-= Les Cours de Zi Hackademy =-

Newbie cours 3, by CrashFR

PLAN DU COURS :

- Cracking de mots de passe
. BIOS
. pwl, SAM, Passwd
. screensavers
. services HTTP, FTP, etc

- Anonymat
. Proxy

- Accès aux fichiers
. Disquette demarrage
. Exécuter
. Internet Explorer
. fichiers .bat
. fichier HTML
. Commandes MS-DOS - ActiveX

1 Qu'est ce que le cracking?

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

II 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 passe pour protéger l'accès a votre système d'exploitation (User Password) ou a la configuration du bios (Supervisor Password).

Sur le plupart des ordinateurs il faut appuyer sur le bouton "FI ", ou "F2", ou "Suppr", ou "CTRL+ALT+S" de votre clavier lors du démarrage de votre PC pour accéder a la configuration du BIOS (Bios Setup).

Il existe plusieurs méthodes pour cracker un pass Bios. Mais avant tout le hackeur 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.Premiere méthode.
Elle consiste a 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 !

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

- Appelle le programme "c:\DOS\debug" ou "c:\Windows\command\debug"

En 2 mots, ce prog avec le paramètre -O (Output) permet de transmettre directement un octet à un port de sortie dont l'adresse suit.
Q permet de quitter le prog. Inutile de préciser qu'il est assez dangereux à utiliser.

Sur les BIOS AMI :

"chemin"/debug -07017 -07117
-Q

Pour les BIOS Phoénix :

"chemin"/debug -0 70 FF -071 17
-Q
Généric : "chemin"/debug -0 70 2E -071 FF
-Q

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

Il existe aussi divers petits softs qui permettent de voir et d'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

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

2. Deuxieme 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 des fois une journée entière sera exigée pour que la mémoire se vide.

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

3.Troisième méthode.
Sur certaines carte mère il est possible de reset le pass BIOS en changeant de position d'un cavalier (en général le cavalier en question se trouve à coté du BIOS). Référez vous au manuel de votre carte mère pour plus d'informations. Des 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.Quatrieme méthode.
Elle consiste a court circuité 2 pattes du CI Bios a l'aide d'un strap. Pour cela il faut avoir la doc constructeur du CI qui nous permettra de savoir à quoi correspond chaque patte. Il faut faire très attention car un mauvais court circuit peut endommager votre CI et le remplacement sera inévitable.

5.Cinquieme méthode.
Si aucune de ces méthodes ne fonctionne, il faut reprogrammer le BIOS. Pour cela il faut démonter le BIOS, avoir un programmateur d' EEPROM (on peut trouver cela dans tous les magasins d'électronique) et surtout l'image de votre BIOS (fichier binaire contenant le BIOS).
Pour trouver l'image de votre BIOS il faudra faire un tour sur le site du fabriquant. Flasher un BIOS consiste a le reprogrammer. Il faut faire très attention avec le Flashing BIOS car il peut endommager votre EEPROM ou votre carte mère. La connaissance des bases d'électronique est conseillé.
On peut aussi flasher le bios a 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 a la suite des autres). Pour faire un dictionnaire efficace, il faut relever un maximum d'informations sur les utilisateurs du serveur cible. On peut trouver sur intemet une multitude de dictionnaires déjà tout fait, ainsi que des générateurs.

L'attaque par brute force
Cette attaque prouve bien qu'aucun pass n'est inviolable! En effet l'attaque par brute force consiste a essayer toutes les combinaisons possibles suivant un certains nombre de caractères. Si le mots de pass a cracker comprend plusieurs caractères spéciaux, chiffres et lettres, il sera plus long a brute-

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

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

1.Les fichiers .pwl de Windows 9x/ME:
Les fichiers ayant l'extension .pwl contiennent vos mots de pass Windows, ils se situent dans le répertoire racine (c:\windows).
Biensur tous les fichiers .pwl sont cryptés, vous pouvez le voir si vous essayer d'en ouvrir un avec un éditeur de texte comme notepad par exemple. (Restez appuyer sur la touche MAJ et faites un click droit sur le fichier pour faire apparaître le menu "ouvrir avec").
Ces fichiers peuvent contenir les mots des pass de connexions, écran de veille, sessions...

