pluriel) ont fini par se complexifier, à se diversifier, à envahir d'autres systèmes d'exploitation... Le plus complet et l'un des plus célèbres de nos jours reste certainement Back Orifice 2000, mais le plus illustratif et démonstratif, de par sa simplicité d'utilisation, est Netbus.

Expérimentation

Afin de bien vous mettre en conditions, nous allons expérimenter, tester, et ainsi voir quelle peut être l'utilité d'un trojan. Dans cet exercice, nous allons prendre deux machines. L'une d'elles représentera la victime, l'autre le pirate. Le but de l'exercice est d'arriver à prendre un contrôle total et utile de la machine piratée. Nous utiliserons Netbus 1.7, car, bien que ce ne soit pas la dernière version, elle est largement suffisante pour nos démonstrations. Nous avons pris pour faire les essais deux machines dans un réseau local. L'une est infectée, l'autre sert à simuler la machine du pirate.

Interface



L'interface graphique de Netbus ne se compose que de boutons (grand bien fasse aux Script-Kiddies). Par défaut, l'adresse IP entrée dans "Host name/IP" est la vôtre. Et le port indiqué est "12345", qui est en fait le port qu'utilise le serveur de Netbus par défaut. Pas de danger lorsque vous exécutez le client : il n'est pas infecté par l'infâme cheval de Troie "netbus", quoiqu'en dise votre anti-virus.

Connection

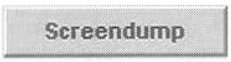
1. Utilisez la zone "Host name/IP" et indiquez-y l'adresse IP (ou le nom d'hôte) de la machine infectée

2. Cliquez sur "Connect!"

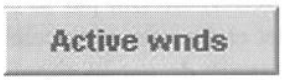
3. Une fois connecté, le logiciel devrait vous le signaler

Espionnage

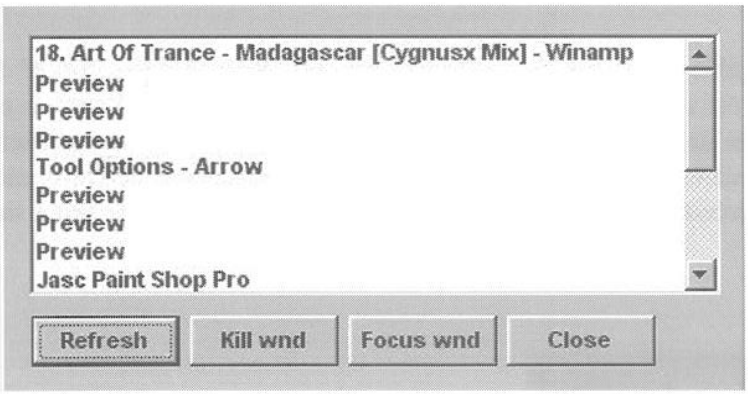
1. La première fonction d'espionnage que vous pourrez exploiter sous Netbus est certainement "Screendump", qui sert à faire des photos d'écran de la victime et à vous les envoyer directement.



2. Ensuite; vous pourrez toujours visualiser les processus actifs de la victime, comme si vous utilisiez son gestionnaire d'applications, grâce à la commande "Active wnds" ("Active windows", en français : "Fenêtres actives").

