N°7 MAI - JUIN **EXCLUSIF : GAGNEZ AU LOTO PAGE 55**

PIRAT'Z

HACKERS & GAMERS

1,9€

LECHATKITU

PIRATER 50 ORDIS EN 5 MINUTES

Divx max kalité • BOSS DU TCHAT

P2P ATOMIK • CRACKING PRO

CONSOLES : PS2 CHIPS, TRICHEZ SUR TOUT

SVCD : le DVD-R à 50cent

AVANT-GARDE

Y'a pas à dire, ce nouveau numéro de Pirat'z , c'est l'avant-garde. Les projets extraordinaires et les nouvelles technologies prometteuses sont là, sur le Net. Les gens ne développent plus leur shareware seuls dans leur coin, c'est terminé. Maintenant, les efforts sont communautaires, et les projets ouverts, libres. Mais cette ébullition a le désavantage de noyer les vraies perles dans une masse d'idées parfois douteuses, qui n'aboutissent pas toujours.

Pourtant nous veillons ! Dans ce numéro, nous vous présentons deux logiciels libres qui renversent le principe du P2P : iRate Radio et Konspire2b. Le second, surtout, ouvre de nouvelles possibilités de diffusion en masse sur le Net, en introduisant une forte notion de confiance jusqu'alors inconnue dans le monde du partage de fichiers. Nous y croyons. Et si vous jouez le jeu, nous diffuserons du matos qui vous ravira par ce canal. Surveillez notre site internet, et notre forum (qui finira bien par fonctionner correctement...).

La deuxième technologie que nous voulions vous faire découvrir, c'est le format Matroska, et les codecs vidéo dernier cri. À ce qu'on observe dans les milieux non autorisés, les gens sont restés prisonniers des antiques formats divx, moins efficaces, moins beaux, moins confortables. Il est temps de bouger les amis, et de se renseigner (qu'on lise Pirat'z au petit déjeuner !).

À part ça, on vous sert une bonne dose de hack de premier choix, toujours grâce à l'équipe de Espionet.com. Attention, le niveau monte un peu. Mais nous vous faisons confiance et savons que vous serez persévérants s'il le faut. Bien sûr, n'hésitez pas à nous poser des questions.

DE BAZANDE
http://piratz.fr.st

SOMMAIRE

http://piratz.fr.st

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, Captain Cavern

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

LE VIRUS RUSÉ QUI FAIT SA LOI

Généralement, un virus, c'est maaal, c'est méchant, et ça ne cause que des ennuis. Mais parfois, certains virus sont créés dans un but un peu plus glorieux que juste "écraser quelques fichiers capitaux au hasard". C'est le cas du virus NetSky, dont les premières variantes étaient destinées à... éliminer le ver Blaster ainsi que quelques autres virus. Une sorte d'"antivirus" se propageant à la manière des virus, quoi. Mais la dernière variante de ce virus (NetSky-Q) va encore plus loin : elle s'attaque au piratage, en mettant en place une attaque de déni de service contre les sites de Kazaa, eDonkey et eMule, tout simplement (ainsi que d'autres sites reliés au piratage, comme des sites de cracks). Vers la mi-avril, tous les PC infectés devraient donc flooder ces sites, ce qui risque fort de les désactiver temporairement si le virus s'est suffisamment répandu sur le Net. L'auteur de cette variante du virus reste inconnu, mais certaines rumeurs laisseraient entendre que son nom finirait par "AA"... Je vous laisse deviner les suspects potentiels.

http://www.espionet.com

LES LOIS ANTI-PIRATAGE

Apprentis pirates, attention ! En France, la loi réprime sévèrement toutes les formes d'attaque. Les articles 323-1 à 323-7 du code pénal répriment par des peines jusqu'à 3 ans d'emprisonnement et 45 000 Euros d'amende l'accès ou le maintien frauduleux dans un système informatique, ainsi que l'entrave volontaire au fonctionnement d'un système informatique. Et n'oubliez pas que la simple tentative, même si vous échouez lamentablement, est punie des mêmes peines.

EN FRANCE

COMMENT PIRATER 50 ORDIS EN 5 MINUTES ?

AVEC 2 DOIGTS ET AUTANT DE NEURONES

Vous allez voir à quel point il est encore simple, de nos jours, de pénétrer des centaines d'ordis en quelques clics... Nous allons utiliser pour cela les failles Netbios et VNC.

NETBIOS

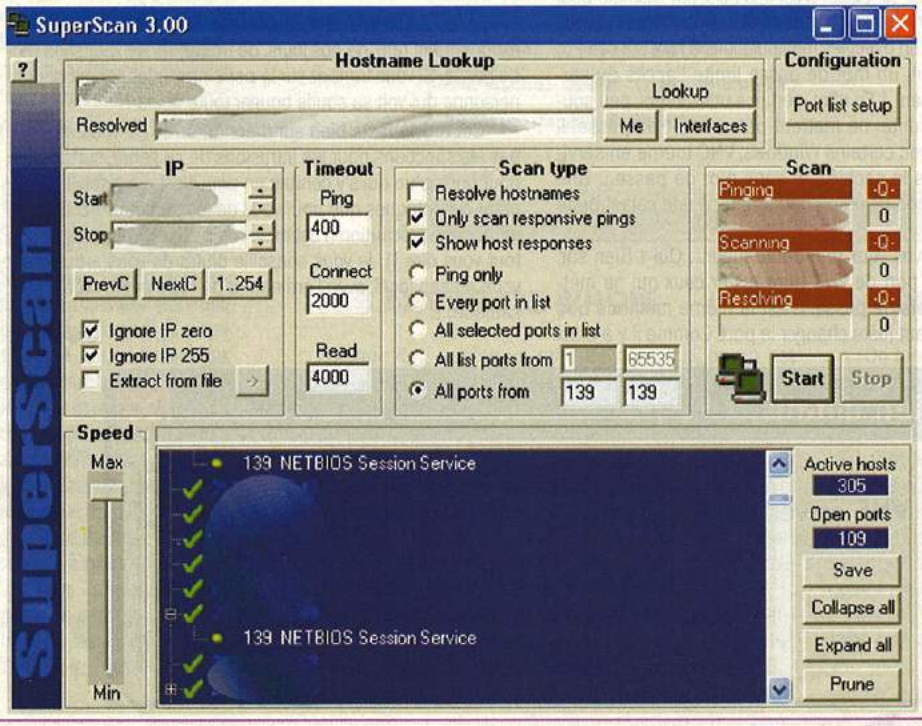
L'interface Netbios est très utilisée pour Windows, par exemple pour partager des ressources réseau telles que des fichiers ou des imprimantes. C'est pratique, mais très mal sécurisé.

