

ACCEDER À VOTRE WINDOWS XP EN VOUS TAPANT DU MOT DE PASSE

www.hackernewsmag.it

HACKER Magazine^{news}

**REPORTAGE
EXCLUSIF**

NOUS SOMMES ENTRES DANS LE BUNKER

La forteresse de 2 ex-hackers où
sont conservées les données les plus secrètes

• RESEAU SECRET : WASTE V.2.0

DEFENDEZ VOTRE LIBERTE INFORMATIQUE

LA POLICE VEUT VOUS PIEGER !

*Comment ils font
pour vous pister
dans le réseau
P2P!*

**INTERVIEW
KEVIN MITNICK
L'EX « SUPER » HACKER
PASSÉ DE L'AUTRE CÔTÉ
DU MIROIR**

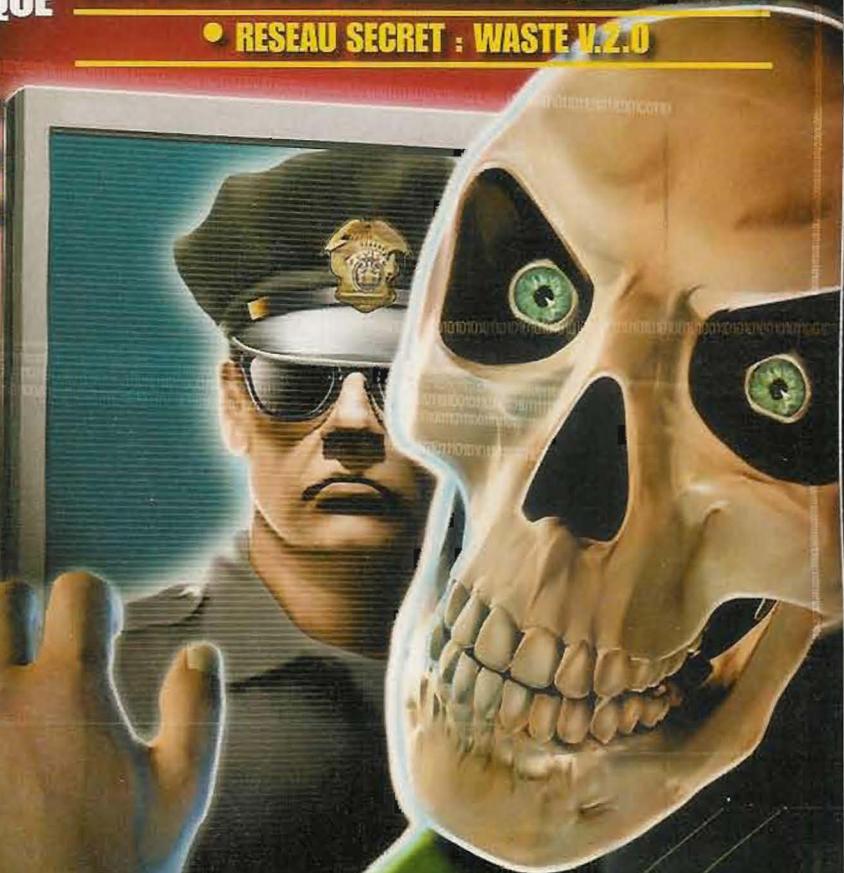
2€
0% de publicité
Juste des articles

M 02736 - 15 - F : 2,00 € - RD



NUMERO # 15 / DEC. 2006 - JAN. 2007
BEL/LUX : 2,40€ - SUISSE : 4 FS - DOM : 2,50 €
TOM - 490 XPF - MAROC : 25 MAD

Sprea
editions



MORTEL : L'EMPOISONNEMENT DU DNS

ASTUCE DE HACKER : TRANSFORMER UN VULGAIRE SPOT EN SPOT POLYCHROME

UN CHEF D'OEUVRE DE VIRUS : SASSER SÉVIT TOUJOURS !

Les camarades de la rédaction européenne :
Christian Antonini, Bismarck.it,
Gualtiero Tronconi, Edoardo Bracaglia,
One4Bus, Barg the Gnoil, Amedeu
Bruguès, Silvio De Pecher.
Contents by MDR.

Contact France:

Sprea Editions
Parc d'affaires SILIC
1 Place Gustave Eiffel
Po Box 10225
94 528 Rungis Cédex
international@sprea.com

Design:

Alessandra Calo

Assistant Art Director:

Davide "Fo" Colombo

DTP: Marco Colombo Giardinelli
Copertina: Daniele Festa

Publishing company:

Sprea Editori SpA
Via Torino, 51
20063, Cernusco S/N (MI) Italy

Printing:

Roto 2000,
Via Leonardo da Vinci 18/20
Casarile (MI) Italy

Distribution:

CCEI - 33 rue Henard
75012, Paris France

Direttore Responsabile:

Luca Sprea

Dépôt légal : à parution

ISSN : en cours

Sprea
Editions

Copyright Sprea Editori SpA

Tout le contenu est

Open Source sur le web.

Les droits sont réservés et protégés

Pour la version imprimée.

La rédaction n'est pas responsable des
textes, documents, photos, dessins qui
lui sont communiqués et n'engagent
que la responsabilité de leurs auteurs.

Sauf accord particulier et publiés ou
non, ils ne sont pas renvoyés.

Les indications de prix et d'adresses
sont de l'information fournie sans
aucun but publicitaire.

"Personne qui s'amuse à explorer les spécificités des systèmes de programmation et la façon d'étendre leurs capacités, contrairement à de nombreux utilisateurs qui préfèrent n'apprendre que le minimum nécessaire"

Editorial

HACKER
Magazine

Les véritables problèmes se terrent dans l'ombre...

Certains souhaitent nous distraire. Avec des histoires de conspirations, de complots. A travers des intrigues. On lit les choses les plus absurdes. N'importe quel sujet semble aujourd'hui faire l'affaire. Il y a eu le 11 septembre. Les tours jumelles ont été percutées par deux avions. Certains vont vous dire que c'est vrai. Mais en réalité, ils les ont démolies. Un complot. Une conspiration secrète. L'homme est allé sur la Lune. Mais pour certains, ce n'était qu'un canular monté de toute pièce. Tout un film tourné dans un studio souterrain. Top Secret. Au beau milieu du désert. Ceux qui savaient ont été enlevés. Non, ils ont été tués. Non, enlevés et tués. Plus vous faites marche arrière et plus il y a de complots. Au final, nous sommes tous d'accord. La Joconde a été peinte par Léonard. Mais pour certains, il suffit de la regarder pour comprendre que Léonard est gay. Non, que Léonard a peint son autoportrait. Non, que la Joconde sourit parce qu'elle est enceinte. Nous sommes tous à la recherche des vérités cachées. Et moi, je me suis vraiment cassé la tête. Car ce ne sont pas les vérités cachées que nous devons chercher. Ce sont celles évidentes ! Celles que nous avons sous nos yeux et que personne ne voit ! Ceux qui dénoncent les complots, parlent toujours de choses très lointaines. New York. Afrique profonde. Afghanistan. Chine. Moi, j'aimerais bien voir un complot à côté de chez moi. Vous écoutez et ils vous expliquent tout du 11 septembre. C'était la CIA. Noms et prénoms. Je leur demande : si vous êtes si préparés, dites-moi qui est réellement intercepté par les Telecom. Silence radio. Pour parler des complots à la Maison Blanche, ils sont tous prêts. Moi, j'aimerais savoir si mon téléphone est sur écoute. Mais je ne peux pas. Je me demande si quelqu'un est en train d'espionner mon trafic Internet. Quoi que je fasse, personne ne me le dira. Certaines équipes auraient-elles réellement arrangé des matchs ? Personne ne le sait. Si en revanche, vous souhaitez tout savoir du faux débarquement sur la Lune, il vous suffit d'un instant. Noms. Dates. Circonstances. Détails. Documents. Incroyable ! C'est un secret ultra-confidentiel et ils en sortent des livres à des millions d'exemplaires. Comme s'il ne s'agissait pas d'un secret. Sur les personnes interceptées, vous trouverez au mieux un petit article de journal. Etrange ! Je me serais plutôt attendu à des noms, dates, circonstances, détails et documents. Je n'ai en revanche que du vent ! Peut-être qu'en ce moment même, le Mossad est en train de conspirer sur Mars. Je parie qu'ils vont très prochainement nous écrire un livre sur le sujet. Peut-être qu'à un mètre de mon ADSL, quelqu'un m'espionne. Et personne ne veut me le dire. Les véritables complots sont ceux qui se terrent chez nous. Ceux qui restent vraiment secrets et qui sont les plus dangereux de tous. Car inventer une histoire sur des gens situés à 5 000 kilomètres n'est que pure plaisanterie. Comprendre pourquoi il y a quelqu'un qui vous suit dans la rue est impossible.

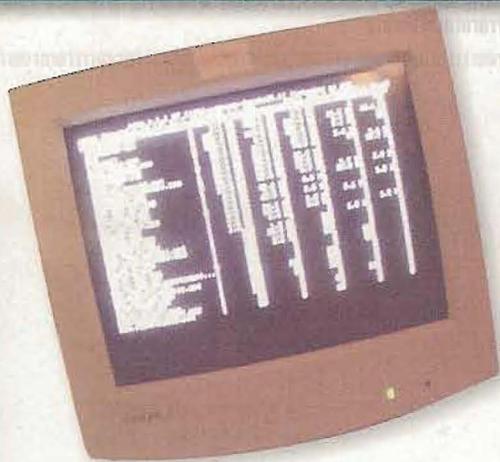
Monde hacker : apprenons ! Les complots les plus terribles sont ceux qui se terrent dans l'ombre. Plus ils sont proches et plus ils sont terribles...

theguilty@hackerjournal.it

Hacker News : votre magazine

Vous souhaitez apporter votre contribution, donner votre avis, faire partager votre démarche ou vos trouvailles : les colonnes de Hacker News magazine vous sont ouvertes sous réserve que vous sachiez convaincre la bande de pirates qui tient la rédaction. Celle-ci a domicilié son site quelque part en Italie, mais elle est européenne, on peut donc s'adresser à elle également en français.

redazione@hackerjournal.it



Tous aux ABRIS !

*Internet Explorer
ou Firefox ? Tout
dépend de la fail-
le que vous êtes
prêts à affronter !*

Il semblerait que l'on ait trouvé une faille de sécurité dans Firefox. Mais sur ce plan, Microsoft n'entend pas renoncer à sa position de leadership... et en définitive, cette pseudo faille n'était qu'une mauvaise plaisanterie ! Internet Explorer restant le navigateur «passoire» par excellence. Mais une fois sur mille, personne n'y échappe, et cette fois-ci, même Firefox semblait dans la ligne de mire. C'est sur l'estrade de la Convention hacker ToorCon, fin septembre, que Mischa Spiegelmock et Andrew Wbeelsoi ont déclaré qu'une page web contenant un code JavaScript suffisamment agressif était susceptible de pénétrer dans une faille de Firefox et prendre ainsi le contrôle de l'ordinateur par une attaque éclair de type 0-day. Mischa, qui dans la vie travaille chez SixApart, (une société qui édite des blogs) a expliqué en détail cette faille et même montré une fenêtre contenant les parties clés du code servant à attaquer le browser.

Une vulgaire plaisanterie !

Quelques jours plus tard, on pouvait lire sur le blog des développeurs de Mozilla que Mischa nous avait tout bonnement joué un mauvais tour ! «Nous voulions juste faire parler de nous... nous avons évoqué une faille dans Firefox mais le co-

de que nous avons présenté ne fonctionne pas. Nous n'avons pu faire exécuter aucun code dans Firefox, et je ne connais personne qui y soit arrivé». Vous trouverez le texte intégral de la déclaration de Mischa, qui a tout démenti en bloc, sur <http://snipurl.com/xwek>.

Firefox appelle, Microsoft répond

Entre-temps, deux jours avant la fausse révélation sur Firefox, Microsoft faisait savoir qu'une vulnérabilité de Microsoft Windows shell, la partie du système d'exploitation qui présente l'interface graphique pour les utilisateurs de Windows, disposait d'un élément qui ne fonctionnait pas correctement, nommé WebviewFoldericon. Un criminel pourrait très bien créer une page web exploitant cette faille et, comme d'habitude, utiliser Internet Explorer pour acquérir le contrôle de l'ordinateur. Tous les détails sont sur <http://snipurl.com/xln4>. Mais l'information la plus importante, c'est que Microsoft était au courant de cette faille depuis plusieurs mois déjà ; une faille qui a été mise au jour à partir du moment où certains ont présenté sur Internet un code permettant de lancer une attaque à proprement dit.

QUAND LES VERS GRANDISSENT

Les cybers-criminels découvrent JavaScript. En juin, le ver Yamanner a attaqué la poste électronique via le web de Yahoo, avec un message ayant pour objet New Graphic Site. Quelques mois auparavant, Samy envahissait MySpace.com en exploitant des failles spécifiques au site. Toujours à partir de JavaScript.

Nous devons nous débrouiller seuls

Le jour suivant les révélations de Microsoft, la société de sécurité Determina a proposé un patch indépendant pour y remédier. C'est déjà la seconde fois qu'apparaît une faille dans Windows et ce, en l'espace de quelques semaines seulement. En attendant que Microsoft daigne se réveiller, quelqu'un se doit de recoller les morceaux. Microsoft ne recommande pas l'utilisation d'autres patches, dans la mesure où ils pourraient compromettre les mises à jour futures et provoquer des problèmes. A l'heure où nous écrivons ces lignes, début octobre, Microsoft déclarait qu'elle allait proposer un patch officiel le 10. Entre-temps, 90% des ordinateurs du monde entier vont rester exposés pendant plus d'une semaine à une attaque que Secunia a qualifiée d'extrêmement critique. Sur Firefox, on peut en rire dans la mesure où le navigateur reste extrêmement sûr. Sur Explorer, hélas, le sérieux reste de mise et on a plus que ses yeux pour pleurer.

Nyarlathotep

Il Caos Strisciante

nyarlathotep@hackerjournal.it

QUAND EXPLORER EXPLOSE

Nous n'entrerons pas dans les détails, car cette information ne doit en aucun cas arriver aux mains de personnes mal intentionnées, mais.....

```
var a = new ActiveXObject('WebviewFoldericon.WebviewFoldericon.1');  
a.setSlice(0x7fffffff, 0, 0x41424344, 0);
```



LES BAFFLES DE LA CHAÎNE HI-FI POUR LE PC

Salut à tous !

Je souhaiterais modifier une petite chaîne Hi-fi que j'utilise pour des enregistrements à partir de cassettes audio, pour les convertir ensuite au format wav ou mp3. Etant donné que ma chaîne ne dispose pas d'entrée auxiliaire, je voulais savoir s'il était possible de brancher la sortie audio du PC à l'amplificateur de ma chaîne pour faire office de haut-parleurs pour mon PC. Cette modification me serait vraiment très utile. En posant la question à d'autres personnes, on m'a donné différentes réponses sur ce point... du style : «Tu ne peux pas, parce que la ligne de sortie de ton PC est déjà amplifiée et il n'est pas possible de réamplifier un signal déjà amplifié» ou encore : «oui, c'est possible, mais il est très difficile de trouver les branchements du positif et du négatif sur l'amplificateur, étant donné que l'amplificateur est en mono tandis que le signal PC est en stéréo...»

Félix

Difficile de te répondre avec exactitude sans savoir précisément de quel modèle il s'agit. Quoi qu'il en soit, c'est une opération totalement réalisable. Trouve l'amplificateur intégré de ta chaîne Hi-fi (il est généralement situé à proximité des fils des haut-parleurs). Après quoi, tape la référence du circuit intégré sur Google, cherche le datasheet et regarde quelle est la broche d'entrée du signal. Tu peux également essayer en touchant les pin à l'aide d'un tournevis et voir lesquels font le plus de bruit dans les haut-parleurs....ces pin sont donc ceux auxquels il faudra relier les sorties (droite et gauche) de la carte audio. La masse va avec la masse. Il se peut que le signal soit trop puissant, c'est pourquoi il est conseillé d'installer en série une résistance ou un double potentiomètre entre signal et masse. Un condensateur chimique d'environ 10 microF installé sur chaque entrée pourrait aussi s'avérer utile pour éviter des composantes continues, sauf en cas de distorsions. Il faut donc tout essayer !

Open source et tu es des nôtres.

Salut à tous, je tenais tout d'abord à vous féliciter pour votre magazine et la qualité des sujets traités.

Je voulais vous faire part de mon site perso, né un peu par jeu et un peu par ennui, en pleine période d'accalmie, et surtout au lit, avec la varicelle !

Ce site a été créé dans l'idée d'en faire un site promotionnel. Mais après quelques jours de développement, j'ai abandonné cette idée, en élargissant en revanche les thématiques qui me tenaient le plus à cœur. Ceux qui l'ont vu l'ont trouvé intéressant,

surtout ceux qui ne sont pas forcément experts en informatique. Je profite donc du message qui apparaît fréquemment dans vos pages, et qui invite les lecteurs à donner l'adresse de leur site.

A très bientôt !