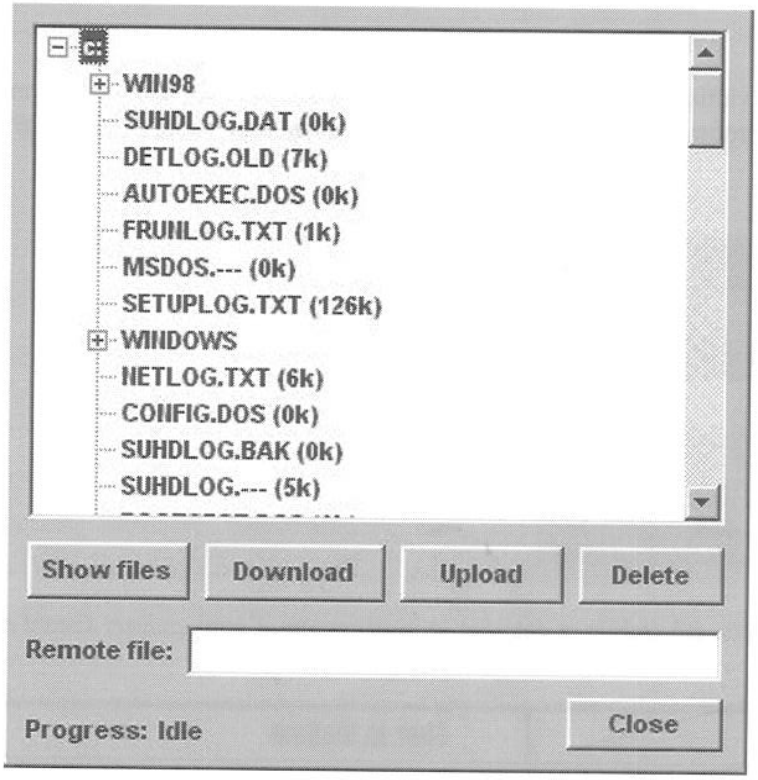


Ce qui vous offre, par l'intermédiaire d'une fenêtre interne, un listing des applications ouvertes. Il est nécessaire de rafraîchir régulièrement cette liste afin de maintenir une surveillance continue sur une cible.



3. Le gestionnaire de fichiers à distance est aussi très pratique et même effroyable. Lancez-le par l'intermédiaire de la touche "File manager"

Cliquez ensuite sur "Show files", ce qui aura pour fonction de télécharger toute l'arborescence du disque dur de la victime. Il devient désormais possible d'envoyer, d'effacer, de télécharger n'importe quel fichier sur le disque dur de la victime à son insu.



4. Les fonctions de Keylogging vues préalablement sont toujours actives : en effet, Netbus intègre un gestionnaire de clavier très performant puisque, non seulement vous pouvez lire en direct ce qu'écrit la victime, mais vous pouvez aussi écrire à sa place ! Ceci grâce à la fonction "Listen"

Une fois dans le gestionnaire de frappe de Netbus, sachez que toutes les touches (Oui, toutes ! Même ALT, TAB ou ENTREE) sont prises en compte.

Après quoi, vous avez la possibilité d'enregistrer ce qui a été frappé par la touche "Save text".

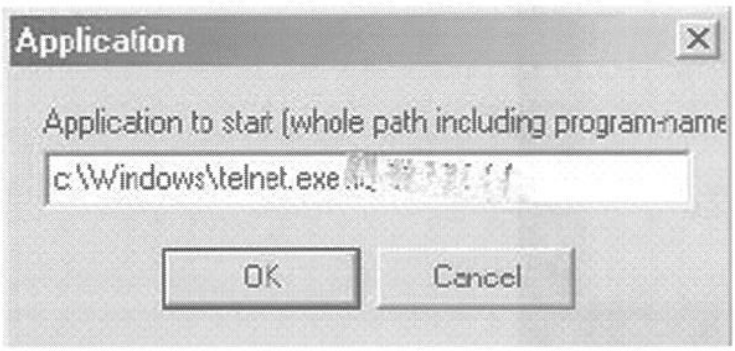
Démonstration d'une prise de contrôle

L'utilisation de trojans est quelque chose que beaucoup de pirates ont en horreur : c'est trop simple, ce sont des logiciels qui ne s'adressent quasiment qu'à l'attaque d'internautes, et non pas de véritables serveurs d'entreprise... Bref, la réputation du trojan au sein de l'underground laisse fort à désirer. Cependant un bon pirate peut faire une utilisation intelligente et calculée d'un trojan. Plutôt que de bêtement redémarrer l'ordinateur de la victime, il va essayer d'en prendre le contrôle afin de perpétrer ses attaques sous le couvert de l'anonymat le plus total. "Total", pourquoi ? Petit scénario :