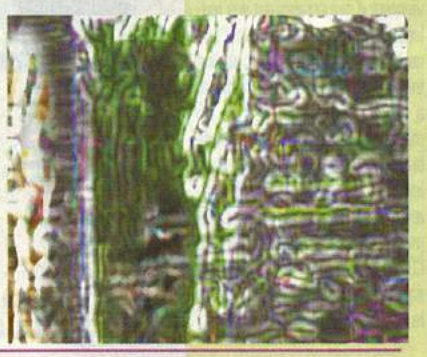
Comment s'amuser avec ? Vous avez besoin de deux logiciels : Internet explorer et un scanner de port, celui que vous préférez... Nous prendrons ici Superscan version 3 pour Windows (disponible sur http://www.foundstone.com/ ; la version 4 n'est pas terrible à mon goût, et elle ne marche d'ailleurs que sur XP et 2k). Dans un premier temps, le but de la manipulation est de trouver le plus grand nombre de personnes dont le port de Netbios est ouvert. Ce qui est très fort, c'est que vous n'avez pas besoin d'utiliser le partage de ressources (pour votre réseau local, par exemple) pour que ce port soit ouvert (merci Windows !). On va donc scanner un ensemble d'adresses IP, mais pas n'importe lequel. En effet, nous allons chercher des ordinateurs qui restent connectés en permanence – la meilleure cible étant les connexions haut-débit. Or, les fournisseurs d'accès à Internet distribuent toujours les mêmes IPs aux connexions ADSL. Si vous l'avez, prenez des IPs qui sont autour de la vôtre, vous serez certain de scanner des ordinateurs ayant l'ADSL. Par exemple, si votre IP est 257.124.25.13, il faudra faire un scan de 257.124.25.0 à 257.124.25.255. Ici, le logiciel scannera 255 IPs qui auront l'ADSL à coup sûr. Pour lui indiquer de scanner seulement ces IPs, il faut indiquer celle de départ et celle d'arrivée, en d'autres termes la première et la dernière. Il va donc prendre chaque IP une à une et scanner les ports à la recherche de ceux ouverts.

Ce qui nous intéresse, c'est Netbios, donc le port 139. Il faut donc dire au scanner de restreindre le scan au port 139 (il suffit pour cela de lui dire que le port de départ est le même que celui d'arrivée : le 139). Sur le screenshot, le rang d'IP est à gauche et le port est bien réglé...

Attention... 3... 2... 1... Start ! En 30 secondes, on peut scanner plus de 750 IPs. Parmi toutes ces IPs, environ la moitié est active. Sur les 375 ordinateurs connectés, un tiers a le port 139 ouvert. On peut donc dire qu'un PC sur six a son port Netbios ouvert. Ces victimes potentielles sont indiquées par Superscan, avec un petit plus à côté de l'IP.

Bien, on a une centaine de PC dont le port est ouvert. Le but, maintenant, est de trouver ceux qui n'ont pas mis Windows à jour ou qui n'ont pas de firewall. C'est le moment d'utiliser Internet explorer. C'est tout bête, il suffit de recopier les adresses (celles indiquées par Superscan par un +) dans la barre d'adresse d'Internet explorer, de cette façon : \\257.124.25.13 (\\ipdelamachine). Il faut tester toutes les adresses et vous tomberez à un moment ou à un autre sur une IP qui marche. Les résultats de chaque requête seront de trois types :





LES DANGERS DU PRÉSERVATIF PERCE

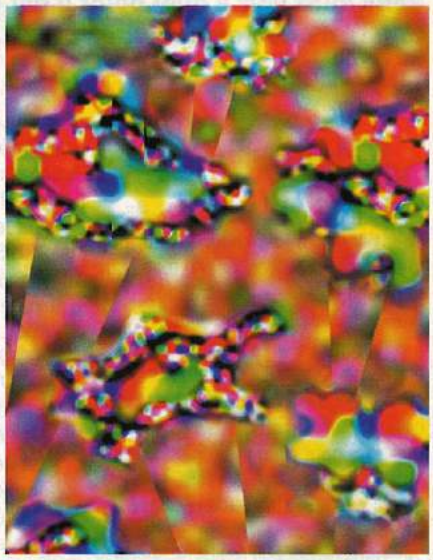
Un ver assez radical a mis hors de service plusieurs milliers d'ordinateurs fin mars. Assez ironiquement, ce ver exploitait une faille dans des firewalls, ceux de Black Ice et de Real Secure Internet. Et voilà comment un logiciel censé vous protéger est devenu une source de gros ennuis. Ce ver s'amuse en effet à écrire un peu n'importe où sur le disque dur, ce qui rend rapidement la machine inutilisable. Un comportement loué par les experts en virus, car l'infection a ainsi été assez limitée. Les victimes, elles, sont moins heureuses.