Pour les décrypter, il faut utiliser un soft comme Pwltool (http://soft4you.com/vitas/pwltoo1.asp) qui va se charger de cracker le fichier et nous afficher les pass en clair.

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

Pour commencer une attaque il faut sélectionner le fichier .pwl en clickant sur le bouton "Browse", Ensuite essayez de clicker sur "Glide" (cette options ne fonctionne que pour les anciens fichiers PWL de windows 95 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 continue alors :)

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

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

L'attaque par Brute force :

Clickez sur l'onglet "Brute force"
Le paramètre "Password length" vous permet de définir la longueur du mot de pass à forcer (plus la plage est large, plus le nombre de combinaisons augmente).
"Charset string" vous indique les caractères a utiliser durant le brut force (vous pouvez y inclure des chiffres ainsi que les caractères spéciaux comme "@" par exemple). Pour lancer l'attaque clickez sur "SearchPasswordFast" (+ rapide que "SearchPassword" car il n'utilise pas les API windows), si l'attaque ne réussie pas clickez sur "SearchPassword".
TI m'a fallut environ 4 minutes pour venir a bout d'un password composé de 4 lettres...

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

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

Contourner le pas de Win 9x :
Lorsque que l'on démarre win9x si des pass on été configuré pour accéder a l'OS, il vous demande une identification par login et pass. Nous allons voir dans cette section les diverses techniques pour contourner cette identification....
-Essayez de clickez sur "Cancel", normalement vous devriez avoir accès au système.
-Au démarrage de votre ordinateur clickez sur "F8" pour faire apparaître le menu de démarrage (ou

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

2.Le fichier Sam de WINNT ou WIN2k:
Le système Windows a 2 failles de cryptage qui permettent de décrypter un fichier pass Windows plus vite qu'un fichier pass Unix par exemple.
L'une de ces failles provient du hachage de LANmanager car il divise les pass en chaînes de 7 caractères. L'autre vient de l'absence de salt (fonction rendant le hachage différent pour 2 pass identiques).En clair, si 2 utilisateurs choisissent le même pass, le cryptage sera exactement le même, ce qui facilite la tache du hackeur. Comme pour win9x, il existe des softs qui permettent de cracker les mots de pass des utilisateurs ou de l'admin. Sur les systèmes NT, les mots de pass sont sauvegardés dans un fichier SAM (Security Account Manager) crypté se trouvant dans c:\WINNT \system32\config\SAM .
Vous ne pouvez pas visualiser ou copier le fichier SAM lorsque WINNT tourne car il est verrouillé par le noyau du système.

I.Lorsque l'on installe WINNT, une copie de la base de données des mots de pass (fichier SAM) est crée dans le répertoire c:\WINN1\repair .
Cette copie ne contient que les pass par défaut crée lors de l'installation, donc seulement le pass de l'administrateur. (ce qui intéresse le plus le hackeur). Lorsque l'administrateur met à jour le disque de dépannage, le fichier SAM est lui aussi mis ajour (dans ce cas la, le fichier SAM contient tous les comptes). On pourrait donc se procurer le fichier SAM a partir du dossier repair car celui ci n'est pas verrouillé par le noyau. Si le dossier repair ne contient pas le fichier SAM, il vous reste quand même une chance de l'obtenir...
2.TI faut faire booter le PC a partir d'une disquette de démarrage ou a partir d'un autre système d'exploitation. Ainsi WINNT n'est pas exécuté et donc le fichier SAM n'est pas verrouillé. On peut donc copier le fichier SAM sur une disquette et le cracker par la suite.
TI 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 LC sur:
http://www.atstake.comlresearchllc3/download.html .

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

LC propose 4 méthodes :

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

Clickez 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 (clicker sur Browse pour lui indiquer le fichier password a utiliser)
La deuxième, c'est pour l'attaque hybride, vous pouvez config l'attaque hybride dans le menu "File"--> "Préférences" de la 'interface principale.
La dernière vous l'aurez deviné, c'est pour le brut force (le "-" permet de spécifier une plage de caractères, ici le brut force utilisera tous les caractères de l'alphabet ainsi que tous les nombres) si vous désirez changer de plage il vous suffit de c1icker sur la petite flèche a droite.

Clickez 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.

Clickez sur suivant et attendez le résultat ;)

Le fichier passwd d'Unix:
Unix utilise un systeme de cryptage unique.
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 facilitai la tache du crackeur.
En tapant: more /etc/passwd sur un système Unix on affiche le fichier passwd.