Fulvio Mhu

Un bon travail, simple mais original. Surtout avec la varicelle ;-)

NORTON, PAS TRÈS INTELLIGENTE

Je m'appelle Alexkingdom, j'ai 15 ans et je lis votre journal depuis un an environ. Un de mes amis, lui aussi passionné d'informatique, a un problème avec Norton qui reste désespérément bloqué. En effet, depuis quelques temps, n'étant pas administrateur et disposant du contrôle parental, il lui est impossible d'aller sur votre site. Un message indique en effet qu'il appartient à une catégorie indésirable. Pouvez-vous nous dire comment faire pour tromper Norton ?
Alexkingdom

C'est un problème connu depuis longtemps. Il n'existe aucun moyen de tromper Norton sans désactiver le contrôle parental. Tu as deux solutions : discuter avec tes parents et leur expliquer qu'Internet est beaucoup plus sûr quand on surfe ensemble ; deuxièmement, contacter Symantec et leur expliquer leur erreur. Le site de Symantec est un véritable labyrinthe mais vous devriez trouver le bon

formulaire sur <http://snipurl.com/xhzs>. Dans le cas contraire, vous pouvez toujours contacter Symantec de 9h00 à 17h00 les jours ouvrables, au 02 48 27 00 00. Si vous optez pour cette solution, vous devrez d'abord expliquer à Symantec que vous n'êtes pas le grand méchant loup, et dire ensuite à vos parents qu'Internet est avant tout une grande opportunité, et non pas un danger.

PSP downgrade

Salut à vous, pirates de l'informatique ! Je voudrais juste savoir si ma PSP avec une mise à jour 2.5 pouvait faire l'objet d'un downgrade vers la version 1.5 sans courir de risques.

Merci !

Sammano123

Sans courir de risque, non !

Non sans risques (la fin de ta PSP), tu peux toujours tenter de suivre ce tutoriel pour le moins intéressant : [http://](http://www.psp-ita.com/forum/forum/viewtopic.php?t=30664)

www.psp-ita.com/forum/forum/viewtopic.php?t=30664.

Attention, nous nous dégageons de toute responsabilité quant à son fonctionnement effectif !

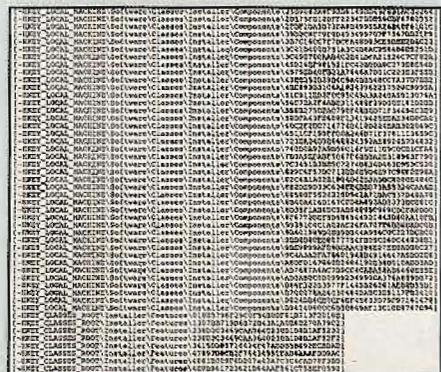
Quant aux pirates... si le drapeau est bel et bien le même, ce terme doit être perçu dans le sens d'une alternative aux solutions dominantes, non pas dans le sens de l'illégalité ! Celle-là, nous la laissons aux lammers et crackers. Nous, nous nous occupons uniquement d'étudier et d'apprendre, en cherchant la vérité.

QUAND NORTON S'EN MÊLE...

Au secours ! Je n'arrive plus à recevoir mes e-mails et Skype ne fonctionne plus, même si j'arrive toujours à naviguer sur le net. Bref, tout fonctionne comme si j'avais toujours eu un firewall... que je n'ai pourtant jamais installé ! J'ai tout essayé. J'ai désactivé le firewall de XP, désactivé l'antivirus, bref, j'ai tout désactivé, mais rien à faire ! Auriez-vous une solution, avant d'en arriver au formatage ? Ce qui me semble étrange, c'est que les icônes d'une ancienne version de Norton, installé à l'époque, sont toujours présentes alors que je l'avais déjà désinstallé il y a belle lurette. Help me !

David

Symantec a encore frappé. L'une des plus grandes sociétés de software au monde n'a toujours pas résolu le problème d'une désinstallation «propre» de ses produits, si ce n'est à travers une procédure exigeant les connaissances d'un... hacker, et écrite dans les profonds méandres de son site officiel (avec une adresse qu'on ne pourrait même pas porter ici, tant elle est longue). Inutile de désinstaller normalement les produits Symantec : il restera toujours des fichiers éparpillés ici et là et des registres corrompus qui ont pour effet d'empêcher le bon fonctionnement des communications IP de votre PC ! La seule solution, c'est d'utiliser ce lien <http://snipurl.com/wejw>. Vous verrez que tout rentrera dans l'ordre (sauf pour les icônes, qui restent malgré tout faciles à supprimer, tandis qu'elles n'ont aucune influence sur le bon fonctionnement des programmes...).



▲ Ce n'est qu'une partie des registres système qui doivent être... réorganisés

Mais que se passe-t-il donc en Allemagne ?

Salut à tous !

J'ai lu, non sans une certaine angoisse, les informations sur les serveurs Tor crackés en Allemagne. Mais le plus grave, c'est surtout qu'avec ces actes stupides, l'Union européenne va serrer la vis en matière de lutte contre les crackers, les pirates mais aussi les simples hackers. Est-ce vrai ?

K4pt41n

Vois-tu, cher Capitaine, le fait est que si l'on s'en tient à une série de règles simples et normales, alors il n'y a rien à craindre : nous souhaitons tous changer le système, mais les changements les plus efficaces sont ceux réalisés dans la légalité, à savoir ceux effectués de l'intérieur, en conformité avec les lois en vigueur. Tenter de changer les choses de l'extérieur, par la force, nous le savons tous, n'est en aucun cas la marche à suivre. Si quelqu'un veut faire du hacking sans commettre le moindre délit, il n'a alors absolument rien à craindre. Même s'il est Allemand ! Car même si en Europe les choses sont en train de devenir de plus en plus restrictives, en Allemagne la situation est autrement plus sérieuse. Le problème, c'est qu'on a trouvé de véritables vides juridiques au niveau des lois allemandes, et certaines situations n'étaient donc pas prévues. Le gouvernement allemand souhaite changer les choses, en introduisant de nouveaux articles et normes. Parmi les informations qui ont filtré, nous pouvons te dire que ces nouvelles lois prendront en compte les délits d'accès non autorisé, jusqu'à différentes violations portant préjudice aux utilisateurs individuels privés. Jusqu'à présent, en Allemagne, seuls sont considérés comme des délits, les attaques informatiques lancées contre des organismes publics ou des entreprises.

DES HACKS INTERESSANTS ?

Nous attendons d'autres contributions des lecteurs. Vous avez envie de vous familiariser avec le vrai hacking ? Vous avez réalisé des expériences intéressantes ? Vous êtes capables de décrire certaines techniques que vous

avez adoptées en tant que vrai hacker ? Écrivez à one4bus@kackerjournal.it. Nous évaluerons l'ensemble des travaux en vue d'une éventuelle publication sur les prochains Hacker News.

Des fusées à 40 mètres.

Salut à toute la rédaction ! Du haut de mes 48 ans (!) je me permets de suggérer l'utilisation du bouchon que je montre sur la photo, et que j'ai utilisé par le passé. C'est une fixation rapide pour compresseurs, que je conseille d'utiliser pour une pression autour de 12 atm. En remplissant les bouteilles de 1,5 l à moitié, on atteint des hauteurs considérables (autour de 40 m). Ces bouteilles ne représentent pas un gros danger en retombant, et même sans aileron, l'eau qui est au fond leur donne toujours une direction verticale.

Si vous voulez vous faire mal, ne les remplissez pas d'eau... mais surtout, restez bien éloignés et bouchez-vous les oreilles... il faut le voir pour le croire !!!

Le filetage du bouchon de la bouteille devient le point faible du système et donc ce-

lui qui cède en premier...

Bon courage à tous !

Marc

Réponse de Standard Bus :

Merci pour tes précieux conseils, Marc ! Ne t'inquiète pas, il n'y a pas que des «petits jeunes» qui lisent HNM... De notre côté, nous en connaissons pas mal qui s'amuse encore à lancer des fusées !



◀ Notre lecteur se réfère à l'article sur le hardware estival publié dans notre numéro 106 !



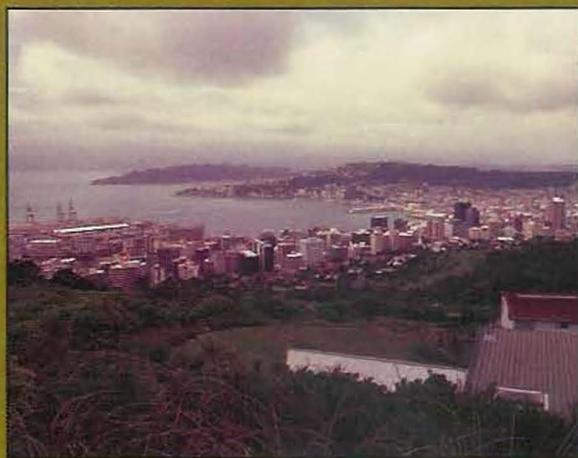
QUI A GAGNÉ ?

On affirme que le vote électronique constitue l'avenir des élections politiques au mépris de toute garantie et de toute sécurité. Mais lorsqu'on met ce système à l'épreuve, il y a de quoi s'inquiéter ! Sur YouTube (<http://hardclicker.com/PyC6ow>), on peut en effet visionner un film inquiétant : un technicien de l'Université de Princeton aux USA, tente de saboter un petit appareil destiné au vote électronique, et il y parvient en moins de dix minutes sans que personne ne s'en aperçoive ! Le résultat des urnes donne gagnant un candidat qui, en réalité, a obtenu moins de votes que son adversaire. La machine à voter se nomme Diebold AccuVote-TS. Souvenez-vous en lorsqu'elle arrivera également chez nous. Du moins, si elle arrive...

TOUS EN

NOUVELLE-ZELANDE !

Tandis que partout dans le monde, l'étau se resserre sur les hackers, la Nouvelle-Zélande pourrait bien être la nouvelle Terre promise. Voyez plutôt par vous-même : un chercheur de 39 ans, Gerasimos Macridis, a réussi à s'introduire dans le système téléphonique de la Reserve Bank, en découvrant des failles dans son système de sécurité. Il a ensuite contacté la banque en essayant de se faire payer ses services, non requis. La banque l'a dénoncé et Macridis, malgré ses antécédents en matière de fraude, s'est uniquement déclaré coupable d'avoir infiltré les ordinateurs de la banque. Etant donné que Macridis file droit depuis longtemps et qu'il n'a pas utilisé ces informations pour nuire à la banque, mais plutôt pour l'aider, le juge du tribunal de Wellington a levé toutes les accusations qui pesaient sur lui. Vous pourrez lire cette news pour le moins étrange mais véridique, sur les pages du New Zealand Herald, en cliquant sur : <http://hardclicker.com/xSfHzY>.



▲ Légende : Wellington, la nouvelle terre promise ?



MICROSOFT TENTE DE CACHER SES SECRETS

On ne devrait même pas le savoir, puisque le site de Redmond n'ébruie quasiment aucune information. Mais cette fois, c'est au tour de McAfee, Symantec et d'autres fabricants d'antivirus de s'inquiéter. Il semble en effet que Microsoft leur ait refusé l'accès à Windows Vista, qui sortira Dieu seul sait quand. Comment vont-elles bien pouvoir faire pour prévoir des antivirus adaptés ? Cela reste un mystère...

et c'est même plutôt inquiétant, à tel point que McAfee a acheté une page publicitaire sur le Financial Times pour dénoncer cette situation sans précédents, même si elle ne s'est pas encore officiellement retournée contre Microsoft à cet égard.



LA BRITISH LIBRARY EN GUERRE CONTRE LA GDN

Voici un allié inespéré et inattendu pour tous ceux qui se battent contre la GDN et que vous pourrez trouver au sein d'un établissement aussi influent qu'ancien : la British Library ! C'est en la personne de Lynne Brindley, chief executive de l'institution britannique, que l'éminente BL a décidé d'adopter une position vraiment intéressante et qui ne peut que nous réjouir. Dans un document que vous pouvez consulter à



HOT NEWS

A L'UNIVERSITE AVEC GOOGLE

Désormais, Google propose vraiment de tout : il ne lui manquait plus que les cours universitaires, mais le géant de Mountain View a comblé ses lacunes. En vous connectant au site : <http://video.google.com/ucberkeley>, vous pourrez en effet suivre des séminaires et colloques de l'University of California de Berkeley. Vous trouverez plus de 250 heures de cours mises à votre disposition gratuitement.



EN GUERRE CONTRE FAIRUSE 4WM

Microsoft part en guerre contre l'auteur (ou les auteurs) de FairUse4WM, un logiciel qui permet de retirer les protections Windows Media DRM, utilisées par plusieurs distributeurs de musique online (il suffit de citer Napster et Yahoo! Music). Il y a quelque temps, la société de Redmond que nous connaissons bien, avait menacé les sites autorisant le téléchargement de FairUse4WM, mais cette menace s'est avérée beaucoup plus lourde de conséquence qu'il n'y paraissait à première vue, puisqu'il s'agit d'une véritable plainte. En effet ! Ils sont en train de saisir la justice et ce, non sans une certaine virulence ! Les experts de Microsoft soutiennent que le cracker travaille justement dans leur entreprise, mais un démenti de Viodentia est déjà arrivé (surnom derrière lequel se cache l'auteur du logiciel).

VOUS VOULEZ

25 000

DOLLARS ?

Voici la valeur du premier prix du concours lancé par New Numa (www.newnuma.com). Pour avoir une chance de remporter ce concours, créez-vous un compte sur YouTube (www.youtube.com) puis réalisez une vidéo qui utilise la chanson "New Numa", que vous pouvez écouter et télécharger sur le site. Votre vidéo doit durer au moins une minute et pas plus de 9'59". Vous pouvez y mettre ce que vous souhaitez (dessins animés, personnes en chair et en os...), mais pas de scène ou langage vulgaire ou pornographique. Vous retrouverez le règlement complet sur le site susmentionné. Bien sûr, il n'y a pas que le premier prix : le second s'élève à 10 000 dollars et le troisième à 5 000 dollars. 125 dollars sont ensuite offerts aux candidats classés entre la 4ème et 50ème place. Vous avez jusqu'au 23 mars pour déposer votre vidéo, mais dépêchez-vous ! A l'heure où nous écrivons, il y a déjà 400 vidéos sur le site !



DES PROBLEMES DE PORTABLES QUI N'EN FINISSENT PLUS

Les propriétaires d'ordinateurs portables se sont vus demander de restituer à la maison mère les batteries fabriquées par Sony, soit quelque 526 000 pièces.

Un chiffre impressionnant, sans aucun doute ! IBM et Lenovo sont les dernières marques qui viennent s'ajouter au groupe d'entreprises touchées par le pro-

blème. Elles tentent d'ailleurs ces jours-ci de préserver les utilisateurs de ThingPad de problèmes explosifs. Nous sommes vraiment face à une situation d'urgence !



l'adresse suivante : <http://www.bl.uk/news/pdf/ipmanifesto.pdf>, la British Library soutient que la GDN viole les lois sur le droit d'auteur, surtout dans la mesure où elle ne prévoit pas d'échéance en matière de protection, et puis parce qu'elle entrave des droits jusqu'à présent reconnus, tels que la copie pour un usage personnel dans le cadre d'études, ou le droit de faire des copies en vue de conserver le contenu des documents. Le fait même que la British Library prenne position de façon aussi explicite ne pourra que peser dans le débat en cours sur la Gestion Numérique des Droits.

LA GUERRE SUR LES BREVETS

Octobre est un mois crucial pour l'avenir des brevets en matière de software en Europe. Le Parlement européen devrait en effet examiner une proposition de loi appelée "European Patent Litigation Agreement", qui devrait permettre aux grandes sociétés informatiques de contourner la réglementation actuelle, qui est en revanche plus favorable aux petits développeurs et aux auteurs de software open source. Breveter un software (ou une idée, même si elle est déjà diffusée et dont il est difficile d'établir la paternité) a en effet un coût qui ne représente rien pour les géants de l'informatique contrairement aux petites entreprises dont les moyens sont beaucoup plus limités. C'est donc avec attention que nous suivons l'évolution de cette histoire, car de son issue pourrait dépendre une bonne partie de l'avenir du software libre.

La parole au



Les déclarations de Kevin Mitnick sur son passage au monde des affaires après une célèbre carrière de hacker "hors-la-loi"

Pour beaucoup, il suffit d'évoquer le nom de Kevin Mitnick pour penser à ces hackers perspicaces et rusés, capables de narguer les agents du FBI et ce, des mois durant. Mais, Kevin s'est ensuite fait épingle et a passé plusieurs mois en prison sans même pouvoir toucher un téléphone (alors imaginez un ordinateur). Puis, il est retourné à la vie civile en tant que consultant en sécurité informatique pour de grandes sociétés. Mais peut-on toujours parler de hacker lorsqu'on se fait de l'argent à la pelle ? L'idée que nous nous faisons des hackers est-elle juste ou devons-nous revoir certains aspects ? Lisez plutôt l'avis de Kevin.

Hacker News Magazine : D'où vous vient cette renommée ? Et quelle est la

part de faux dans tout ce qui a été raconté ?