MICROSOFT PREND LES CHOSES EN MAIN

La firme de Billou prétend vouloir dynamiser le combat contre le piratage en renforçant la sécurité des systèmes (il serait temps). Steve Ballmer a ainsi annoncé un " nouveau firewall qui, notamment, stoppera les spammers ". Wow, là je suis impressionné, on se demande pourquoi personne n'y avait pensé avant. " Sécuriser Internet est une de nos responsabilités ", a-t-il ajouté, précisant qu'il leur fallait " trouver de nouvelles manières de poursuivre les hackers, en collaboration avec le FBI ". Des déclarations qui font un peu froids dans le dos.

• une erreur : vous ne pouvez pas rentrer, laissez tomber... Le moindre firewall bloque ce genre d'attaque (comme quoi ça sert quand même à quelque chose !).
• une invite de connexion (voir illustration) : Windows est peut-être à jour, ou la personne a eu la bonne idée de mettre un mot de passe. Les plus forts d'entre vous peuvent essayer de cracker le passe. Certains logiciels sont spécialisés dans le cracking des passes Netbios, mais ce n'est pas très intéressant vu la lenteur des requêtes...
• une page contenant des dossiers partagés : gagné, c'est les fichiers de l'ordinateur cible. À tous les coups, vous avez l'accès en écriture, puisque le propriétaire pense partager ses ressources uniquement sur son propre réseau... erreur ! Pour pousser le vice encore plus loin, si une imprimante est partagée, vous pouvez l'utiliser... Il y a des trucs marrant à faire, je vous laisse y réfléchir !

Si vous allez assez vite, vous pouvez en tester une centaine en 5 minutes. Et d'après mes statistiques, sur 100 PC testés, une dizaine marche, et sur cette dizaine on peut accéder à un PC qui partage entièrement son disque dur... ça fait peur !



AVEC VNC

C'est quoi ? VNC (pour Virtual Network Computing : www.realvnc.com) est un freeware qui tourne sur presque tous les types d'ordinateurs. C'est une application client/serveur qui permet de contrôler un ordinateur à distance, comme si on était devant l'écran : quand le client se connecte au serveur, une fenêtre s'ouvre avec une reproduction de l'écran de l'ordinateur serveur, dans laquelle vous pouvez bouger la souris et taper au clavier, comme si vous étiez sur place. C'est très utile, par exemple pour l'apprentissage : une personne vous demande un conseil et vous pouvez lui montrer en direct les manipulations à faire sur son PC.

Généralement, un mot de passe limite l'accès du serveur... Généralement ! En effet, certains utilisateurs, peu soucieux de leur sécurité, ne mettent pas de mot de passe. Il arrive aussi qu'avec certains Windows, VNC tourne en service sans que vous le sachiez, et sans mot de passe... Une simple erreur de configuration peut mener à une catastrophe n'est-ce pas ?

Je vois dans vos yeux une petite lueur... Oui ! Bien sûr, on va scanner le port de VNC pour tester ceux qui ne mettent pas leurs mots de passe. C'est la même méthode que pour Netbios : il faut juste changer le port. Comme il y a deux ports, le 5800 et le 5900, je vous conseille de créer un fichier nommé vnc.lst dans le dossier de superscan, contenant ceci :

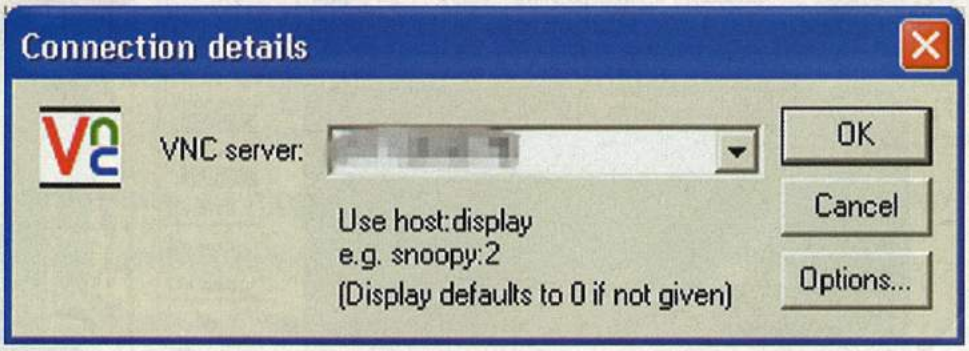
+,5800,VNC,,,
+,5900,VNC,,,

Ensuite, chargez la liste dans le gestionnaire des listes de Superscan et sélectionnez "Every port in list" dans le panneau principal. Comme pour Netbios, sélectionnez une plage d'IP et scannez. Ensuite, prenez votre client VNC et testez-les toutes une par une.

Je vais peut-être gâcher votre plaisir, mais sachez qu'il est extrêmement rare, de nos jours, de trouver un serveur sans mot de passe. Si vous tombez sur la perle rare, effet garanti pour la personne qui voit sa souris bouger toute seule !

Cet article reste bien sûr théorique... Je ne vous rappelle pas les sanctions pour les intrusions de ce genre, surtout que pour quelqu'un qui s'y connaît un peu, il est aussi facile de repérer ces attaques que pour vous de les perpétrer ! D'ailleurs, ici, aucune précaution n'est prise (on n'allait quand même pas tout vous dire !). Je vous conseille plutôt de vous amuser sur votre réseau local, avec l'ordinateur de votre petite sœur (petit sadique)...

CAPASHEN



'IZ

LINDOWS FAIT LE DOS ROND

Après des décisions de justice négatives en Europe, Lindows a décidé de changer carrément de nom hors des États-Unis. On ne sait pas encore quel sera le nouveau nom, sans doute quelque chose comme " IhateBill " ou un truc du genre. C'est en tout cas un sérieux revers pour ce Linux à la sauce Windows, qui gardera quand même son appellation aux États-Unis. En effet, la procédure judiciaire qui y est engagée n'est pas près de se terminer, ce qui laisse le temps à Lindows de voir venir. Et de trouver un meilleur nom plus tard.