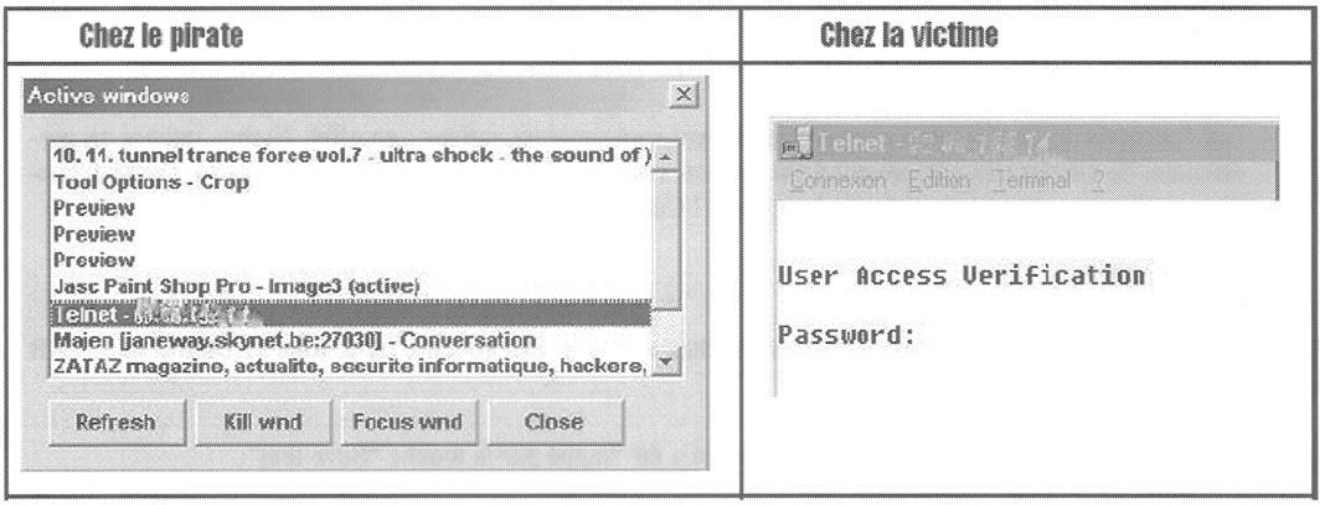
1. Le pirate désire attaquer le serveur X.
2. Il sait que s'il l'attaque de front ce serveur, son adresse IP risque d'être repérée au niveau des systèmes de sécurité du serveur X (firewalls, IDS, systèmes de logs...)
3. Il va donc utiliser un système par lequel il fera transiter ses demandes de connections, comme un routeur.
4. Sauf que, si il y a une enquête approfondie sur l'attaque, le pirate sait qu'ayant laissé son adresse IP sur le routeur, il prend des risques.
5. Il va donc utiliser l'ordinateur d'un malheureux particulier pour se connecter sur le routeur et ensuite attaquer le serveur X.
6. Il prendra ensuite soin d'effacer toute trace de ses manipulations chez la victime. Si l'opération se passe bien, il y aura une prise de risque quasi nulle, et, au pire, ce sera sa victime qui se fera inculper.

Pratique

En premier temps, le pirate se connecte à la victime. Cela fait, il lance une application telnet, afin de se connecter au routeur, par le biais du bouton "Start Program". Ce qui est brouillé sur l'image représente l'adresse IP que nous avons tenue au secret.



Il s'assure ensuite que la communication a bien été établie et ceci par le gestionnaire d'applications distant ou la fonction "Screendump"



Ensuite, il bloque le clavier de l'utilisateur, de sorte que celui-ci ne puisse intervenir dans les manipulations futures qu'il va effectuer, grâce aux touches "Key manager" puis "Disable all Keys".