Kevin Mitnick : Je n'ai pas déjoué les systèmes informatiques du FBI ni commis d'autres infractions qui semblent tout droit sorties d'un film style War Games. Ce sont ni plus ni moins des inventions qu'on a reliées à des événements qui eux, ont effectivement eu lieu, comme la subtilisation d'un code source chez Motorola et Nokia en vue de son étude. Je crois que toutes ces rumeurs ont joué en ma défaveur quant à la peine qui m'a été infligée. Certains avaient peur que je puisse commettre des exactions du style lancer des missiles nucléaires en sifflant dans un téléphone public ; je ne pouvais pas m'en sortir car j'étais défendu par un avocat avec, à ma disposition, un budget très limité. Mais je n'ai pas été accusé de tout ce que l'on a écrit sur moi. Si j'avais cracké le NO-RAD ou m'étais infiltré dans les fichiers du FBI, on me l'aurait sûrement fait savoir. Si j'ai eu des problèmes, c'est pour les choses que j'ai faites, et non pas pour celles que je n'ai pas faites. Dans tous les cas, ce sont les journaux qui m'ont traité comme si j'avais été Oussama ben Mitnick !

HNM : Vous étiez le hacker le plus recherché des Etats-Unis et après être sorti de prison, vous vous êtes exprimé devant le Sénat et avez fondé une société de sécurité informatique. C'est plutôt pas mal comme évolution !

KM : Le piratage peut être utilisé à des fins légales ou criminelles, et c'est pour cette raison que je piratais à l'époque par curiosité et par goût du frisson, tandis qu'aujourd'hui je peux le faire pour renforcer la sécurité informatique : les

gens me chargent de trouver des failles dans leurs systèmes de façon à pouvoir les réparer avant que certains pirates informatiques ne les exploitent. En tant que hacker, je peux en revanche commettre des infractions de façon à aider la communauté.



▲ Le voici, notre Mitnick ! Portrait d'il y a quelques années lors d'une visite à Milan

mitnicksecurity
Home company products services investigations presentations workshops resources press speaking requests contact

Mitnick Security Consulting, LLC

January 2007 - Public Service of Investigation
"Computer Forensics" - TechCrunch

September 7, 2006 - Red Herring
Kevin Mitnick on WPA Hack Attack

October 2006 - "Relighting Risk in Usability"
"Computer Forensics" - TechCrunch

March 6, 2006 - Cnet.com
Kevin Mitnick: The Art of Deception

February 24, 2006 - The Jerusalem Post
Legendary Hacker Mitnick Turns Legit

January 26, 2006 - The Register
The Art of Deception

January 4, 2006 - InformationWeek
Mitnick Reveals

October 13, 2005 - CNN International
A Computer Hacker Debunks Osama Bin Laden

April 16, 2005 - InformationWeek
Kevin Mitnick to Receive Distinguished Achievement Award

Special Agents
Agents of the FBI, the military, and others.

Check Out Kevin's New Book
The Art of Deception: Controlling the Human Element of Security

▲ Le site de la société Mitnick Security : <http://www.kevinmitnick.com>

HNM : Votre retour au monde online et, aujourd'hui, vos activités, agacent-ils certains ? Certaines personnes ont-elles peur que vous puissiez les atteindre ?

KM : Il y a beaucoup de gens dans le secteur de la sécurité qui ne me font pas confiance, mais c'est plus une question de concurrence qu'autre chose. Je n'ai reçu aucun appel de gens me disant : je suis désolé, mais on ne peut rien pour vous car vu votre passé.... J'imagine qu'il y a des gens qui ne tiennent pas à me connaître du fait de mon passé de hacker et de mon séjour en prison. Je ne sais pas s'ils

sont nombreux. J'espère que non.

HNM : Par rapport à l'époque où vous étiez un hacker hors-la-loi, les choses ont-elles changé ? Est-il toujours aussi facile de s'infiltrer dans un ordinateur ? La sécurité s'est-elle améliorée ? Pourriez-vous encore faire ce que vous faisiez il y a encore quelques années ?

KM : Parfois, entrer dans un ordinateur est aujourd'hui plus facile qu'avant. En réalité, tout dépend du type de client ou, si l'on s'adonne au piratage éthique, du type de cible. Je dois également dire que la technologie a beaucoup changé et que les problèmes techniques en matière de sécurité sont différents, mais l'ingénierie sociale est restée la même. Cela dépend des propriétaires et des opérateurs informatiques et opérateurs réseaux, et de leur niveau de vigilance. Mais c'est aussi un peu le reflet de la vie, pas vrai ?

HNM : Et monsieur tout le monde ? Est-il vulnérable ? Jusqu'à quel point ? Certes, cela dépend des protections adoptées, mais supposons qu'elles soient les plus efficaces du moment, qu'en est-il ?

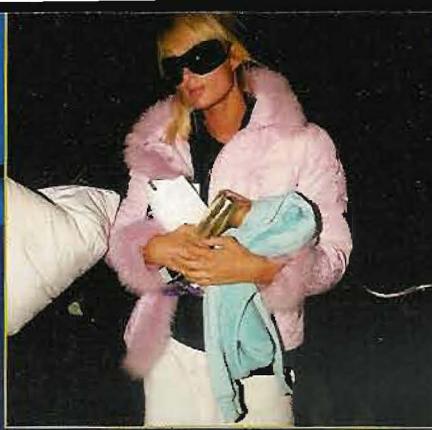
KM : J'ai mené une étude dans laquelle nous avons installé un réseau honeypot, spécifiquement conçu pour attirer des attaques, composé de six sous-réseaux différents constitués d'ordinateurs tournant sur des systèmes d'exploitation différents. Puis, nous avons attendu pour connaître leur durée de survie avant d'être infiltrés. L'un des ordinateurs a flanché après seulement quatre minutes ! C'était surprenant !

HNM : Vous avez parlé avant d'ingénierie sociale. Quel sens donnez-vous exactement à ce terme ?

KM : L'ingénierie sociale c'est utiliser la manipulation, l'influence et la ruse pour arriver à satisfaire l'une de nos exigences : comme par exemple entrer illégalement dans un cinéma ou acquérir des informations confidentielles d'une entreprise, ou infiltrer un ordinateur ou encore un réseau. Ce n'est pas toujours bien d'utiliser l'ingénierie sociale. On doit avoir une bonne raison pour ça. Il faut être vraiment cinglé pour molester les gens rien que pour s'amuser.

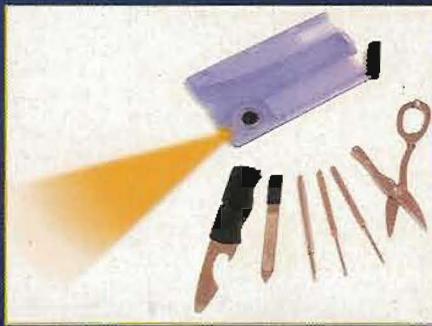
HNM : Comment les hackers d'aujourd'hui utilisent-ils l'ingénierie sociale ?

KM : Souvenez-vous de Paris Hilton. Elle a été attaquée sur son propre portable. Quelqu'un s'est rendu sur le site de son opérateur téléphonique et a réussi



▲ Même Paris Hilton n'a pas échappé aux attaques d'ingénierie sociale !

à réinitialiser son mot de passe. Paris a reçu un SMS pour lui annoncer son nouveau mot de passe. Le type est parvenu à faire un ID spoofing (feindre d'être quelqu'un ou autre chose) et à l'appeler en se faisant passer pour un technicien de son opérateur téléphonique. Alô ! Excusez-moi, j'appartiens à T-Mobile, auriez-vous reçu par hasard un SMS de changement de mot de passe, pourriez-vous me lire son contenu ? Paris est tombée dans le panneau, le gars a pris le mot de passe et a pu lire tout le contenu de son site, son courrier électronique, ses adresses et sûrement bien d'autres choses encore. Ça c'est une leçon ! Vous dépensez des millions en sécurité mais, si votre entourage n'est pas fiable, vous êtes en danger.



▲ Nombreux sont les outils qui permettent d'intervenir sur une carte pour l'"ouvrir" !

HNM : Faites-vous confiance au système bancaire online et aux cartes de crédit online ?

KM : Oui, parce que s'il arrive quelque chose, au final c'est la banque qui est perdante, pas moi. Ils ont tout intérêt à disposer d'un maximum de sécurité.

HNM : Vous n'avez jamais été piraté ?

Mitnick : Bon sang, bien sûr que si ! Dommage qu'ils ne m'aient pas volé mon identité lorsque j'étais recherché par la police. En effet, ils m'ont récemment volé mon identité pour demander un contrat de téléphone en utilisant mon

DE NOKIA A SHIMOMURA

La chasse à l'homme «Kevin Mitnick» a commencé en 1992, lorsque Kevin est devenu hors-la-loi. Il a été accusé d'avoir violé le système Voice Mail de Pacific Bell et, sous le surnom de Condor, d'avoir soustrait des informations confidentielles à Motorola, Nokia, Fujitsu, Novell, NEC, Sun et d'autres sociétés. Il aurait causé des préjudices à hauteur de 80 millions de dollars. Kevin a été arrêté en 1995 par une équipe dirigée par Tsutomu Shimomura, expert en sécurité, qui lui avait lancé un défi. L'erreur de Kevin fut d'accepter ce défi et d'entrer dans l'ordinateur de Shimomura, qui lui avait tendu un piège. Après cinq ans de prison et une période de liberté provisoire pendant laquelle il lui était interdit d'approcher un ordinateur et un téléphone, il est aujourd'hui un consultant confirmé pour la sécurité des systèmes d'exploitation.

nom. Mais je n'ai pas peur d'utiliser ma carte de crédit online. Les attaques existent, mais il est improbable qu'elles soient dirigées contre un individu. Plutôt contre la banque. Il est plus sûr d'utiliser sa carte sur Internet que dans une pizzeria où le fils du propriétaire est peut-être un voyou qui lui ouvre son tiroir caisse contenant les reçus de paiement.

HNM : Et maintenant, après tout ce qui s'est passé, après tout ce qui se dit sur vous dans les forums, à la télévision et dans les revues spécialisées... comment vous sentez-vous face à votre célébrité ?

KM : Mal lorsqu'elle a servi à aggraver mon cas face à la justice. Bien lorsqu'elle m'aide dans ma profession. Non pas en vertu de ce que j'ai fait dans le passé, mais dans la mesure où elle favorise la connaissance de mes capacités.

HNM : La vie du Hacker fugitif vous manque-t-elle ?

KM : Non. Ce que j'ai fait, c'est du passé, je suis satisfait de ma vie actuelle. J'ai commis certaines erreurs, même graves, et je suis heureux qu'on m'ait accordé une seconde chance et de pouvoir être utile à d'autres personnes.

David Nool
davenool@gmail.com

SÉSAME, ouvre-toi !

*Vous avez perdu votre mot de passe ?
Pas de panique ! Voici comment accéder
à un PC fonctionnant sous Windows XP,
sans même connaître son mot de passe...
très utile quand on n'a plus de tête !*

Tout le monde a forcément vécu cette situation un jour ou l'autre : vous vous retrouvez devant votre PC sans pouvoir y accéder. Pourquoi ? Tout simplement parce que vous ne connaissez pas le mot de passe... ou, pour être plus précis, vous l'avez oublié !

A lors comment faire pour contourner un tel problème ? Il vous suffit d'effectuer une simple opération. Le fait est que les mots de passe de Windows XP (mais aussi de Windows 2000 et NT) sont archivés sous forme de hash dans un Security Account Manager, où les mots de passe sont stockés sous forme cryptée à 128 Bit. Lorsqu'on tape un mot de passe, le système le crypte et compare le résultat avec la forme mémorisée. Si les deux coïncident, le système vous autorise l'accès. Sinon, il existe une seconde possibilité !

Commençons par le début

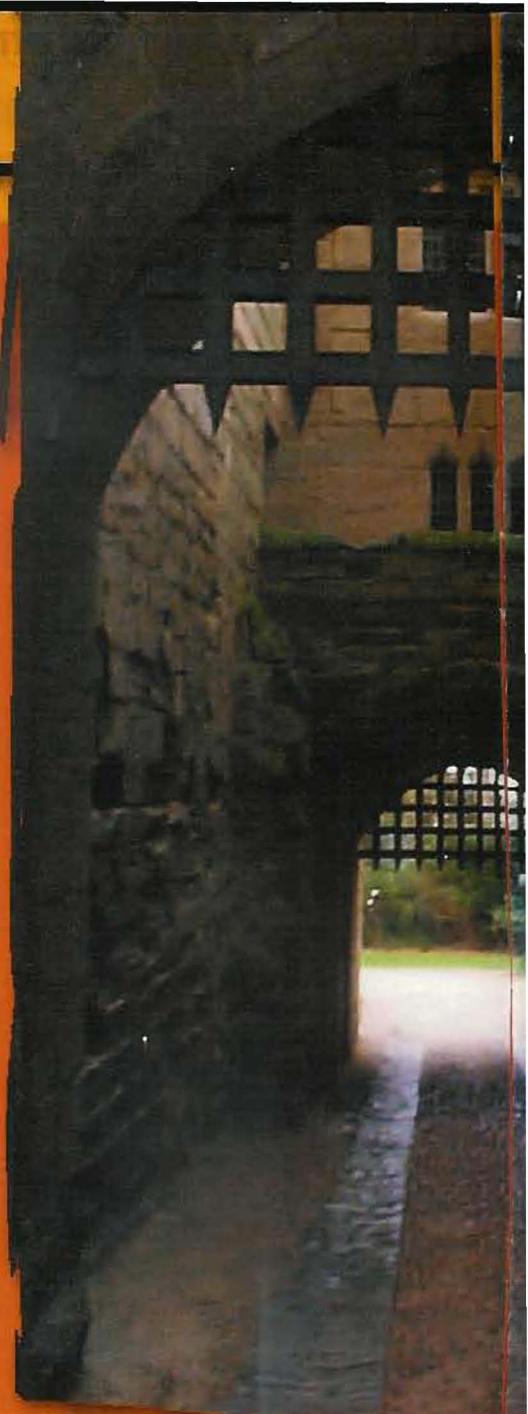
Nous devrions commencer par nous de-

mander comment un mot de passe système est-il archivé : aucun système

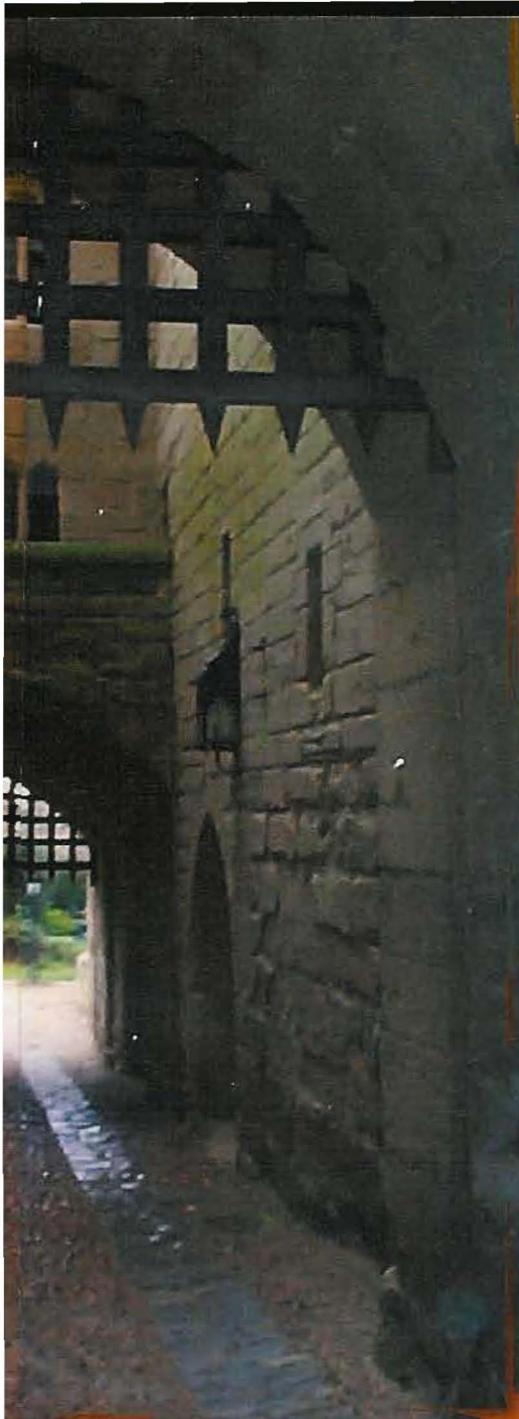


▲ Le SAM est utilisé par de nombreuses applications. En voici la liste.

moderne ne se limite à le conserver tel quel, non codé ! Sous NT, le mot de passe est généralement présent sous forme de hash, irrémédiablement modifié en suite de caractères codée, selon un critère bien précis. D'un point de vue cryptographique, changer et transformer de façon réversible signifie qu'une suite ABC, par exemple, se transforme en CBA après cryptage. En choisissant un codage irréversible, il est impossible d'obtenir le mot de passe à partir de sa forme cryptée, dans la mesure où le changement n'est pas biunivoque.



▲ La pile de sauvegarde du Bios est facilement reconnaissable et vous pouvez la retirer en toute sécurité.