ITUNES SANS PROTECTION

Apple, qui a lancé récemment le service de musique en ligne iTunes, vient d'apprendre une leçon à laquelle on s'attendait tous. En effet, la protection des fichiers téléchargés a déjà été cassée. Il faut savoir que " normalement ", un fichier téléchargé sur iTunes ne devait pouvoir être lu que sur l'iPod et sur trois ordinateurs différents. Évidemment, ces belles restrictions peuvent être dépassées, par exemple en utilisant le logiciel m4p2mp4. Comme d'habitude, protection rime avec illusion.

FASHION CD PLATS

60 000 CD-Roms provenant du Warez viennent d'être écrasés par des rouleaux compresseurs en Equateur ! Ce qui les rend encore plus plats, et c'est très joli. Le gouvernement équatorien a estimé qu'il y avait plus de 25 millions de CD illégaux, provenant de la Scène et autres, en circulation dans leur pays. Une autre opération bulldozer a été prévue pour le mois prochain mais avec la destruction de 80 000 CD ! Picasso n'a qu'à bien se tenir, les équatoriens pourraient bien vendre leurs œuvres !

LA COLLECTE D'INFORMATIONS

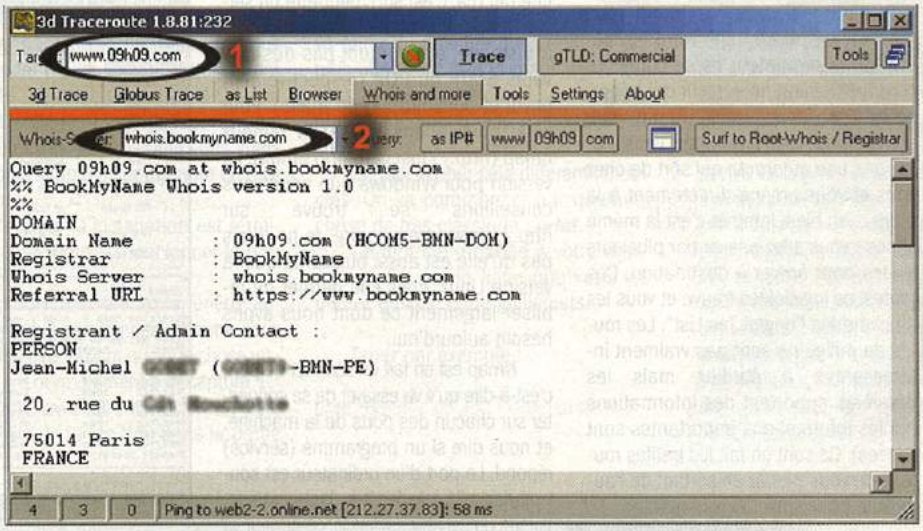
Vous allez voir dans cet article comment, à partir d'un simple site internet, on peut trouver toutes les informations que l'on souhaite sur son webmaster et le serveur qui l'héberge...

Dans le dernier numéro de Pirat'z, vous vous êtes mis dans la peau d'un hacker utilisant le social engineering pour compromettre la sécurité d'un serveur. Au début du scénario, vous aviez récupéré des informations sur l'entreprise à attaquer. Nous allons voir plus en détail comment procéder pour en trouver un maximum sur le webmaster et sur sa machine, avec quelques logiciels et Google.

Partons d'un site assez humoristique : www.09h09.9online.fr

Le principe de ce site est original : le webmaster prend tous les jours une photo de lui à 9 heures 9 minutes, et l'affiche sur son site. Pour notre plus grand malheur, les coordonnées de cette star interplanétaire ne sont pas indiquées... Bouhouhou ! Comment vais-je faire pour avoir des informations sur ce génie ? Je suis un fan et je veux le contacter, comment s'y prendre ? C'est un jeu d'enfant...

En naviguant sur le site, on remarque une version anglaise. En s'y rendant, on voit que l'adresse change : http://www.09h09.com. Un domaine .com ? Génial, c'est sûrement lui qui l'a acheté, il est donc référencé dans une base donnée. On va pouvoir trouver le propriétaire en utilisant un simple "Whois"



LES SERVEURS WHOIS

Lorsque l'on achète un nom de domaine, on en est responsable. C'est pourquoi on doit donner ses coordonnées. Il faut cependant être conscient que ces données personnelles sont en principe accessibles à tous, par une simple consultation du serveur whois approprié. Pour trouver à qui appartient www.09h09.com, nous allons utiliser le logiciel 3D Traceroute, un freeware disponible sur le web (), mais on pourrait aussi utiliser des services online, comme VisualRoute. Nous allons utiliser deux fonctionnalités de ce programme : d'abord le whois, puis le tracing.

Les informations sur les noms de domaines sont centralisées sur plusieurs serveurs whois principaux. Pour les .COM, par exemple, on utilise whois.internic.net. Pour l'Europe, c'est whois.ripe.net. Il y a quelques années, ces serveurs contenaient toutes les informations, mais avec l'explosion d'Internet, ce sont les revendeurs de noms de domaines qui gardent les détails personnels. Ainsi, une requête pour 09h09.com chez Internic nous apprend que les infos se trouvent sur whois.bookmyname.com. On indique donc ce serveur dans le champ approprié de 3d Traceroute, comme on le voit dans l'illustration.

On trouve dans le résultat des informations très intéressantes. En voici un extrait, certaines informations étant effacées pour des raisons évidentes de discrétion (ces données sont cependant publiques) :

Domain Name : 09h09.com
Registrant / Admin Contact :
Jean-Michel *****
20, rue du **********
75014 Paris FRANCE
phone : +3314321****

Impressionnant, non ? On a son nom, prénom, adresse, et téléphone. Ça fait déjà pas mal d'infos, mais moi je suis un fan, un vrai, alors je veux tout savoir sur lui ! Pour cela, on va faire appel à un outil surpuissant : Google !