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 :

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 sours Windows (http://www.openwall.comljohn/)

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

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

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.

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, 5MB, etc...

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

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

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

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

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

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

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

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

2.Lorsque l'écran de veille est actif:

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

V - Les pass cachés avec des astérisques:

Imaginons vous vous connectez à intemet de fassons automatique (le pass n'est pas demandé a chaque démarrage d'intemet). 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.coml).

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 hackeur a trouver votre pass.
Changer assez souvent de pass comme ça le hacker n'aura sûrement pas le temps de cracker votre pass, vu qu'il changera a chaque fois.
Mettre un pass BIOS pour accéder au Setup, au système d'exploitation et changer la séquence de boot pour éviter de booter a partir d'une disquette.
Éviter de demander à Windows de sauvegarder vos pass (access intemet, 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.

Links:
- 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)

Accès 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.

1ere méthode : Vous connaissez tous l'explorateur windows ;) (Appuyez sur la touche windows de votre clavier + E)

2e méthode : Clikez sur "Parcourir..." et dans "Type :" choisissez "Tous les fichiers"
Il ne restera plus qu'a trouver le fichier a sauvegarder.
Cette méthode s'applique pour beaucoup de softs sous windows (ex: Notepad).

3e méthode : Faites un click droit sur votre fond d'écran et clickez 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.

4e méthode : Il est aussi possible d'accéder aux fichiers du disque dur a partir d'Internet Exploreur.
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 au ressources partagées.

5e méthode : Cette dernière méthode consiste à redémarrer l'ordinateur a partir d'une disquettede 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 clickez sur "Ajout/Suppression de Programmes", onglet "Disquette de démarrage", Insérez une disquette vierge dans votre lecteur et clickez 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 clickant 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 tesUxt 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>
<TITLE>Ma première page web</TITLE>
</HEAD>
<BODY>
</BODY>
</ITML>
```

Pour plus d'info sur le language HTML --> http://www.ac-grenoble.fr/gblhtmldoc.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 que vous pouvez trouver dans les vrai cours permettra l'écriture d'un fichier .bat sur votre disque.
Il est a inclure dans une page HTML entre les balises <BODY> et </BODY>.

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:

```
cd..
cd [repertoire]
choice
cls
copy [fichier] [dossier]
del [fichier]
dir
@echo off
echo.
echo [texte]
edit [fichier]
erase [chemin fichier]
format [lecteur]
goto
if
mem
mkdir [dossier]
pause
```

ren [fichier] .[nouvelle extension]
rename [fichier] [nouveau nom]
rmdir [dossier]
type [fichier texte]
ver
vol [lecteur]
c:\windows*. *
c:\windows* . [extension]

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 !?

Solution pour se protéger :
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, clickez sur "affichage"-->"source" dans lE.
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 c1ickant 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 conseille de mettre toujours l'option "demander" ou "désactiver".

Links:
- http://www.chez.comlscudo/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.comlregionifr/resources/scripthtml (les scripts malicieux)
- http://evolvae.free.fr/documentations/activex.htm (Quelques Scripts ActiveX)

Anonymat:
Mais...comment font ces hackeurs 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".

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 visiter.
Vous pouvez configurer lE pour qu'il passe automatiquement par un proxy à chaque connection. Pour cela clickez 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.
Clickez sur "Options", onglet "Proxy Server List". Dans cette fenêtre vous pouvez apercevoir les proxies qu'utilise Muliproxy. Un proxy précédé d'un cercle rouge, signifie qu'il ne fonctionne pas (vous pouvez le supprimer pour éviter de le tester a chaque démarrage).

Pour ajouter une nouvelle liste de proxy il suffit déjà d'une trouvée une. Allez faiœ un tour sur http://www.multiproxy.org/anon_listhtm .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" clickez sur "Menu" --> "Files" --> "Import proxy list".

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.

- 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/genlfl1087.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 clickez 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 1 080.
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 sockcaps quel soft il doit faire passé par le proxy Sock. Dans l'exemple j'ai pris ftp.exe se trouvant dans le répertoire c: \WINNT\system32\ftp.exe (pour Win2k). Cliquez sur "OK" pour refermer la fenêtre.

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

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

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