Security Options

Password | Notify | Proxy Access | Send Options

Old password:

New password:

Confirm new password:

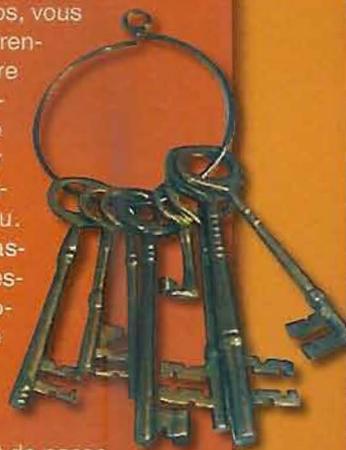
Clear Password

▲ *Combien de fois oublie-t-on son mot de passe ? On ne les compte plus !*

:: Quand RIP nous vient en aide

Les micro-distributions Gnu pour Linux...peuvent s'avérer très utiles pour faire face à la «perte» d'un mot de passe. Des micro-distributions qui nous permettent de sauver notre système face à certains événements catastrophiques comme, justement, la perte d'un mot de passe. Cette possibilité offerte par le RIP est également intéressante dans la mesure où elle ne nécessite aucune expertise spécifique sur Linux ! RIP inclut de nombreux programmes de sauvegarde et vous permet de conserver vos fichiers présents sur un disque défectueux ou de lancer un boot sur un disque sécurisé de façon

à pouvoir exécuter différentes opérations système. La fonction CMOSPWD (CMOS Password) retrouve quant à elle la très grande majorité des mots de passe Bios existants. Après avoir rebooté à partir d'une disquette, vous ferez apparaître votre mot de passe en tapant la commande Cmospwd. Après avoir obtenu l'accès au Bios, vous pourrez modifier différents paramètres de votre PC. Vous pouvez copier comme backup le Bios ou remplacer l'ancien mot de passe par un nouveau. Mais si le mot de passe Bios est celui nécessaire pour allumer votre PC, cette astuce ne marchera pas ! Dans ce cas, vous pourrez malgré tout le supprimer ! Le mot de passe est automatiquement réinitialisé en retirant la pile de sauvegarde du Bios de la carte mère ! Simple et rapide. Vous la reconnaîtrez dans la mesure où c'est la seule pile bouton de tout l'ordinateur. En redémarrant votre PC sans pile, le Bios conditionnera le système pour qu'il s'allume sans paramètre de mot de passe. En remettant la pile et en redémarrant, vous accéderez au Bios, mais sans protection. Le mot de passe du Bios est important car il vous permet de changer les options de boot et de démarrer à partir d'une disquette.



:: Question de hash

Votre PC pourrait toutefois valider le mot de passe même s'il ne connaît que sa forme codée.

C'est le cas, suite à une comparaison des hashes, dès que le mot de passe entré pour accéder à Windows a lui aussi été modifié dans un hash spécifique.

Les hashes bénéficient d'une fonction de codage MD4. Cette fonction de codage modifie les suites de caractères en un mot de longueur fixe égal à 128 bit (128 divisé par 8 = 16).

Il s'agit d'un standard de sécurité pour les trois systèmes traités.



▲ *Bien souvent, pour accéder aux informations les plus précieuses, il suffit tout simplement de... changer de clé !*

Changer de mot de passe

RIP possède également une autre puissante fonction : CHNTPW pour Change NT Password (mais ça fonctionne aussi pour XP !). Cette fonction trouve le fichier SAM et remplace le hash présent par celui que nous souhaitons. Le problème c'est que la version du kernel de Linux présente dans RIP ne nous permet pas d'accéder aux partitions NTFS en mode lecture. Ainsi, nous pouvons accéder au SAM de Windows XP mais nous ne pouvons pas le modifier...du moins pour l'instant. Vous pouvez remplir le kernel Linux avec le module NTFS Lecture E Ecriture mais cela demande du temps. Nous évoquerons peut-être ce sujet une prochaine fois. Il existe un RIP automatique spécifique dans lequel l'utilisateur doit seulement répondre à certaines questions et enregistrer son compte. Ce programme enregistre les données téléchargées sur une disquette (à condition de l'avoir insérée préalablement !). Une fois le software copié sur le disque, il vous suffira de rebooter à partir de celui-ci...

DES OUTILS TRÈS UTILES

Vous pouvez trouver nos outils aux adresses suivantes :

RIP : <http://tux.org/pub/people/kentrobot/looplinox/rip>
 CMOSPWD : www.cgsecurity.org/cmopwd.html
 CHNTPW : <http://home.eunet.no/pnordahl/ntpsswd>

Nous y sommes !

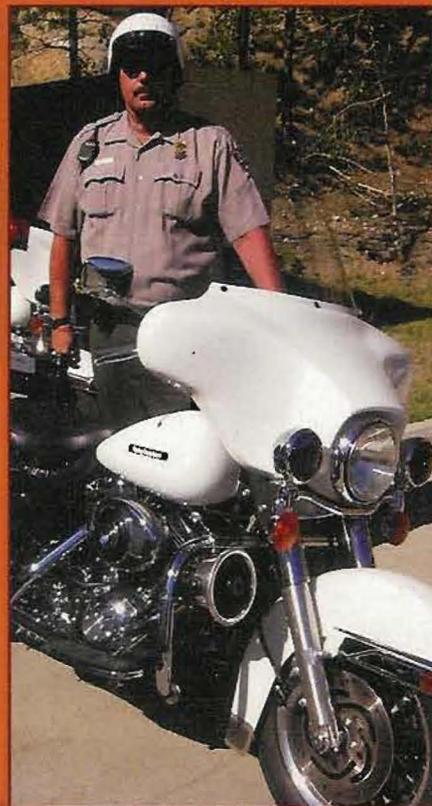
Une fois la disquette lancée, un microkernel de Linux se lance à son tour et vous verrez vos lignes de code apparaître automatiquement. A la fin du chargement, le système vous demandera si vous possédez un disque SCSI. Un simple message de formalité qui devrait disparaître aussi vite. Dans le cas contraire, vous devrez alors télécharger un autre programme sur le site de RIP. Imaginons que cette procédure ne soit pas utile et répondons par «N». A présent, le script affiche une liste des partitions en montrant

celle qui sera utilisée par le boot. Le système vous demande ensuite si le parcours vers le fichier SAM est celui habituellement utilisé. Le parcours standard est celui normalement utilisé pour NT : `winnt/system32/config`

Sous Windows 2000 ou XP, le parcours est le suivant : `Windows/system32/config`

Il vous suffit maintenant d'entrer le nom d'utilisateur auquel vous souhaitez accéder. En tapant « ! », vous verrez apparaître tous les utilisateurs disponibles pour choisir ensuite le vôtre. Vous disposerez alors de différentes informations sur le compte, avec le hash du mot de passe ! Vous pouvez à présent entrer votre nouveau mot de passe. Si vous laissez le champ blanc, rien ne changera. En tapant votre nouveau mot de passe et après avoir appuyé sur Entrée, le programme affichera le nouveau hash et l'insérera au lieu du précédent à l'intérieur du SAM. Pour que le mot de passe actif soit votre nou-

▼ Attention à ne pas jouer de mauvaises plaisanteries sur l'ordinateur d'un autre. Les collègues de ce monsieur pourraient ne pas apprécier !



▲ Chercher son mot de passe sur Google est totalement inutile !

veau mot de passe, redémarrez l'ordinateur.

Vous pouvez maintenant de nouveau exécuter le login avec votre compte modifié et le nouveau mot de passe.

TROUVER LES MOTS DE PASSE

Certes, si l'on perd en revanche le mot de passe d'un programme et non le mot de passe d'accès au système, la situation n'est alors plus la même. En attendant d'écrire un article sur ce sujet (aussi intense et fastidieux que celui traité sur ces trois pages), signalons un software spécialement créé dans ce but.

ABF Password Recovery est un outil spécialement conçu pour récupérer les mots de passe perdus ou oubliés, optimisé pour fonctionner avec la majorité des applications tournant sous Windows. Cela ne règlera peut-être pas tous vos problèmes de mots de passe de façon définitive, mais ce petit programme peut tout de même s'avérer très utile.

Le software inclut toute une série d'outils extrêmement utiles comme Password Picker (pour choisir le mot de passe à récupérer), Hidden Passwords Browser (qui permet de passer en revue les mots de passe occultés) et un Personal Folder Recovery qui va à la pêche aux dossiers personnels.

L'interface du programme est personnalisable en fonction des goûts et des préférences des utilisateurs. La version disponible à ce jour peut gérer les programmes suivants : Internet Explorer, Outlook Express, Office Outlook, Office Access, Total Commander et FAR Manager... pensez-y !

Pour plus d'informations, rendez-vous sur le site du téléchargement <http://www.abf-soft.com/download.shtml>

Comment détourner l'attention de sa nounou ?

*Avons-nous vraiment besoin d'une nounou ?
De quelqu'un qui limite nos navigations ?
Certains filtres sont vraiment casse-pieds,
voici comment les contourner ...*



Certains programmes filtre ont été créés pour empêcher l'accès à des sites Internet dont les contenus pourraient heurter la sensibilité des plus jeunes ou être inadaptés à certains surfeurs. Mais l'ennui avec ces programmes, c'est qu'en fonction de certains critères, ils parviennent à limiter la navigation ! Il s'agit clairement d'une forme de censure, un concept qui ne plaît pas beaucoup à ceux qui ont soif de connaissances et qui souhaitent préserver leur droit en matière d'accès aux informations. Bref, le libre arbitre. Mais alors, que peut-on faire ?

:: Méthode 1

Eh bien ! Vous pouvez vous débarrasser de ce maudit chien de garde, voilà ce que vous pouvez

◀ *Net-Nanny n'est que l'un des programmes qui, tout en partant de bonnes intentions, met en place une censure qui, parfois, va trop loin ! De notre côté, nous estimons que toute forme de censure est condamnable ...*

faire ! Prenez par exemple Net-Nanny. Vous pouvez supprimer les blocages de Net-Nanny en partant des commandes Démarrer>Exécuter de la version 4.0 (il y en a plusieurs en circulation !). A présent, tapez "msconfig" et lancez la configuration du système. Pointez et cliquez sur Démarrer et décochez "nntray.exe" et "NNSvsc". Il ne vous reste plus qu'à redémarrer et le tour est joué.

:: Méthode 2

Un autre système consiste à "endormir" la "nounou" (Nanny signifiant Nounou en anglais). Pour ce faire, désactivez le programme à partir du gestionnaire de tâches en appuyant sur CTRL-ALT-SUPPR.

Cherchez dans la fenêtre qui s'ouvre la rubrique de la tâche OCRAWARE ou Wnl-dr32 (l'une ou l'autre rubrique apparaît en fonction de la version de NN).

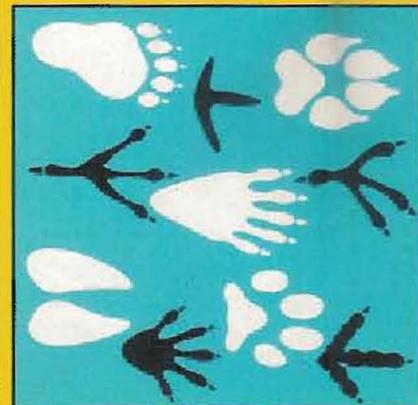
Pour tout arrêter, il suffit de cliquer sur "Terminer opération". Si en revanche vous souhaitez retirer totalement ce filtre de censure, vous devrez trouver le fichier c:\windows\system.ini et en faire une copie de sauvegarde avec un nom différent. Dès lors, ouvrez le fichier récupéré en utilisant le Bloc-Notes.

Trouvez l'intitulé [boot] qui devrait être immédiatement suivi de la rubrique "drivers=" à laquelle s'ajoute une liste qui comprend wndrv16dll". Effacez cette dernière rubrique avant d'enregistrer le fichier.

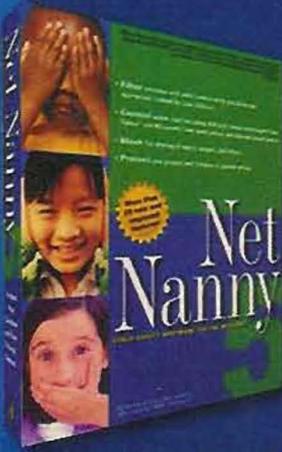
COMMENT EFFACER TOUTE TRACE ?

Vous pouvez effacer toute trace de vos navigations "exploratrices" en suivant une procédure à la fois simple et rapide. Vous devez avant tout trouver le fichier Wnn3.log. Il devrait se trouver dans le répertoire normalement utilisé par Net-Nanny. Il s'agit d'un fichier composé de chiffres.

Comme le savent tous les hackers dignes de ce nom, vous ne pouvez pas le modifier. Tout ce que vous pouvez faire c'est le supprimer totalement. Et voilà, le tour est joué... le log avec vos "traces" a disparu !



▲ *Chacun d'entre nous laisse un type de traces différent... même dans le log ! Apprenez à les effacer, car on ne sait jamais...*



Linux à vos ordres !



Voici comment prendre le contrôle total du Live-Cd Linux !

Live-CD Linux est vulnérable. Très vulnérable ! A tel point qu'on pourrait presque y rentrer comme dans un moulin.

Bien sûr, certains outils s'avèrent nécessaires, sans oublier une bonne dose de connaissances. Le fait est qu'il se passe certaines choses lors du boot d'un Linux Live, et les procédures de chargement pourraient facilement être exploitées par des agresseurs malintentionnés.

:: Une exploration agressive

Toute attaque passe d'abord par une opération de reconnaissance. Dans notre cas, l'idéal était d'obtenir une image iso du CD à attaquer. Imaginons que nous ayons à notre disposition Slax. Procurons-nous le C, ce qui est relativement simple, dans la mesure où il nous suffira de lancer la ligne de commande suivante à partir d'une shell Linux :

```
# dd if=/dev/hdc of=/directory/desiderata/slax.iso
```

Le segment «/dev/hdc» devra être remplacé par le vrai path de notre driver. Ouvrons notre iso. Nous devons rajouter le répertoire dans lequel nous avons créé le dump de l'iso et nous créerons un autre répertoire, en

codifiant ensuite les commandes qui apparaissent ci-après. Si tout fonctionne correctement, nous verrons apparaître les fichiers de la distribution.

```
#mount -t iso9660 -o loop slax.iso mydir
# cp -rp mydir slax
# umount slax.iso
# rm -rf mydir
# cd slax
```

:: Entrons dans le bios

Pour exécuter un Live-CD, accédons au Bios (le CD doit être prioritaire sur le disque dur concernant le boot). Pour en revenir à Slax, le boot loader qui nous servira est isolinux, composé d'isolinux.bin (le boot loader principal) et isolinux.cfg (qui règle la configuration). Jetons-y un coup d'œil :

```
#cat isolinux.cfg
display splash
default slax
prompt 1
timeout 50

label slax
kernel vmlinuz
append max_loop=255
initrd=initrd.gz init=linuxrc
livecd_sudir=/ load_ramdisk=1
prompt_ramdisk=0
ramdisk_size=7777
root=/dev/ram0 rw lang=it
```



:: Mais qu'est-ce que ça signifie ?

Tentons de déchiffrer ce qui est écrit : avec la première ligne, nous visualiserons le fichier dénommé « splash ». La seconde ligne de notre ensemble d'informations nous permet de déterminer le label normalement prédéfini. La troisième assure le lancement du prompt «boot» : ce passage est nécessaire pour transmettre d'autres paramètres éventuels au kernel. La rubrique «label slax» nous montre l'étiquette effective de lancement de l'OS de no-



tre Live-CD. La commande «kernel» permet de définir les fichiers du kernel, qui recevra justement certains des paramètres, comme par exemple ceux qui se trouvent près de l'instruction « append ». Les autres paramètres éventuels pourront être transmis par l'utilisateur à travers le prompt «boot». Ces paramètres sont représentés dans le fichier «splash». Observons les paramètres de base, car ce sont ceux qui nous intéressent plus particulièrement. Nous devons surveiller notamment les «initrd=» et «init=».

Après avoir décompressé le fichier initrd, tentons de le monter en loop. Ainsi, nous devrions obtenir :

```
#gunzip initrd.gz
#mkdir initrd_mount
# mount -o loop,rw initrd
initrd_mount
# cd initrd_mount
```

:: Pénétrons à l'intérieur !

Voici venu le moment d'entrer et de voir un peu ce qui se passe aux alentours. Mais avant tout, il convient de rappeler une fois encore que les informations présentées ici le sont uniquement dans un but essentiellement didactique.