GOOGLE, SI BAVARD

On lance la recherche : "Jean-Michel *****" (essayez avec votre nom, vous pourriez être surpris !). On trouve son site perso. Allez, on y va, peut-être trouverons-nous des infos... Bingo ! On est déjà sûr que c'est bien lui avec les photos, et la liste de ses autres sites le confirme (09h09.com est là).

On trouve aussi sur ce site sa généalogie complète. Ce sont des informations extrêmement utiles lors d'une attaque par social engineering. N'êtes-vous pas en confiance quand quelqu'un vous parle de la part de votre cousin ou de votre tante ? Toutes ces informations peuvent être exploitées. De plus, on a les coordonnées de son responsable technique, imaginez pour qui on pourrait se faire passer ;)

SHAREREACTOR EXPLOSE EN VOL

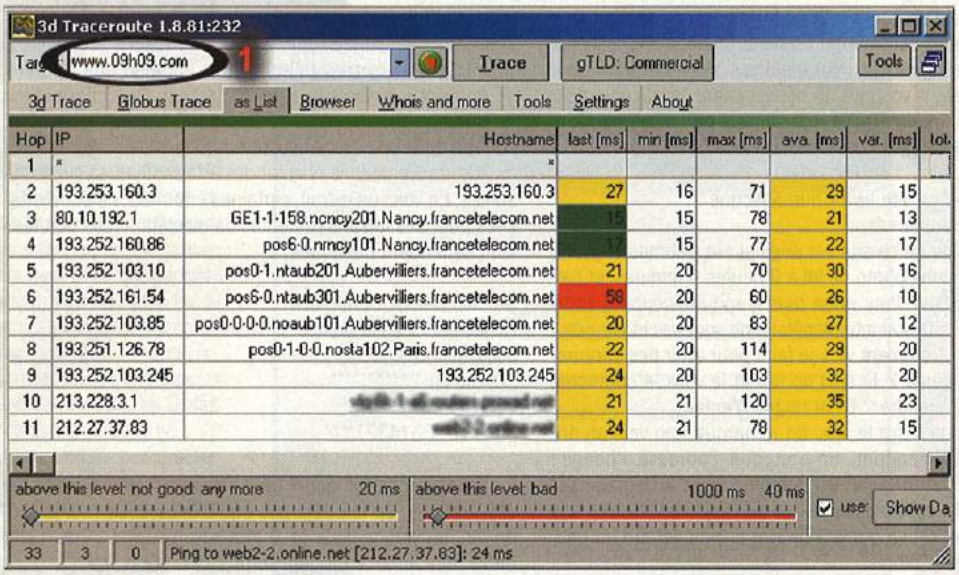
Le site ShareReactor était, depuis déjà plusieurs années, une référence incontournable pour les liens eDonkey. Ce site proposait une liste assez impressionnante de liens qui, une fois chargés par eDonkey, vous permettaient de lancer immédiatement le téléchargement de multiples jeux, logiciels ou films. Le site, lui, se défendait d'être illégal en disant ne fournir que des liens. C'était peut-être vrai, mais apparemment, ça n'a pas suffi à convaincre tout le monde, puisque le site ne fonctionne plus. Si la raison officielle n'est pas connue, la possibilité de pressions externes (menaces de poursuites) reste le plus probable. Après ce gros coup de massue sur la communauté eDonkey, d'autres sites ont fermé leurs portes, comme le moteur de recherche Jigle.com, qui permettait de chercher efficacement sur le réseau eDonkey. Et comme si ça ne suffisait pas, le site du logiciel PeerGuardian (censé vous protéger contre les offensives de la RIAA) a connu quelques remous, semblant maintenant s'établir sur http://homepage.ntlworld.com/tim.leonard1/pgupdate.htm.

SCO DOIT SE JUSTIFIER

Si vous voulez toujours être pompier lorsque vous serez plus grand, je vous conseillerais plutôt avocat spécialisé dans les technologies de l'information, il y a de l'avenir... Car on parle encore de procès, celui de SCO contre IBM (SCO accusant IBM d'utiliser Linux, dans le noyau duquel il y aurait du code propriétaire de SCO). Le juge en ayant marre d'entendre les avocats se battre à coup de " mais si ", " mais non ", a ordonné aux deux parties de mettre le code sur la table, histoire d'y voir plus clair. Vivement qu'on en finisse !

TRACEROUTE

Toujours avec le logiciel 3D Traceroute, après avoir indiqué 09h09.com dans le champ de l'adresse, allez dans l'onglet "as List" et cliquez sur Trace. Le logiciel va tracer la connexion jusqu'à sa source. Mais que se passe-t-il exactement ? Eh bien, en fait c'est le principe d'Internet, la toile. Quand vous tapez une adresse dans votre navigateur, votre ordinateur ne se connecte pas directement au serveur qui héberge le site. Réfléchissez, quand vous allez en vacances à la plage, vous n'avez pas une autoroute qui sort de chez vous et vous amène directement à la plage... eh bien, Internet c'est la même chose : vous allez passer par plusieurs routes pour arriver à destination. Ces routes, ce logiciel les trouve et vous les affiche dans l'onglet "as List". Les routes du milieu ne sont pas vraiment intéressantes à étudier, mais les dernières apportent des informations (ici les informations importantes sont grisées). Ce sont en fait les petites routes que vous prenez en sortant de l'autoroute pour arriver à la plage...



Le serveur se trouve donc à Paris... Mais ce n'est pas si étonnant que ça, puisqu'il est hébergé par 9online.

Bon, maintenant ça suffit pour notre Jean-Mich ;)

PORT SCAN

Continuons notre collecte d'informations, mais sur un ordinateur du Net, maintenant. Prenons un site qui ne nous donne aucune information de départ : www.perdu.com. Encore une fois, un humour subtil... Je vous laisse découvrir ce site.

C'est parti, on va récupérer un maximum d'informations sur le serveur qui l'héberge.

Première étape, trouver son IP. Ça, on le fait les doigts dans le nez : on ouvre une console (Démarrer > Exécuter > cmd.exe), et on tape :
ping www.perdu.com.
Les résultats indiqueront l'IP de la machine : 64.62.206.***.

Maintenant, nous allons voir ce qui tourne sur cette machine. Il y a un serveur http permettant d'afficher le site internet (ça, c'est sûr), peut-être un serveur ftp pour uploader les pages du site à distance, et pourquoi pas des serveurs SMTP ou POP (respectivement envoi et consultation de mails). Pour cela, nous allons utiliser le fameux nmap (http://insecure.org/nmap). La version pour Windows que nous vous conseillons se trouve sur http://www.nmapwin.org. Je ne dirais pas qu'elle est aussi puissante que la version Linux, mais elle permet de réaliser largement ce dont nous avons besoin aujourd'hui.

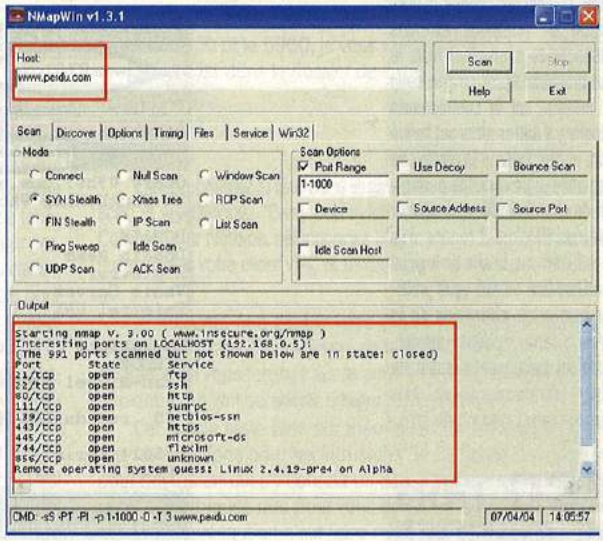
Nmap est en fait un scanner de port, c'est-à-dire qu'il va essayer de se connecter sur chacun des ports de la machine, et nous dire si un programme (service) répond. Le port d'un ordinateur est souvent assimilé à la fenêtre d'une maison. Lorsqu'un serveur est lancé, ce dernier va ouvrir une fenêtre pour proposer ses services aux passants. Nmap va nous permettre de lister ces fameux serveurs. Il nous permet également de connaître le système d'exploitation utilisé.

Ce genre de scan est très bruyant. Vous êtes repérés à l'instant même où vous lancez le scanner, mais vu l'utilisation que nous allons faire de ces informations et le caractère ultra-secret des documents de ce site, nous pouvons nous le permettre.

Comme mode, cochez "SYN Stealth" et, dans Scan Option, indiquez 1-1024 dans la case Port Range (les services intéressants tournant habituellement sur cette plage de ports). Pas besoin de toucher aux autres onglets, les réglages par défaut conviennent très bien.

J'allais oublier, entrez l'adresse www.perdu.com dans le champ Host ;)

Pour les plus curieux d'entre vous ou pour ceux qui utilisent Linux, la commande qui correspond aux réglages que nous avons demandés est affichée en bas de la fenêtre. Vous auriez exactement le même résultat en entrant cette dernière dans un terminal Linux.



Après quelques secondes, on obtient les résultats de la capture d'écran. Déjà, on voit que le serveur tourne sur Linux (la version du noyau est également indiquée).

La liste des services est répertoriée dans la colonne du même nom, on voit, entre autres, un serveur http et ftp comme prévu, ainsi qu'un serveur ssh. On remarque aussi que le port 443 est activé (http via ssl). On essaye donc de visiter https://www.perdu.com. Rien de bien intéressant, une page par défaut. Mais c'est en testant de petits trucs comme ça qu'on récupèrera les meilleures informations.

C'est ainsi qu'avec la liste des services, le pirate pourrait passer à la phase d'attaque en cherchant les vulnérabilités dans chacun d'entre eux. Mais cet article s'arrête à la récupération d'informations, nous n'irons donc pas plus loin ;)

Capashen

VOTEZ ÉCOLO !

Même s'il est trop tard, vous le saurez pour la prochaine fois : il fallait voter pour les Verts. En effet, la Ligue Odebi (www.odebi.org), qui organise la lutte contre la Loi sur l'Économie Numérique, a demandé aux partis politiques quelle était leur position vis-à-vis de cette loi. Si la droite n'a pas daigné répondre, les Verts s'y sont déclarés opposés. Le PS, lui, dit en gros que c'est difficile de légiférer là-dessus (s'étant bien planté précédemment), et que la droite s'y prend mal (évidemment). Plus d'infos sur le site d'Odebi.

LA PROGRAMMATION DEMYSTIFIEE

Alors comme ça, tu veux devenir un vrai hacker des temps modernes ? Tu as sûrement déjà entendu ce qui est dit sur le Net : un bon hacker sait bien programmer ! Voici une bonne occasion de s'y mettre, même pour les plus débutants d'entre vous.

D'après les grands gourous, le hacker doit aussi être sous Linux, mais on verra ça un autre jour. Nous allons pour l'instant essayer de voir ensemble ce que l'on appelle la programmation.

J'en vois déjà qui ont des frissons dans le dos et qui s'attendent à un article où ils ne vont rien comprendre, car la moitié sera écrite dans un langage qui est tout sauf du Français et qui passe bien au-dessus de l'humain moyen.