▲ *Damn Small Linux : une version de Linux... minuscule mais puissante !*

Cela signifie qu'en suivant la philosophie légitime qui caractérise le hacker, nous apprenons à étudier les choses, à comprendre leur mécanisme, à nous faire une idée des lois et règlements qui se cachent derrière ces choses. Etre capable de violer une protection ou savoir cracker un programme ne nous autorise pas pour autant à le faire, à moins... qu'il ne s'agisse

de choses qui nous appartiennent effectivement. Dans le cas contraire, nous commettons ni plus ni moins un délit. Poursuivons : nous devons surveiller la



▲ *Réussir à prendre le contrôle total d'un Live-CD de Linux peut apporter certaines satisfactions.*

se de choses qui nous appartiennent effectivement. Dans le cas contraire, nous commettons ni plus ni moins un délit. Poursuivons : nous devons surveiller la valeur de «init=» Il s'agit de «linuxrc». Si nous lançons ls à l'intérieur du mount point de l'initrd, nous devrions alors noter la présence d'un fichier système Linux au complet. A ses côtés, on trouvera également un script Bash dénommé linuxrc. Tentons de l'ouvrir : nous pourrions effectivement voir qu'un autre fichier bourne shell-script est importé, et qu'il est doté de certaines des fonctions qui sont normalement utilisées dans linuxrc. A ce stade, nous pouvons comprendre quelles sont les opérations qui sont effectuées par ce fichier. Il s'agit de la création d'un fichier système virtuel de zéro octet, de la décompression des images présentes, de la procédure de copie de ces dernières dans le fichier system, du changement du répertoire et de root (ce processus est généralement appelé chroot = change root). Enfin, nous avons le lancement du système décompressé. Une fois ces opérations achevées, nous verrons apparaître une fenêtre d'introduction et le prompt de login : notre Linux Live est maintenant sous contrôle. Il est bien évidemment possible d'entreprendre dorénavant une série de nouvelles étapes, mais cela fera éventuellement l'objet d'un autre article.

Ra23R_One
RazerOne@mailinator.com

IMAGE ISO

Le terme «Image ISO» indique en principe les fichiers contenant le fichier système ISO9660, c'est-à-dire une représentation de ce qui se trouve à l'intérieur d'un disque ou de ce qui le composera à l'avenir. Une sorte d'aperçu, pour ainsi dire. Le programme Winrar est capable de lire les fichiers iso avec une extension «.iso». Winrar peut les décompresser dans un dossier spécifique, et s'il s'agit d'une application, les fichiers seront enregistrés sur le disque dur. Si notre ISO correspond à un système d'exploitation, nous pourrions alors procéder uniquement à l'installation de certaines des applications qui le composent et non du programme dans son ensemble. Ubuntu est un cas particulier, dans la mesure où certains des logiciels d'application en circulation peuvent l'installer complètement, même à partir de Windows, en mode dual boot. Cela permet également de choisir entre Windows et Linux au démarrage du système. Il existe une méthode d'utilisation des programmes qui prévoit la création d'une partition supplémentaire avec un lecteur CD virtuel. Le fichier décompressé à partir de l'ISO sera sauvegardé dans cette zone du disque dur. Bien qu'il soit effectivement présent sur l'ordinateur, le système le lira comme s'il était présent sur le CD et exécutera l'installation. Exécuter des programmes enregistrés sur le disque dur offre l'avantage d'une installation plus rapide, outre un lancement et une exécution des commandes plus «nerveux».

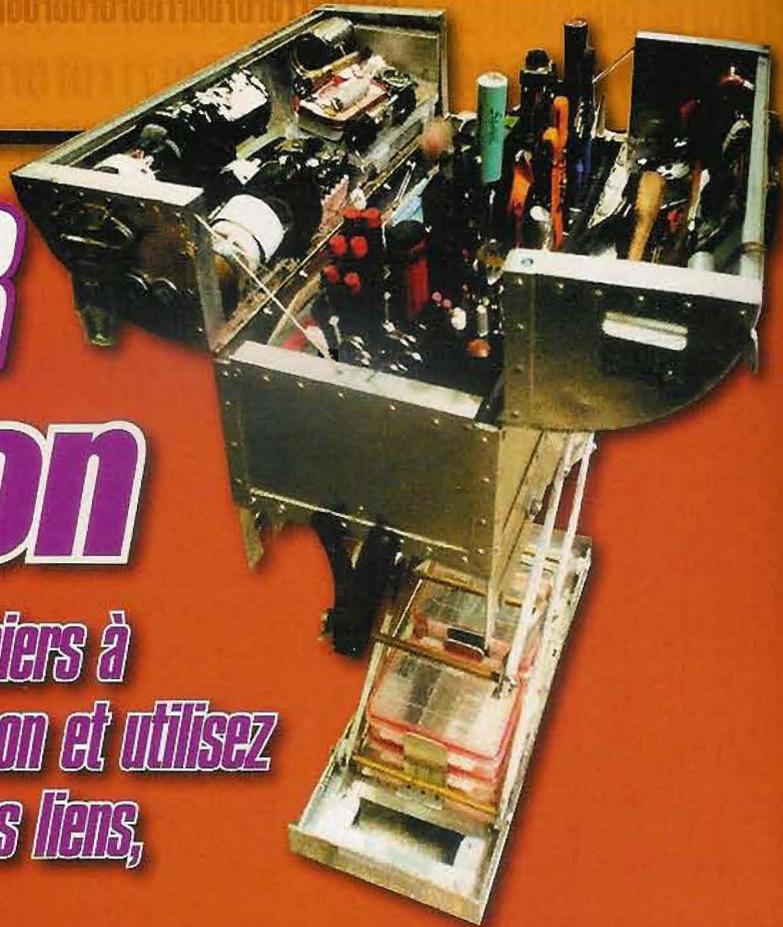


Nous n'irons peut-être pas jusqu'à le faire chanter ou danser, mais les fonctions offertes par APT sont réellement en mesure de contrôler le pingouin.



SERVEUR maison

Partagez vos données et fichiers à l'aide d'un serveur web maison et utilisez un wiki pour sauvegarder vos liens, commentaires et notes.



Avec les connexions Internet à bande large, et les forfaits illimités, il est aujourd'hui possible de laisser son PC connecté au réseau 24h/24. Alors pourquoi ne pas exploiter cette possibilité pour créer un serveur domestique auquel accéder depuis n'importe quel ordinateur équipé d'une connexion Internet (à l'école, à l'université, etc. ?). Un serveur domestique peut prendre différentes formes, mais le serveur web est sans aucun doute le plus utile et le plus polyvalent. Vous pouvez créer des pages Html pour partager des informations avec vos amis, parents et collègues de travail (comme vos photos de vacances ou encore une recherche pour l'école), leur permettre de télécharger des fichiers sur votre ordina-

teur ou encore installer des applications web à proprement dit comme un forum ou un wiki. Voici comment installer un serveur web Apache et une application permettant de gérer un wiki. Nous utiliserons notamment ce dernier comme «cahier de notes» afin d'accéder et modifier nos informations personnelles et ce, où que nous nous trouvions.

:: Installons le serveur web
Lorsqu'on parle de serveur web, le premier nom qui nous vient à l'esprit est Apache (w), le logiciel open source le plus répandu sur le net. Si vous utilisez Linux, Apache est inclus dans la plupart des distributions les plus utilisées. Sur des distributions basées sur Debian (w),

comme Ubuntu Linux (www.ubuntu.com), il vous suffit d'installer le pack «apache2» (la version 2 du serveur) avec le programme shell «apt-get» (ou ses équivalents graphiques, comme Synaptic) :

```
apt-get install apache2
```

Vous pouvez accéder au serveur à partir du PC sur lequel vous l'avez installé en tapant h sur votre navigateur web et vérifier que l'installation s'est effectuée correctement. Vous ne pouvez accéder à votre serveur web depuis un PC extérieur que si vous connaissez son adresse IP ou si vous utilisez un service de DNS dynamique comme DynDNS (w) grâce auquel un nom de domaine à proprement dit vous sera assigné. Si vous créez des pages Html et que vous souhaitez les voir sur le serveur web qui vient d'être installé, vous devez alors copier les fichiers dans le répertoire prédéfini «/var/www/» (vous pouvez également reconfigurer Apache pour utiliser un répertoire différent – pour les détails, consultez l'aide d'Apache sur la procédure à suivre).

Vous pouvez rendre votre serveur encore plus polyvalent en installant le langage Php (w) et le moteur de base de données

LE NOM DE DOMAINE INTERNET

Condition importante pour accéder à votre serveur web domestique : celui-ci doit être doté d'un nom de domaine internet. Dans le cas contraire, vous serez contraints de connaître l'adresse IP. Dans la mesure où votre adresse IP change même si vous utilisez une connexion à bande large, la seule solution au problème consiste à utiliser un service de Dns dynamique comme par exemple celui de DynDNS (w). S'inscrire et bénéficier de ce service gratuit s'effectue en quelques clics et vous permet d'obtenir un nom de domaine de troisième niveau comme par exemple «votre nom.homelp.net».



▲ *WikkiTikkiTavi est l'un des moteurs de wiki écrits en PHP les plus utilisés grâce à ses fonctions avancées. Il reste malgré tout léger, même pour une utilisation domestique.*

MySQL (w) avec lesquels vous pourrez créer des sites dynamiques en utilisant les très nombreuses applications web disponibles sur le net (forum, wiki, galeries d'images, etc.) ou encore en programmant directement par vous-même tout le nécessaire. Sur des distributions Debian-based, installez les packs nécessaires :

Relancez ensuite Apache :

```
/etc/init.d/apache2 restart
```

Pour installer MySQL et la librairie Php nécessaire à son utilisation :

```
apt-get install php5
apt-get install libapache2-mod-php5
```

Enfin, installez PHPMyAdmin (w), une application Php qui vous permet de créer et gérer des bases de données MySQL grâce à une interface Web très pratique :

```
apt-get install phpmyadmin
```

Si quelque chose ne fonctionne pas, il pourrait être nécessaire d'activer le support de MySQL dans PHP. Editez le fichier «/etc/php5/apache2/php.ini» et supprimez le commentaire de la ligne «extension=mysql.so» (concrètement, vous devez supprimer le point virgule initial).

```
apt-get install libapache2-mod-auth-mysql
apt-get install php5-mysql
```

Enfin, relancez une dernière fois Apache :

```
/etc/init.d/apache2 restart
```

PHPMyAdmin pourra être utilisé à l'adresse <http://localhost/phpmyadmin> (depuis l'accès distant, remplacez localhost par le nom de domaine ou l'adresse IP de votre PC domestique)



▲ *PHPMyAdmin est une application web très pratique qui vous permet de gérer toutes vos bases de données MySQL de façon simple et rapide.*

:: installez le wiki

Il existe de nombreuses alternatives pour le wiki, certaines très complexes comme Mediawiki (w) qui est le moteur de wiki avec lequel est gérée la célèbre Wikipedia (w) mais dans notre cas, nous voulons installer une application simple et disposant de toutes les fonctionnalités essentielles, sans être trop lourde pour autant.

A la fin, vous utiliserez le wiki pour gérer des notes, commentaires, listes de liens et bien d'autres choses encore, de façon à ce que ces informations soient toujours disponibles et mises à jour et ce, où que vous vous trouviez (il vous suffit tout simplement de vous connecter à votre serveur web). Nous avons sélectionné trois alternatives susceptibles de vous être utiles dans ce cas précis. Il s'agit de WikkiTikkiTavi (<http://tavi.source-forge.net>), PmWiki (<http://www.pmwiki.org>) et miniWiki (<http://miniwiki.sourceforge.net>). Les deux premiers sont des moteurs de wiki assez répandus, également

utilisés sur des sites à fort trafic, tandis que miniWiki est un projet Open source relativement nouveau mais qui nous a semblé très intéressant : c'est un wiki qui s'adresse à l'utilisateur individuel ou à de petits groupes de travail même si ce software n'est pas encore aussi abouti que les deux autres. Ces trois softwares utilisent PHP ainsi qu'une base de données MySQL pour mémoriser les pages (à l'exception de PmWiki). Leur procédure d'installation est très simple : il suffit de copier les fichiers dans le répertoire de votre serveur web, puis d'éditer le fichier de configuration et de régler les paramètres requis. Par exemple, dans le cas de miniWiki, vous devez éditer le fichier «userprefs.php» en entrant les données pour la connexion à la base de données. Courage, lancez-vous !



▲ *Pas de panique, votre serveur ne devrait pas ressembler à ça ! Soulagés ?*

SERVEUR POUR WINDOWS

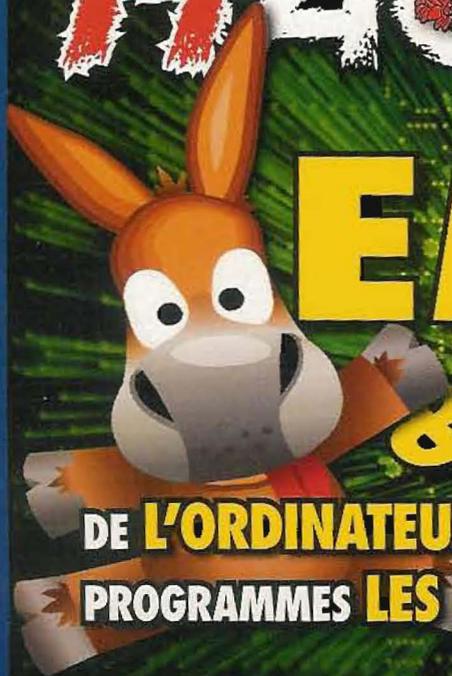
Installer tous les logiciels nécessaires pour disposer d'un serveur web sur votre PC domestique est une opération extrêmement simple même si ce dernier tourne sous Windows. Il vous suffit en effet d'installer XAMPP (w) qui est une sorte de distribution d'outils pour serveur web. Un programme pratique de set up installe en une seule fois Apache, PHP, MySQL et PHPMyAdmin. Il vous suffit de copier les fichiers Html ou les scripts Php dans le dossier «htdocs» contenu dans le parcours d'installation de XAMPP puis d'activer le serveur grâce au panneau de configuration que vous trouverez dans le menu Programmes.

LE COMPLÉMENT INDISPENSABLE

LE MAGAZINE AVEC SON CD-ROM EXCLUSIF

HACKERS

MAGAZINE



EMULE & ASSOCIES

DE L'ORDINATEUR AU PORTABLE TOUS LES
PROGRAMMES LES PLUS PUISSANTS POUR LE P2P



LES PROTECTIONS DU VRAI HACKER

LES SYSTÈMES POUR BLOQUER TOUS
LES ACCÈS INDÉSIRABLES

☑ SUR LE CD-ROM 630 MB :

- 38** LOGICIELS COMPLETS DONT
- 5 ÉDITEURS DE TEXTES POUR VRAIS HACKERS
 - 5 POUR LES ÉCHANGES DE FICHIERS
 - 4 NOUVEAUX SYSTÈMES D'EXPLOITATION
 - 2 LOGICIELS DE SÉCURITÉ

Sprea
édition



ISSN 1720-7673
M 02192-16 F 4,99 €-PD
REVUE 41-2008 BEL LUX S.C.
- SUISSE - 8 878 - 0013 S.P.C. CAN. \$ 5.00 CAD

EN VENTE DEPUIS LE 18 NOVEMBRE

Mais qu'arrive t-il donc au réseau secret ?

Né en tant que réseau d'échange sécurisé et crypté, Waste prend aujourd'hui du galon et s'apprête à un nouveau départ

Waste est un outil incroyable, un réseau secret, parallèle, entièrement sécurisé. Ce système permet à plusieurs utilisateurs de partager des idées et des projets grâce à une interface de chat, pour pouvoir partager ensuite les fichiers grâce aux fonctions classiques de téléchargement.

:: La structure

Waste est configurable en fonction des groupes qui l'utilisent et permet de franchir les conventions globales auxquelles nous contraignent les géants du web traditionnel.

La version 1.5.1 de Waste est déjà une

belle réussite en soi, mais la version 2.0 devrait bientôt pointer le bout de son nez ! Pour faire court, Waste offre la possibilité d'ériger un réseau de peer-to-peer extrêmement sécurisé. Il utilise le système de chiffrement de Blowfish avec une authentification par clef publique : RSA. Grâce à ces astuces, nous pouvons échanger des fichiers sans que personne ne puisse déchiffrer les termes ou contenus de la communication. Ça mérite un joli coup de chapeau ! Il s'agit d'un réseau privé de host ou chacun doit s'authentifier face aux autres, de façon à ce que le transfert crypté puisse ensuite avoir lieu.

:: Comment communique-t-il ?

La communication entre utilisateurs de Waste utilise trois catégories différentes de messages. D'abord, les messages transmis normalement, qui sont envoyés par un host lorsque celui-ci souhaite notifier ou demander des informations à tous les autres hosts du réseau. On trouve ensuite les messages adressés, à savoir ceux qui sont envoyés en réponse à un message normalement transmis. Ces messages reviennent directement au host qui avait lancé la communication. Dernière catégorie, celle des messages de gestion locale, envoyés directement entre deux nœuds (il est possible d'en avoir jusqu'à 50 !), de façon à négocier les paramètres de configura-

tions des liens.

La structure des messages du réseau est flexible et permet d'adopter de nouvelles catégories de messages dès lors que les groupes qui les utilisent en ont besoin. Ces types de messages ont assuré jusqu'à présent une communication sécurisée et protégée. Une véritable manne !