Et bien oui, hahaha, le but de cet article est que vous ne compreniez absolument rien ! Hum, plus sérieusement, vous pouvez vous rassurer, nous rencontrerons exceptionnellement quelques lignes de codes dans cet article, mais son but est justement de vous montrer qu'il n'y a rien de compliqué dans la programmation. Il suffit de s'y intéresser un peu pour en comprendre le fonctionnement et en maîtriser les bases. Pour l'anecdote, j'ai récemment initié mon frère de 11 ans à la programmation en Basic et il n'y a pas eu de problèmes. Cela prouve bien qu'il n'est ni besoin de parler Anglais couramment ni besoin de sortir de maths-spé pour créer un programme.

PREMIÈRE SALVE EN QBASIC

C'est bon, vous êtes prêt, on peut y aller ? Alors commençons par répondre à une question simple, mais dont la réponse n'est pas totalement inutile :

On va où sur l'ordinateur pour créer un programme ?

Il faut un logiciel spécifique ? Pour répondre à cette question, il faut distinguer deux types de langages : les langages interprétés et les langages compilés.

Lorsque le langage est dit compilé, votre ordinateur doit créer ce que l'on appelle un exécutable à partir du code que vous lui donnerez. Vous avez sûrement déjà rencontré ces fameux exécutables, il s'agit de tous les fichiers portant l'extension .exe. Cette transformation est réalisée par un logiciel spécifique appelé compilateur. Nous utiliserons tout à l'heure comme exemple Rapid-Q Basic http://basicguru.com/rapidq/ compiler, qui vous permettra de créer vos premiers programmes dans un langage très simple : Qbasic.

Pour les langages interprétés, c'est encore plus simple. Il suffit d'éditer un fichier texte avec votre logiciel préféré (le bloc note fait très bien l'affaire), puis de l'enregistrer avec l'extension appropriée. Votre programme, que dans ce cas là on appellera plutôt un script, est alors prêt à être utilisé (exemples : Perl, Python, VBScript, etc.).

Il existe des éditeurs spécialisés pour certains langages, rendant la programmation plus simple à l'aide de couleurs ou de listes de fonctions, mais l'utilisation, bien que très agréable, n'est pas obligatoire.

C'est bon, vous suivez ? Allez, on passe à la suite :-p

Le compilateur, ça ressemble à quoi ?

Comme je vous l'ai dit, on va commencer par Qbasic. Je vais donc vous demander d'aller vous installer devant votre PC, de télécharger Rapid-Q basic et de continuer à lire ensuite. (Si vous ne voulez pas, tant pis pour vous, mais c'est plus simple à comprendre en pratiquant :-)

C'est bon, l'installation est terminée ? Vous pouvez alors lancer le programme.

A l'ouverture, fermez la fenêtre appelée Form 1 et agrandissez l'autre. Vous vous retrouvez devant quelque chose ressemblant normalement à la capture 1.

Vous l'avez sûrement deviné, c'est au centre de la fenêtre, dans la partie blanche, que vous allez pouvoir taper votre code. Rien à voir avec des codes pour un jeu vidéo qui vous permettent d'atteindre le niveau Super Hacker sans rien faire. On appelle code les lignes de programmation qui vont permettre à votre ordinateur préféré de créer le programme de vos rêves.

Pas mal... et je tape quoi comme code ??

Bonne question. Il faut pour cela imaginer que vous parlez à votre ordinateur et que vous lui dites ce que vous voulez qu'il fasse. Attention, quand je dis parler c'est en écrivant, ne commencez pas à faire ça à haute voix ou vous risquez de finir dans un asile plus tôt que prévu ;-)

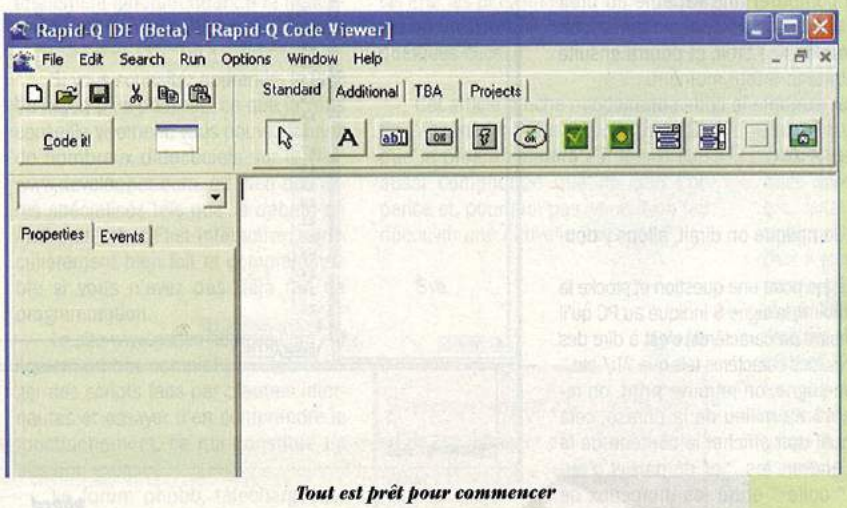
Manque de bol, votre PC ne parle pas Français, à moins que vous ne décidiez de lui donner des cours. Mais on va partir du principe que l'homme est plus intelligent que la machine. Ainsi, vous apprendrez à parler son langage plus rapidement que lui n'apprendra le vôtre.

On utilise pour cela différents mots clés. On va commencer par quelque chose de très classique : ***print***.

Ce mot clé ordonne à votre ordinateur d'écrire la ligne que vous lui mettez ensuite entre guillemets.