:: Les nouveautés

La version 2.0 présentera une documentation renforcée, de façon à favoriser une utilisation qui, pour l'heure, rencontre quelques petits problèmes (elle n'est pas totalement intuitive). Mais ce problème devrait être réglé au plus tôt. Le système d'envoi et de transit des paquets de données sera lui aussi amélioré, avec un échange direct et biunivoque entre les différents utilisateurs. Pour favoriser la diffusion de cet outil la plus large qui soit, un client multiplateforme est actuellement en phase de réalisation et devrait permettre de créer également des réseaux entre utilisateurs disposant de systèmes différents. Bref, toutes les barrières seront franchies ! ☺

OBJECTIF WASTE

PVous trouverez davantage d'informations sur le projet Waste sur <http://waste.sourceforge.net/index.php?id=information>. Vous pouvez également télécharger le software pour votre réseau sur http://sourceforge.net/project/showfiles.php?group_id=82356. Ce petit réseau parallèle est le fruit d'idées très intéressantes et mérite toute notre attention et notre respect.



La police tend des pièges dans le RESEAU

Voici le système qui permet de remonter à l'ip de ceux qui échangent des fichiers... afin de les coincer !

Comment font-ils pour remonter à un surfeur imprudent embarqué dans un échange p2p au contenu illicite ? Comment procèdent-ils pour localiser les utilisateurs lorsqu'ils s'échangent des fichiers mp3, mais dont la facture risque d'être salée si l'on ne possède pas l'autorisation de la Siae, comme il se doit ? L'évolution des réseaux peer-to-peer s'est traduite par

une décentralisation, à savoir la diffusion tentaculaire de nœuds interconnectés entre eux. Ce système présente deux avantages : les sociétés qui produisent le software de connexion ne peuvent pas être accusées d'incitation au délit, dans la mesure où elles ne fabriquent pas "la totalité" du software nécessaire, lequel, en revanche, a forcément besoin de l'ensemble des autres nœuds tout aussi équipés pour fonctionner. Second avantage : si un nœud fait des siennes ou est fermé, personne ne s'en aperçoit car le réseau s'habitue à fonctionner sans lui.

QUI PEUT ROULER LES ESPIONS ?

Quel logiciel pourrait vous protéger des nœuds-espions, lorsque vous êtes dans un réseau p2p ?

Mute est l'un d'entre eux. Il est Open Source et existe pour Linux, Mac OSX et Windows. Vous pouvez le télécharger à l'adresse suivante <http://mute-net.sourceforge.net/>. Sous Linux, vous pouvez utiliser tout un tas d'interfaces qui explorent l'algorithme de Mute et simplifient la vie de l'utilisateur. L'une d'entre elles est Kommute, un client file sharing utilisable avec l'interface graphique open source Kde (<http://www.kde.org/>).

:: Lorsque nous effectuons des recherches...

Le réseau peut être assimilé à une communauté de personnes : tous reliés entre eux, ou à bon nombre d'entre eux. C'est comme lorsqu'on rencontre un ami qui en présente un autre qui lui, est en revanche déjà connu. La relation s'effectue avec le vieil ami mais aussi avec l'autre sans oublier cet autre ami rencontré "par le



▲ Le réseau, ça ressemble plus ou moins à ça : tous connectés à de nombreuses personnes comme lorsque nous nous présentons des copains et copines...

biais" du premier ami. Lorsqu'on recherche un fichier dans le réseau, la demande aboutit aux nœuds auxquels on est connecté, qui envoient à leur tour la demande aux nœuds qui leur sont connectés et ainsi de suite. La demande peut être reçue par plusieurs nœuds ayant un lien avec ce qu'on a demandé. Chacun d'entre eux nous répondra avec son propre contenu.

Supposons que vous demandiez par exemple "beyonce mp3". Un tas de nœuds reçoivent la demande et certains répondent ainsi :

Mon adresse est la suivante :	Et je possède ce fichier :
129.224.12.162	Beyonce__Deja Vu.mp3
129.224.12.162	Beyonce__Suga Mama.mp3
129.224.12.162	Beyonce__Kitty Kat.mp3

L'adresse faisant partie intégrante de la réponse, vous pouvez bien sûr savoir exactement quel nœud possède le fichier qui vous intéresse. Pour télécharger les fichiers à partir du nœud qui vous a répondu, votre PC se connecte directement à l'adresse qui vous a été fournie. Et c'est l'entourloupe ! Car au moment où votre logiciel se connecte au nœud qui possède les fichiers, il envoie à ce dernier votre adresse Ip. Il est contraint de le faire, sinon les paquets de données dans lesquels le fichier est morcelé, ne sauraient pas comment faire pour atteindre votre PC. Une fois les fichiers envoyés, la connexion est fermée.

:: Comment procèdent-ils pour vous coincer ?

Ensuite, le système n'est pas si compliqué lorsqu'on utilise les "programmes espions". Comme dans toutes les enquêtes de police les plus risquées et sophistiquées, le soutien d'un espion est souvent essentiel. C'est ainsi qu'ont dû raisonner les membres de la puissante association américaine Rïaa, ou les différentes organisations européennes, même italiennes, qui tentent d'imposer le copyright sous peine de sanctions, au lieu de trouver des alternatives aux anciennes règles de marché. D'un point de vue technique, un espion est un nœud comme les autres, mais il prend l'initiative de lancer des demandes au réseau pour dénicher des morceaux de musique, films, jeux et logiciels qu'il souhaite absolument garder sous contrôle. Son logiciel p2p lance toutes les demandes de téléchargement à partir du serveur piège en question, demandes qui arrivent également à votre ordinateur. Si vous les possédez, votre PC répond par l'affirmative et le site piège reçoit à maintes reprises tous les fichiers que vous possédez et l'adresse Ip d'où proviennent ses tentatives de téléchargement : votre Ip. Un logiciel spécifique compte exactement le nombre de réponses provenant d'un seul Ip et garde en mémoire de précieuses statistiques à ce sujet. Lorsque certains paramètres, plus

ou moins restrictifs selon l'organisation qui souhaite vous coincer, sont dépassés, le piège se referme. Un coup de fil à votre fournisseur d'accès d'une certaine autorité judiciaire ouvre grand toutes les portes et votre Isp est contraint de donner votre signalement, y compris l'adresse de votre domicile et le log qui montre quand, à partir d'où, combien de fois et à qui vous vous êtes connectés. Bref, vous êtes dans de beaux draps !

:: La défense

Face à cette atteinte à la confidentialité des données et pour éviter que la bataille ne dégénère en guerre, vous pouvez mettre en place certains moyens de défense. L'une des combines consiste à éviter de se connecter directement au nœud contenant les fichiers demandés. L'astuce, c'est vite dit ! La demande comme le téléchargement des fichiers sont orientés vers les nœuds auxquels vous êtes connectés. Chaque nœud du réseau est redéfini avec une adresse fictive qui est générée de façon aléatoire chaque fois qu'il reçoit une demande. Elle n'est donc active que pour votre demande et non pour d'autres. Elle est également totalement renouvelée à chacune de vos demandes. Voici un schéma d'adresse typique :

2313B79881590841GF10CCD1E9A9B723AG16FCQ8

Ce type d'adresse vous indique dans quel nœud se trouve le fichier demandé. Si vous décidez de le télécharger, ce fichier parcourt à nouveau les adresses virtuelles en sens inverse et vous rejoint, mais toujours en passant par d'autres nœuds. Ok, maintenant c'est au tour du serveur-espion d'attaquer. Le PC étant un nœud du réseau, il répond : "affirmatif, j'ai tout ce que vous me demandez". Mais il le fait en indiquant sa propre adresse virtuelle, générée de façon aléatoire par cette demande spécifique et totalement inutile pour remonter au véritable Ip de la machine de l'utilisateur. Dès lors, tout va bien ou presque...

L'espion cherche encore !

Pour tenter de contourner le système qui a été conçu pour protéger les uti-

HE ! MAIS CA FONCTIONNE ?

Les expériences des utilisateurs sont très différentes, mais dépendent également beaucoup de la zone géographique de l'Ip, de la bande disponible, de la disponibilité effective de nœuds Mute actifs à cet instant et de tout un tas d'autres paramètres que souvent, on ne parvient même pas à déterminer... En réalité, pour certains, Mute fonctionne mieux que pour d'autres et très souvent, son bon fonctionnement dépend pour beaucoup de l'installation et de l'ouverture du pare-feu sur le système. Consultez les forums (une bonne recherche sur Google, et vous trouverez tout ce dont vous avez besoin) et l'expérience de ceux qui l'ont déjà installé demeure dans tous les cas un bon conseil, surtout pour ceux qui font leurs premières armes. Mute est certainement plus lent, ne l'oubliez pas, que de nombreux autres systèmes "visibles". La raison, vous devriez l'avoir comprise.

lisseurs, le serveur-espion est devenu entre temps plus sophistiqué. En augmentant la capacité de contrôle du réseau, il pourrait localiser le PC qui gère le plus gros trafic et observer son comportement. Si la quantité de demandes que vous faites est égale à la quantité de demandes que vous réémettez, vous présentez tout simplement des nœuds innocents du réseau. Si la quantité de demandes que vous faites est plus importante que celle des demandes que vous réémettez, vous êtes des téléchargeurs sauvages. Du moins dans la logique de l'espion. Le seul moyen pour se protéger dans ce cas, consiste à crypter au maximum et de façon sûre les messages que vous émettez. Ainsi personne, pas même l'espion, ne pourra lire ce qui se trame réellement et encore moins votre adresse Ip. Seuls les nœuds proches de l'utilisateur en question peuvent déchiffrer et comprendre la provenance des messages. Bien sûr, si le nombre d'espions devait augmenter et que chaque nœud était étroitement contrôlé par autant de nœuds espions, dans ce cas, la sécurité des transmissions serait, elle aussi, compromise. Mais il ne s'agit que d'une probabilité de contrôle qui diminue de façon vertigineuse, même si elle ne disparaît jamais totalement. ■

MAP Attack!

Quelques astuces en matière de HTML pour des sites ayant des fonctions vraiment intéressantes

Les sites qui utilisent les images maps sont très nombreux. Mais rares sont ceux qui savent fournir des équivalents en texte pour les browsers de hacker et les personnes plus ou moins habiles. Vous pouvez voir un bel exemple d'image map utilisée en bas de page sur le site suivant <http://leslie.harbold.com/>. Les liens en bas à droite (Archives, By Category, Links et About) ne sont pas des chaînes de texte, mais des zones d'une carte graphique, à savoir une image map. Les images maps peuvent être client side ou server side ; dans le second cas, les informations sur les liens sont fournies par le serveur, tandis que dans le premier, elles sont directement insérées dans la page HTML (et il est intéressant de les étudier pour comprendre leur fonctionnement). Mais que se passe-t-il si une personne vi-

site une page contenant une image map avec un browser texte uniquement, comme Lynx, ou a des problèmes de vue par exemple ? Les indications de l'image map seront perdues. Chaque image intégrée à un site ayant besoin de son équivalent en texte, les images maps doivent également suivre le même processus. On peut insérer par exemple un texte alt relatif à l'image même (dans le tag) et il conviendrait de faire de même pour chaque zone

cliquable de l'image map (dans les tags <area> de la <map> associée à l'image)..

:: Comment la codifie-t-on ?

Gardons toujours à l'esprit le site cité en exemple et observons les liens de l'image map :

Si on ajoute le texte ALT à l'image principale et aux zones cliquables, voici le résultat :

```

<map name="Map">
<area shape="rect" coords="203,114,258,129? href="/archives.html">
<area shape="rect" coords="277,113,348,129? href="/category/">
<area shape="rect" coords="364,113,401,128? href="links.html">
<area shape="rect" coords="418,114,488,130? href="leslie.html">
<area shape="rect" coords="-4,190,131,210? href="http://
www.moveabletype.org">
</map>
```

LE BROWSER LE PLUS RAPIDE

Lynx est uniquement un browser texte, qui ignore les images. C'est donc un browser très pratique lorsqu'on cherche des informations écrites. Il fonctionne bien mieux que les autres sur des connexions lentes et, dans la mesure où il ne charge pas d'image, c'est le browser le plus rapide au monde ! A condition tout de même que les pages soient écrites par des personnes intelligentes, qui pensent aux exigences de tous. Lynx existe pour tout système d'exploitation. Vous le trouverez sur <http://lynx.browser.org>. Ceux qui ont Mac OSX peuvent l'installer facilement par le biais de Fink (<http://fink.sf.net>).



▲ Au bas du site <http://leslie.harbold.com> vous trouverez cette barre de navigation graphique qui est une image map.

Apercevoir dans lynx une page Web contenant une image map avec tous les textes **ALT** à leur place est un réel

```

<map name="Map">
<area alt="previously..." shape="rect" coords="203,114,258,129? href="/archives.html">
<area alt="by category" shape="rect" coords="277,113,348,129? href="/category/">
<area alt="about the site" shape="rect" coords="364,113,401,128? href="links.html">
<area alt="about leslie" shape="rect" coords="418,114,488,130? href="leslie.html">
<area alt="Powered by Movable Type" shape="rect" coords="-4,190,131,210? href="http://
www.moveabletype.org">
</map>
```

plaisir. Essayez de les trouver dans le Réseau... cette recherche vous permettra ainsi de mieux comprendre nos explications données à travers ces pages...

:: Ce qu'il ne faut pas faire

Quoi de plus beau et de plus gratifiant que de parvenir à appliquer ses connaissances fraîchement acquises et d'être capable de tenter de nouvelles expériences. Si ensuite, vous parvenez même à atteindre un niveau supérieur, en passant d'un cadre client à un cadre "serveur", votre satisfaction ne pourra être qu'au beau fixe. Cependant, attention à ne pas trop en faire !

On éprouve un certain sentiment de puissance lorsqu'on écrit des images maps conçues pour une utilisation dans le cadre d'un serveur, où les informations cliquables proviennent du serveur et non de la page. Mettez en revanche l'ensemble du code utile dans la page. Sinon lynx pourrait avoir des problèmes et les logiciels qui aident les gens plus ou moins habiles, des ennuis bien plus graves !

Le web, c'est fantastique lorsqu'on pense à tous !

P. Greco
pgreco@hackerjournal.it

Attention !

Ce symbole indique que le code a été renvoyé à la ligne pour des exigences graphiques. La chaîne doit être considérée dans son ensemble.

JE TE VOIS ET JE NE TE VOIS PAS...

Si nous téléchargeons avec Lynx le site <http://leslie.harpold.com/> et que son auteur n'avait pas codifié l'image map comme il se doit, on ne verrait alors que l'élément suivant à la place des liens en bas de page :

```
[USEMAP:hpfooter.gif]
```

Suivre ce lien conduirait à une page listant tous les liens dans l'image map. Si les textes **alt**, étaient absents, on ne verrait que les URL, qui pourraient être explicatifs ou non :

```
[USEMAP:hpfooter.gif]
```

```
MAP: http://leslie.harpold.com/#Map
```

1. <http://leslie.harpold.com/archives.html>
2. <http://leslie.harpold.com/category/>
3. <http://leslie.harpold.com/links.html>
4. <http://leslie.harpold.com/leslie.html>
5. <http://www.moveabletype.org>

En revanche, en mettant toutes les bonnes codifications à leur place et tous les textes **alt** pour chaque lien et pour l'image, on parvient à un lien écrit en langage naturel : **Site navigation links**. Lequel conduit à des liens également écrits en langage naturel et compréhensible de tous, anglais mis à part, ce qui facilite bien sûr la navigation, tout en étant plus élégant et beaucoup plus "hackeristique".

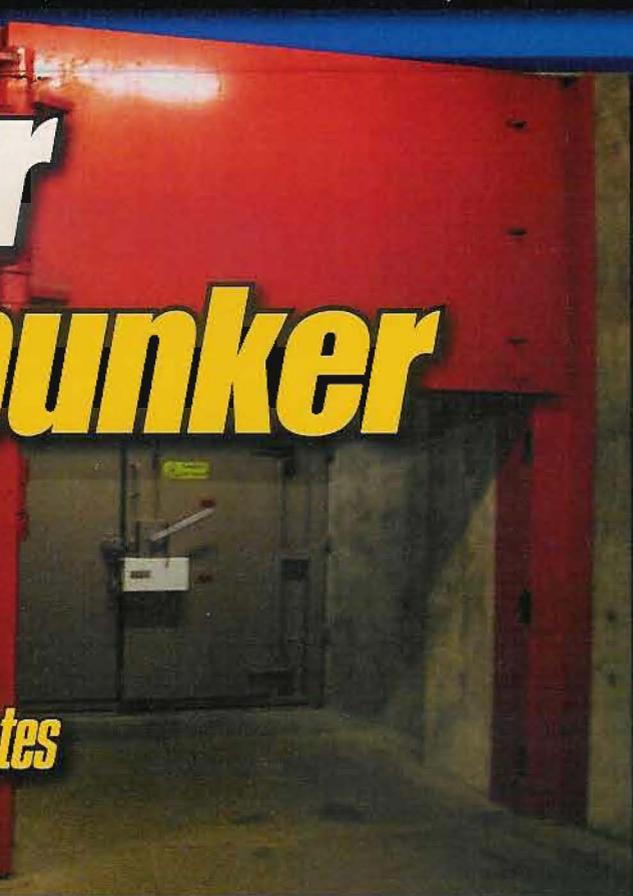
```
Site navigation links
```

```
MAP: http://leslie.harpold.com/#Map
```

1. previously...
2. by category
3. about the site
4. about leslie
5. Powered by Movable Type

Un hacker dans un bunker

Nous avons pénétré dans une enceinte haute sécurité, un abri antiatomique où sont conservées les informations les plus importantes et les plus confidentielles !



Nous y sommes parvenus seuls. Nous avons franchi les barrières de béton avec leurs fils barbelés, passé les patrouilles de garde avec leurs viseurs nocturnes et leurs chiens policiers, pour nous retrouver à présent dans un lieu incroyable, équipé de technologies avant-gardistes à même de protéger les informations les plus confidentielles qui soient, où chaque mur est ici synonyme de sécurité. Hacker News Magazine est entré dans ce Bunker. Voici ce que nous y avons vu.

:: A l'intérieur de la forteresse

Ce Bunker se trouve à Marshborough Road, sur une route du Kent, au cœur de la campagne anglaise, bordée de pâturages avec ses murets de pierres, ses églises normandes et ses pubs. Mais on ne peut certes pas parler d'un édifice à l'aspect bucolique, bien au contraire ! Il s'agit-là d'une fortification militaire, un bâtiment créé en pleine guerre froide pour abriter les nœuds de communication de la Grande-Bretagne en cas de conflit. Ou, pour être plus

précis en cas de conflit atomique. A l'origine, ce Bunker avait en effet été conçu pour résister à une explosion nucléaire qui se produirait dans les environs. Il est devenu aujourd'hui une sorte de coffre-fort où sont conservés dans une sécurité absolue, données, informations, systèmes informatiques et hardwares. The Bunker : tel est le nom de l'entreprise qui gère cette structure. Une société très discrète mais sûre d'elle, au point de nous avoir invités au cœur même de son royaume et ce, pour prouver qu'elle ne craignait nulle intrusion.

:: Le plus beau reste... dissimulé !

Le Bunker est une formidable structure qui n'est pas sans rappeler la forme d'un iceberg... la partie visible dégage à elle seule une certaine puissance, tandis que la partie cachée est encore plus impressionnante. Nous ne pourrions malheureusement pas divulguer une bonne partie de ses secrets, les dirigeants ne nous ayant pas autorisés à prendre des photos des systèmes hardwares utilisés, des ordinateurs présents, et des batteries de serveurs... Domma-

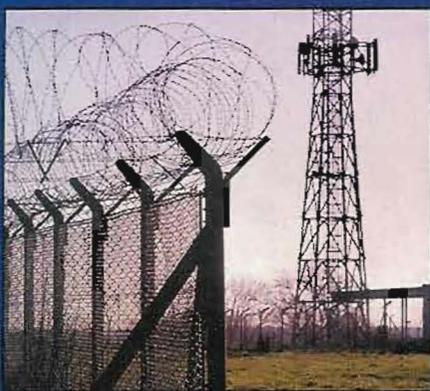
A QUOI A SERT ?

La société des Laurie est composée de cinq éléments.

Un endroit totalement unique : un réseau de bunkers militaires implanté dans une région urbaine à faible niveau de risque. Une réputation et une renommée mondiale, et ce, sans la moindre publicité, totalement inutile. «On ne parle jamais du Bunker dans les journaux, car il n'arrive jamais rien». Une

approche spécialisée et hautement qualifiée, une capacité multi plate-forme pratiquement universelle et un personnel qui fait preuve de capacités innovantes et d'une polyvalence sans égal.

Bien sûr, les honoraires du Bunker sont proportionnels à la qualité des services proposés : www.thebunker.net.



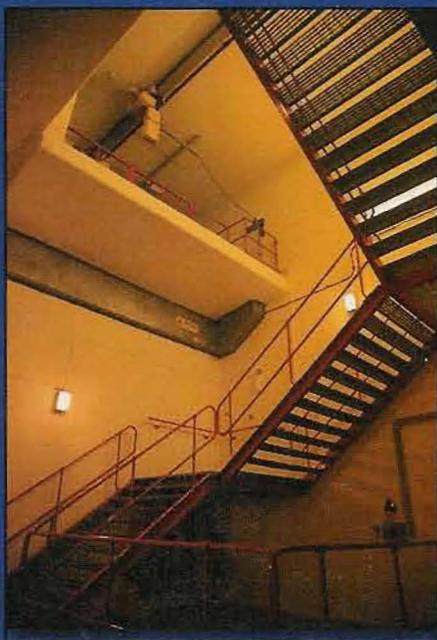
▲ *La surveillance extérieure est assurée par des détecteurs de mouvement, des caméras vidéo, des patrouilles de surveillance et des chiens policiers.*

ge ! Nous avons été conduits au-delà de lourdes portes, où nous avons descendu de longs escaliers métalliques et d'autres en béton armé et ce, jusqu'à 30 mètres de profondeur, dans des pièces totalement scellées, à l'épreuve de toute intrusion, quelle qu'elle soit. Nous avons franchi des barrières et des zones de sécurité jusqu'à atteindre le cerveau du Bunker, une petite salle de réunion où nous avons pu nous entretenir avec Ben et Adam Laurie, les fondateurs de cette incroyable société. Ils nous ont dressé un panorama pour le moins intéressant des services proposés par le Bunker.

:: Services haute sécurité

L'agence des frères Laurie propose différents types de services, tous axés sur la sécurité. Parmi ceux-ci, nous trouvons le Secure Hosting de données et informations, l'extension de services de firewall aux clients sans oublier la gestion correspondante du pack de sécurité, optimisé pour répondre aux exigences de ses utilisateurs, la création de réseaux virtuels privés, spécialement conçus à partir des demandes des clients, et sécurisés par le personnel du Bunker, qui fait de la défense anti-intrusion et de la sécurité une affaire personnelle. Parmi les différentes offres du Bunker, on trouve la «co-location de systèmes. Cela signifie qu'à l'instar d'un coffre-fort, les clients peuvent décider de faire installer leurs propres systèmes hardware à l'intérieur de cette forteresse, où ils seront physiquement en sûreté contre tout type d'infiltration physique ou tout accident. Toute éventuelle communication, de et vers ces systèmes, pourra être ultérieurement sé-

curisée par l'équipe de l'agence : un véritable service de défense. Dernier service proposé et non des moindres : le Disaster Recovery, à savoir la sauvegarde des données et la continuité de l'exercice en cours pour toute société ou entreprise qui en fait la demande. Ce service peut prévoir la récupération complète des données perdues ou détruites d'une grande entreprise, suite à tout type d'événement ou catastrophe (sans aucune exception : on nous a donné des exemples de destructions de données par des pirates et autres hackers, pannes de systèmes mais aussi incendies, tremblements de terre et même ...une explosion nucléaire ! Certes, si le désastre est de grande ampleur, le client doit lui aussi pouvoir se permettre le luxe de récupérer certaines



▲ *Le cœur même du Bunker se trouve à environ trente mètres de profondeur : les données conservées peuvent également survivre à l'explosion d'une petite bombe nucléaire, à condition de ne pas se trouver juste en dessous !*

informations et disposer encore d'intérêts après la catastrophe...).

:: Pourquoi tant de sécurité ?

Mais aussi forte soit une armure, il existera toujours une arme pour la transpercer. Il n'existe pas de défense parfaite et l'agence des frères Laurie ne pourrait pas réellement résister à une

DES HACKERS COMME NOUS

Le Bunker accueille également des conférences sur la sécurité, les failles des systèmes informatiques et les actions susceptibles d'être lancées par des pirates. Qui assure ces conférences ? Les frères Laurie, bien sûr ! Au cours de l'une d'elles, les frères ont expliqué comment un hacker, après avoir pénétré le système de surveillance en circuit fermé d'un hôtel, avait trouvé des informations confidentielles comme des codes de sécurité et des données personnelles. Comment sait-il tout cela ? Facile ! Dans sa jeunesse, Adam Laurie s'est adonné à ces activités et nous lui devons la découverte de l'une des plus graves failles de sécurité du système Bluetooth... Cela fait de nombreuses années que les Laurie tiennent des séminaires de sécurité basés sur leurs propres expériences personnelles.

véritable attaque atomique (bien que les rampes de serveurs soient situées dans une zone souterraine totalement blindée, par le biais également de boutons électromagnétiques avec l'assurance de sauvegarder les données même en cas d'explosion nucléaire. L'idée ne semble donc pas si farfelue que ça...). Mais ce qu'il y a de plus efficace, c'est encore l'esprit qui se cache derrière ces défenses. S'il est attentif, préparé et curieux, alors il sera en mesure non seulement de repousser la quasi-totalité des attaques mais aussi et surtout de les prévenir ! Et ça, nous savons le faire, pas vrai ? Eh bien, les frères Laurie savent eux aussi le faire ! Leur personnel a été formé à cet égard et vous seriez étonnés de savoir que bon nombre d'entre eux a un passé de «hacker» pur et dur. Car il n'y a pas que des professionnels en costume cravate. On y trouve aussi certaines personnes qui, avant d'occuper ces postes, passaient leur temps à essayer de changer le monde... avec les mêmes outils que nous. Il y a ensuite les frères Laurie dont on retiendra une ancienne carrière de hacker. Bref, ce Bunker nous a impressionnés. L'idée de base de cette activité commerciale est très intéressante et toutes ces tonnes de béton armé et de terre cachent une concentration de technologie et d'idées innovantes comme on n'en voit pas beaucoup.

VIEUX MAIS REDOUTABLE !

*Le vieux Sasser continue à faire des victimes :
Etudions ce chef-d'œuvre de l'ingénierie virale !*

Plusieurs années se sont écoulées depuis sa première apparition, pourtant Sasser continue à faire des ravages. Il fonctionne, et comment ! Il s'agit d'un ver doté d'une intelligence qui exploite des failles de Windows et devient vraiment terrifiant si votre système d'exploitation n'est pas bien mis à jour et défendu. Voyons maintenant pourquoi.

◀ *Semplice ed efficace,
Sasser continua a far paura*

26 AÛT
2006

Salut !
Je m'appelle ***** !
J'ai attrapé plusieurs fois le virus Sasser 2004 ! Je n'ai jamais fait de mise à jour de Windows tout en ayant la licence originale !
Que puis-je faire ?

Le principe de Sasser consiste à modifier certaines parties de la configuration du système, en compliquant ainsi l'installation de mises à jour ou de programmes pour le retirer. Avant de pouvoir utiliser un programme spécifique, mieux vaut retrousser ses manches. Au bout du compte, il s'agit d'un vrai travail de hacker...

:: Diagnostics et symptômes

Sasser exploite une faille d'un composant de Windows nommé LSASS.EXE. Le symptôme d'infection le plus courant se traduit par l'apparition d'un message sur l'ordinateur qui déclare avoir détecté un problème, et qu'il redémarrera dans 60 secondes. Si vous le laissez faire, il continue de redémarrer votre ordinateur toutes les minutes et ce, à l'infini. Vous devez l'arrêter.

:: Fermeture rapide

Vous avez 60 secondes. Vous devez cliquer sur le bouton Démarrer

27 JUILLET
2006

Il m'arrive une chose que j'ai déjà subie il y a bien longtemps sur mon ordinateur...

Lorsque je le démarre, il s'éteint directement ou avec un avertissement qui dure quelques secondes et que je ne parviens pas à lire sur un exe, isass.exe ou lsass.exe ... A l'époque, j'avais scanné le disque dur avec Norton 2005, Spybot et Ad-ware via Internet et aucune menace n'avait été détectée... Au final, j'ai tout reformaté...

Aujourd'hui, je suis à nouveau confronté aux mêmes symptômes. J'ai passé Norton 2006 qui n'a détecté aucune menace... A votre avis, qu'est-ce ça peut bien être ?

puis Exécuter. Dans la fenêtre de texte, tapez `shutdown -a`. Ce qui signifie : "ferme tout immédiatement et ne tient pas compte du redémarrage programmé". Vous n'avez rien réparé, mais vous avez arrêté l'action de Sasser. Vous

pouvez préparer dès à présent les contre-mesures. Démarrez votre ordinateur. Sasser devrait rester inactif. Dans le cas contraire, il ne vous reste plus qu'à rebooter votre ordinateur avec un CD-ROM ou à partir d'un disque externe, ou encore d'une clé USB. Dans tous les cas, utilisez toute méthode qui fonctionne et lancez un antivirus. Sinon, vous pouvez poursuivre.

Ouvrez le fichier `\windows\system32\drivers\etc\hosts`

dans le Bloc-Notes. Il devrait contenir une seule ligne, contenant à son tour la mention `localhost`. Si en revanche plusieurs lignes apparaissent et que vous voyez les noms des fabricants typiques d'antivirus, comme Symantec, McAfee etc., le virus a alors frappé.

:: Nettoyez votre ordinateur

Fermez le Bloc-Notes. Ouvrez Windows Explorer dans le dossier qui contient le fichier `hosts`. L'un des nombreux systèmes consiste à cliquer sur Démarrer, Exécuter et à écrire

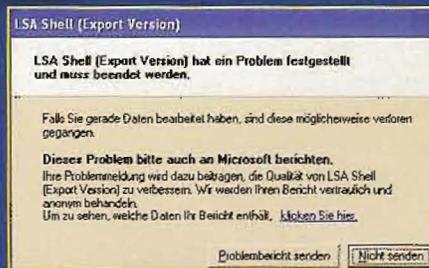
`\windows\system32\drivers\etc`

CEUX QUI N'ONT RIEN A VOIR !

Eh, non ! Vous n'avez pas forcément attrapé Sasser. Des symptômes identiques pourraient bien provenir d'un autre ver, virus ou autre. Voici une liste de systèmes qui ne peuvent pas être infectés par Sasser :

- Windows XP 64-Bit Edition version 2003
- Windows Server 2003
- Windows XP 64-Bit Edition SP1
- Windows Millennium Edition
- Windows 98 Seconde Edition
- Windows 98
- Windows NT 4.0 Service Pack 6a
- Les systèmes suivants peuvent être en revanche frappés par Sasser, s'ils ne sont pas mis à jour :
- Windows XP
- Windows XP Service Pack 1 (SP1)
- Windows 2000 SP2
- Windows 2000 SP3
- Windows 2000 SP4

puis à appuyer sur Entrée. Cliquez avec le bouton droit sur l'icône du fichier `hosts` et sélectionnez la commande Renommer. Donnez-lui un autre nom, par exemple ancien `host`. Retournez à nouveau sur Démarrer -> Exécuter et tapez la commande `netstat -R` et appuyez sur Entrée. Cette commande devrait forcer Windows à réinstaller les éléments et à créer un nouveau fichier `hosts` nettoyé.



▲ Les messages à travers lesquels Sasser vous informe que votre système est désormais infecté, sont toujours inquiétants : agissez très rapidement !

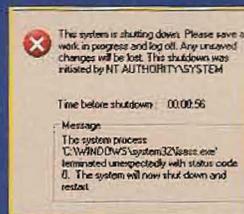
: Installez-le définitivement

Maintenant, vous devriez pouvoir utiliser votre ordinateur pour vous connecter à Internet et accéder aux bons sites. Avant tout : installez un pare-feu ! Si vous n'en avez pas, il est important d'en installer un. Vous pouvez utiliser le pare-feu de Windows ou un produit extérieur, par exemple ZoneAlarm, dont vous pouvez télécharger une version gratuite sur <http://snipurl.com/61s>. Allez sur le site de Microsoft, à la page <http://snipurl.com/mewq>. Vous y trouverez toutes les informations nécessaires, les programmes à télécharger pour se débarrasser définitivement de Sasser et de toutes ses



▲ Sven Jaschan, le créateur de Sasser

◀ Le système s'éteint dans les 60 secondes : si vous le laissez faire, Sasser s'y introduira et il vous sera beaucoup plus difficile de le retirer



LA PAGE DÉFINITIVE

Sasser est un virus qui ne date pas d'aujourd'hui puisqu'il a presque deux ans et demi. Par conséquent, on sait absolument tout de lui. Vous trouverez le meilleur résumé sur ce ver sur le site de Microsoft à l'adresse suivante : <http://snipurl.com/xi2j>. Vous y trouverez également les liens pour accéder aux descriptions de toutes les variantes du ver ainsi qu'une procédure manuelle alternative à celle que nous avons publiée. Si vous rencontrez des problèmes avec une procédure, vous pouvez essayer l'autre !



variantes. Avant de pouvoir utiliser les programmes de suppression du ver, la plupart du temps, il est nécessaire d'installer une ou plusieurs mises à jour de Windows. La page que nous vous avons indiquée contient également les bons liens. Une fois l'opération achevée, vous devrez absolument penser à vous procurer également un bon antivirus.

Car bien sûr, on ne peut pas savoir si Sasser restera toujours le même : il pourrait changer, muter, devenir une menace différente et plus fatale. Et puis... Il y a toujours d'autres virus auxquels vous serez confrontés, pas vrai ?

Comme antivirus... Il en existe un par exemple open source valable pour tous les systèmes existants : Clam AntiVirus (<http://www.clamav.net>). Il a été créé pour

Linux, mais la page de téléchargement contient également les fichiers exécutables pour Windows et pour Mac OS X, avec beaucoup d'autres systèmes. Et comme d'habitude, nous ne cesserons jamais de vous répéter que Windows doit être mis à jour et protégé avec davantage d'attention que d'autres systèmes.

Nyarlatotep
Le chaos rampant
nyarlatotep@hackerjournal.it

ATTAQUE EMPOISONNÉE

Il existe une attaque très efficace, capable d'anéantir quiconque : l'empoisonnement du DNS qui détourne le trafic de données.



La technique de l'empoisonnement du DNS se traduit par une attaque portée directement à la mémoire cache du DNS.

Cette attaque permet de déplacer l'ensemble du trafic de données relatif au site attaqué, sur un espace en réseau sous contrôle de l'agresseur. Il s'agit d'un véritable détournement. D'un rapt. Bref, d'une action criminelle. L'empoisonnement du DNS (DNS Poisoning, pour ceux qui baragouinent quelques mots d'anglais) n'est certes pas une nouveauté en soi : c'est même une technique plutôt ancienne. Pourtant, elle continue de fonctionner. Voyons comment...

PRÉVENTION !

De nombreuses attaques d'empoisonnement de la mémoire cache peuvent être évitées par les serveurs DNS à condition que ces derniers soient un peu plus méfiant quant aux informations envoyées par d'autres serveurs DNS. Peut-être même en ignorant les enregistrements de DNS reçus, qui ne sont pas directement liés à la demande (une bonne méthode pour écarter les attaques de reconnaissance !). Par exemple, les nouvelles versions de BIND contiennent désormais un script qui effectue ces contrôles. Par conséquent, mener ce genre d'attaque – toujours de mise – pourrait s'avérer un peu plus difficile.

:: Spoofing o Poisoning ?

Le DNS spoofing remplace le champ IP de la réponse envoyée au client par un service DNS. Il s'agit de la réponse au client qui a demandé la conversion d'un nom symbolique en adresse IP. Le spoofing est possible si vous avez installé un programme capable de "sniffer" les données du client et de modifier la réponse du DNS. Ainsi, le client se connectera, non pas avec sa véritable adresse IP, mais plutôt avec l'IP de celui qui attaque.

Le DNS poisoning survient également sans avoir le compte administrateur du serveur DNS (celui qui convertit des noms symboliques en adresse IP). Et ce, dans la mesure où celui qui agresse empoisonne depuis un accès distant la mémoire cache du DNS. Si le DNS contient les IP de référence au domaine en question, l'agresseur peut trouver tous les IP en les demandant à bon nombre de services online disponibles (bien que cela laisse une trace qui pourrait être utilisée à l'avenir). Si le DNS est d'un autre type, à savoir non "autoritaire", alors il ne possède pas tous les IP, mais uniquement celui spécifique, au sein de sa propre mémoire cache. Dès lors, après avoir reçu la demande explicite, l'IP sera directement envoyé à l'agresseur.

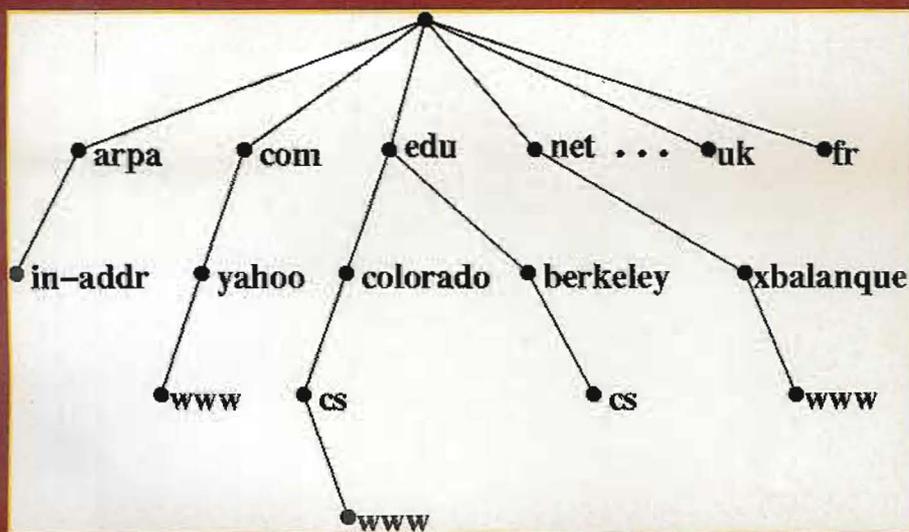
Il peut toutefois arriver que le DNS ne soit pas "autoritaire" pour le domaine

demandé, et qu'il ne le conserve pas non plus dans la mémoire cache ! Le DNS pourrait lui envoyer la demande à un niveau supérieur, jusqu'à ce qu'il atteigne un DNS autoritaire de système



▲ Une fois le DNS empoisonné, vous pouvez détourner toutes les données ! Un véritable coup mortel !

qui répondra directement à l'utilisateur. Comme solution alternative, on pourrait créer une connexion directe entre le host de l'utilisateur et les DNS mis en cause. Ce sera ensuite à l'utilisateur de faire la demande au DNS du système.



▲ La base de données répartie des DNS... Une fois le chemin connu, l'attaque est plus facile

:: Technique d'empoisonnement



▲ Il semble que l'empoisonnement du DNS d'Al-Jazeera ait été l'une des armes utilisées pour "libérer l'Irak"

Voici une procédure efficace.

Après avoir choisi sa cible, l'agresseur doit se procurer l'accès à un serveur : il y détournera le trafic de sa victime.

Cela peut se produire en trompant le serveur DNS autoritaire des domaines, de façon à lui faire croire qu'il est le serveur autoritaire du domaine attaqué.

On y parvient en lui envoyant une fausse réponse avec l'IP du serveur de support pour l'attaque.

La fausse réponse se crée si l'on possède l'ID de la demande du DNS autoritaire des domaines, si la réponse arrive avant celle du véritable DNS et si le DNS du système ne possède pas en mémoire cache le domaine attaqué : un pur hasard !

:: Il suffit d'attendre

L'ID header des paquets UDP utilisés dans la communication des serveurs DNS constitue la seule véritable forme de sécurité du software qui contrôle tout cet ensemble. Le fait est que les réponses d'un serveur doivent avoir le même ID que celui qui fait la demande. Avec les nouvelles implémentations du logiciel, on a tenté de combler la faille de la prévisibilité des numéros IP : il n'y a pas de numéros réellement aléatoires car même les programmes de génération utilisent des algorithmes fixes et le processus pourrait donc être déductible !

Si l'agresseur devait adopter une techni-



▲ Trouver la réponse du DNS qui nous est utile, revient à chercher une aiguille dans une botte de foin !

que offensive réellement efficace, il lancerait alors de nombreuses tentatives d'attaque. La véritable tragédie se traduit par le fait que nous pouvons envoyer n'importe quel nombre de demandes au DNS autoritaire des domaines, car celui-ci générera un nombre égal de réponses... bref, ce n'est qu'une question de temps !

:: Le poison a agi

Une fois l'ID trouvé, le tour est joué. Le trafic est détourné. Celui qui administre le domaine touché, se demande ce qui s'est réellement passé.

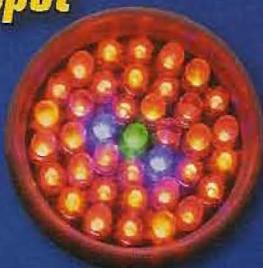
Les données s'échappent et défilent dans le serveur pendant un laps de temps déterminé par l'agresseur ou jusqu'à ce que le problème soit découvert et résolu mais entre temps... entre temps le poison a agi ! Attention, toutefois car il s'agit d'un véritable délit.

BIND ?

Bind est un programme standard. Il s'agit pratiquement du serveur DNS le plus utilisé sur Internet et son nom signifie Nom de Domaine Internet Berkeley (à savoir Berkeley Internet Name Domain : Bind). Il est soutenu par l'Internet Systems Consortium et avait été créé à l'origine par quatre étudiants de l'Université de Berkeley. Actuellement, la version 9 du programme est disponible, conçue pour résoudre les problèmes des précédentes versions : des versions qui "incitaient" quasiment à l'empoisonnement du DNS !

Et la lumière fut !

Voici comment créer un spot polychrome dernier cri en utilisant un groupe de diodes



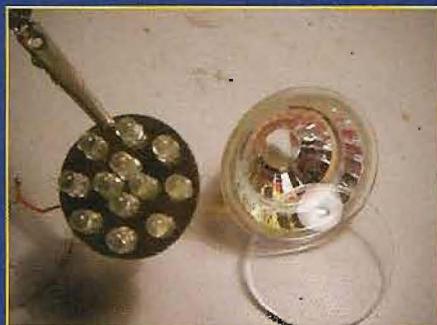
MATERIEL :

Ampoule à 12 diodes blanches, 12 000 mcd (millicandela), 12 Vac ; une douille classique de fixation Edison ou un bout de tube équivalent ; un câble, un interrupteur basculant et une batterie rechargeable 12 V.

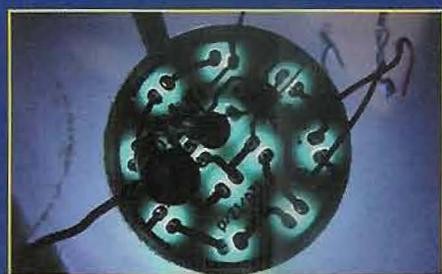
C'est auprès d'un revendeur de matériel électrique que nous avons trouvé une ampoule à diodes de 12 000 millicandela, excellente alternative aux ampoules halogènes des spots classiques de 12 volts qui se montent dans les étagères, faux plafonds ou autres endroits similaires. Nous en avons acheté une qui nous est revenue à un peu plus de 7 euros, même s'il est écrit sur la boîte qu'elle peut être alimentée à 12 Vac, c'est-à-dire avec une tension alternative de 12 volts. Parfaite justement pour remplacer un spot halogène. Moins adaptée en revan-

che à une alimentation par batterie, même si elle fournit la même tension en courant continu. Bien sûr incompatible dans sa configuration d'origine. Mais quel hacker ferions-nous, si un rien nous effrayait ? Seules nous intéressent la partie en forme d'entonnoir et ses diodes, à savoir la partie d'orientation du faisceau lumineux. La fixation ne nous sera pas utile. Procédons donc au démontage du spot en partant donc de cette fixation. Certes, c'est plus facile à dire qu'à fai-

tits coups bien placés et un peu d'attention, on parvient à supprimer totalement la partie des deux contacts électriques. Ces derniers s'enlèvent en effet et révèlent le contenu du spot : un circuit imprimé avec un peu d'électronique et bien sûr les 12 diodes. Pour comprendre son fonctionnement et modifier l'ensemble de sorte qu'il réponde bien à nos objectifs, surtout à notre alimentation, nous devons toutefois le démonter davantage. Le seul système consiste à retirer, sans le cas-



▲Voici le résultat : nous avons extrait la partie électronique et gardé le réflecteur et le verre.



▲L'intérieur est également composé d'électronique. Cherchons à l'aide d'une batterie externe les deux pôles d'alimentation qui permettent d'allumer l'ensemble.



▲Nouveau spot : un marteau et un tournevis vous aideront à casser le culot

re ! Le spot est un bloc de verre et la fixation est noyée dans un matériau qui ressemble à un petit morceau de céramique ou de résine très dure. C'est avec la plus grande attention que nous bloquons le spot dans un étau. Nous mettons des lunettes de protection, et à l'aide d'un marteau et d'un tournevis, nous donnons de légers coups secs de marteau dans la zone la plus étroite de la fixation du spot, à savoir sur la partie arrière. Le verre commence à se briser et il est facile de comprendre à cet instant qu'avec de pe-

ser, le verre situé au-dessus des diodes et à faire sortir ces diodes et la partie électronique justement par l'ouverture la plus large, vers le haut. A l'aide d'un tournevis très fin et à lame plate, nous essayons de soulever le petit verre de devant. Après de nombreuses tentatives à plusieurs endroits différents, celui-ci se détache enfin sans la moindre rayure. Nous pouvons dès lors sortir le circuit en toute liberté. Nous nous aidons pour cela du même petit tournevis pour le pousser par l'arrière. Et voilà ! Le tour est joué

(ou d'une batterie) sur deux points que nous devons déterminer en observant bien le circuit imprimé. Les pistes les plus larges sont à vue d'œil la masse (pôle négatif) et un autre point de soudure plus isolé (le pôle positif). Voici une astuce pour le trouver facile-



▲ *Assemblons le tout avec une colle forte bi-composant et le voilà fini, prêt à diffuser une lumière froide !*

ment : effectuer quelques essais avec le pôle positif de notre alimentation. Soudain, les diodes s'allument de tout leur éclat ! Par curiosité, nous mettons entre l'alimentation et le circuit un testeur sur la position ampèremètre en série. C'est alors que la magie de l'alimentation à courant continu opère : la



▲ *Des composants électroniques sont utilisés même pour allumer quelques diodes !*

consommation totale est d'environ 20 mA ! Ok, il ne nous reste plus qu'à souder deux fils au circuit imprimé, remonter le tout, bien placer les fils et diodes dans le logement de la petite parabole et refermer avec le ver-



▲ *Etudier sa composition est toujours intéressant et très... hacking.*

re que nous collons avec quelques petites gouttes de colle époxydique bi-composant (nous n'utilisons pas l'attack, qui produit des vapeurs qui assombrissent le verre). Nous scellons également l'arrière et passons à la suite.



▲ *La partie la plus critique consiste à casser uniquement le culot du verre. On y parvient à l'aide d'une pince, d'un tournevis et d'un marteau (et d'une paire de lunettes de protection). però a scassare tutto... solo quanto basta.*

:: Montage

Nous prenons une douille classique et retirons la partie interne qui sert normalement à visser l'ampoule, en laissant le fond et le reste du tube.

Nous élargissons légèrement le trou au niveau du fond pour l'adapter aux dimensions de l'interrupteur basculant. Nous fixons bien l'interrupteur et y soudons un fil provenant de la base.

Nous réalisons ensuite un autre orifice sur la paroi de la douille par lequel nous faisons sortir les deux fils de l'alimentation, de la longueur souhaitée afin qu'ils puis-



▲ *Surprenant, n'est-ce pas ?*

sent rejoindre la batterie. Nous avons même utilisé une petite batterie au plomb de 12 volts, mais tout autre kit de batteries dont la tension est de 12 volts pourra faire l'affaire. A vous de jouer maintenant !

Standard Bus
standardbus@gmail.com

:: Modification du système électronique



▲ *Quelle batterie utiliser ? Aucun problème dans la mesure où la consommation n'atteint même pas 20 mA.*

Le système électronique est constitué principalement d'un pont de diodes redresseuses et d'un circuit intégré régulateur LM723, apparemment connecté de façon à maintenir un courant continu. Tout en tenant le circuit entre les pinces d'un support de "troisième main", nous appliquons du 12 volts en courant continu par le biais d'une alimentation



▲ *Plaçons l'interrupteur dans le fond d'une douille et connectons les fils d'alimentation.*



Window sVista

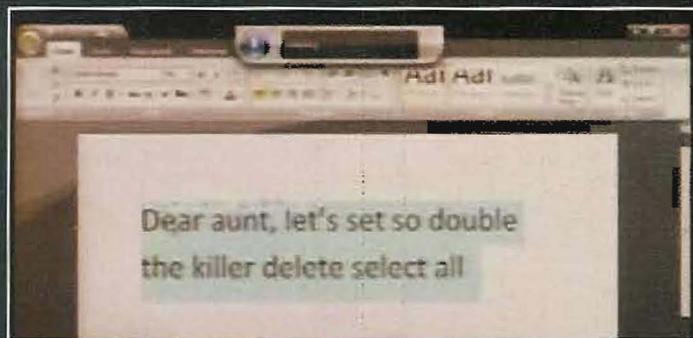


CHERE MAMAN OU CHERE TANTE ?

Pauvre, pauvre Microsoft ! Non seulement, ce sVista lui en fait vraiment voir de toutes les couleurs, mais pour couronner le tout, il n'est toujours pas prêt ! La toute dernière tragédie en date a eu lieu lors d'une présentation des fonctions de reconnaissance vocale, intégrées au futur remplaçant de Windows XP.

Que s'est-il passé ? Un démonstrateur était en train de dicter une lettre lorsqu'au lieu de «Chère maman», le système a compris et écrit «Chère tante». Le démonstrateur a alors tenté de corriger le problème à l'aide des fonctions de correction, toujours vocales. Résultat ? Une phrase totalement absurde et incompréhensible.

Microsoft a imputé ce problème à un bruit de fond imperceptible qui aurait perturbé la dite expérience, tout en reconnaissant ensuite la présence de problèmes dans le sous-système audio. Des problèmes qui auraient empêché au moteur d'analyse vocale de contrôler l'entrée des commandes audio... un véritable désastre !



Vous pouvez voir cette démonstration hilarante de sVista sur <http://video.google.com/videoplay?docid=1123221217782777472>. Certains petits malins se sont immédiatement emparés de la merveilleuse phrase créée par sVista pour en faire un tee-shirt. Nous pensons en acheter pour toute la rédaction...

Sur <https://www.spreadshirt.com/shop.php?sid=4086>, vous pouvez acheter les tee-shirts commémoratifs de cet incroyable événement !

Let's set so double
the killer delete
select all

A l'adresse <https://www.spreadshirt.com/shop.php?sid=4086>, nous pouvons acheter les tee-shirts commémoratifs de cet incroyable événement!