Tapez par exemple :

```
print "Salut, c'est ton PC qui te parle."
```



Tout est prêt pour commencer

LE P2P INSPIRE LES HACKERS

Lorsqu'un hacker souhaite lancer une attaque de Denial Of Service (DOS), un nouveau virus, ou envoyer du spam, il peut bien sûr le faire à partir de son propre ordinateur. Mais tout lecteur de Pirat'z qui se respecte ne commettrait évidemment pas cette bêtise. J'aimerais pouvoir dire qu'il ne penserait même pas à de telles horreurs, mais j'ai comme l'impression que je me ferais quelques illusions. Enfin, une méthode plus efficace et plus sûre consiste à prendre le contrôle d'une petite armée de machines, par l'intermédiaire d'un programme de type cheval de troie, qu'il n'est pas bien difficile de répandre avec toutes les failles qui existent. Auparavant, les hackers se servaient souvent d'IRC pour contrôler leurs " zombies ". Mais certains commencent maintenant à utiliser plutôt un réseau P2P : cela a l'avantage d'éliminer ce point " central " qu'était le canal IRC, un réseau P2P demeurant actif même si on en démantèle une partie. Et c'est évidemment aussi plus sûr pour le hacker. Bon, c'est inquiétant, tout ça, ça veut dire qu'en plus, les hackers deviennent intelligents...

Il faut ensuite appuyer sur la touche F5 pour que le compilateur "fabrique" le fichier exécutable et le lance afin que vous puissiez admirer votre production.

Allez hop la, c'est parti ! Mouais, pas terrible, à moins que vous n'ayez une vision ultra développée, le programme s'exécute tellement vite que l'on a le temps de rien voir.

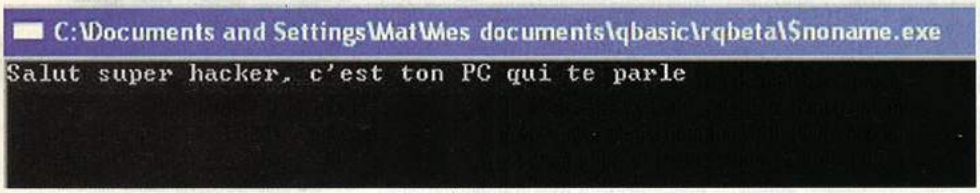
Il va donc falloir utiliser la fonction **sleep**. Le mot sleep voulant dire dormir en Anglais (je fais la traduction, on ne sait jamais, comme j'ai dit au début de l'article qu'il n'y avait pas besoin d'être bilingue ;-) le programme va s'arrêter pendant le nombre de secondes que vous lui indiquerez afin que vous puissiez voir ce qu'il fait. À moins que vous ne comptiez aller faire une pause pipi ou que vous ayez de sérieux problèmes de lecture, 10 secondes devraient faire l'affaire.

Notre code ressemble donc maintenant à ça :

```
print "Salut super hacker, c'est ton PC qui te parle"
sleep10
```

Allez, on appuie sur F5 et ho ça marche ! (Si jamais chez vous c'est plutôt "ho ça marche encore moins qu'avant", vérifiez que vous n'avez pas fait de faute en recopiant le code, votre PC n'a sûrement pas encore assimilé le langage SMS ;-)

Vous obtenez alors la fenêtre de la capture 2.



Premier programme

Eh bien ça y est, vous avez réussi ! Alors, votre pote qui faisait le malin avec ses Hello world n'est peut-être pas vraiment un super hacker. Vous savez en faire autant que lui en tout cas :-)

Mais la programmation ne se limite pas à afficher des phrases préenregistrées ; ça, ça s'appelle un livre et on n'est pas vraiment là pour en écrire un, enfin moi je suis là pour écrire un article mais vous pour programmer ;-)

On va donc voir une nouvelle fonction : ***input***. Son but est assez simple, elle va vous permettre de poser une question à l'utilisateur et d'enregistrer sa réponse dans ce que l'on appelle une variable. On peut comparer une variable au tiroir d'une armoire : le PC va stocker des données, un mot, une phrase, dans ce tiroir, et pourra ensuite en ressortir le contenu à tout moment.

Essayons par exemple le code suivant :

```
input "Salut, c'est quoi ton ptit nom ?", a$
print "Cool, comment ca va "; a$; " ?"
sleep 10
```

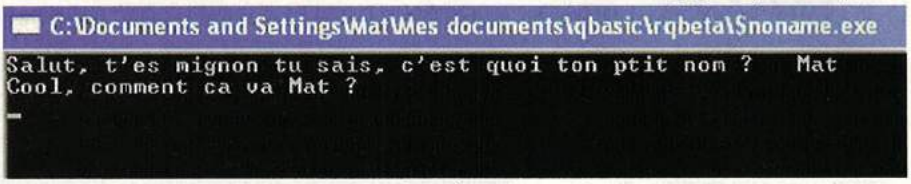
Oula, ça se complique on dirait, allons y doucement ;-)

La première ligne pose une question et stocke la réponse dans le tiroir **a**, le signe **$** indique au PC qu'il va stocker une chaîne de caractères, c'est à dire des lettres, des espaces, des caractères tels que ?!:/ etc...

A la deuxième ligne, on retrouve **print**, on remarque alors le **a$** au milieu de la phrase, cela indique au PC qu'il doit afficher le contenu de la variable a à cet endroit, les " ; " de part et d'autre servent de " colle " entre les morceaux de phrase et la variable. Si vous voulez vous la raconter, c'est un opérateur de concaténation.

Je ne vais pas vous ré-expliquer à quoi sert la dernière ligne, sinon retournez au début de l'article et on reprend tout depuis le débu ;-).

On lance le programme et normalement tout devrait marcher et vous devriez obtenir le résultat de la 3e capture.



Input/Output

Voilà ! Cet article étant une simple démystification, je pense donc que le but est atteint au niveau du Basic. Nous avons pu voir ensemble qu'il n'y a rien de bien compliqué dans tout ça et étudier toutes les fonctions dans cet article serait d'abord très lassant et inutile puisqu'il suffit d'aller chercher un peu sur le Net pour trouver des didacticiels très complets. Vous pouvez par exemple consulter le site http://lyc-sophie-germain.scola.ac-paris.fr/Info/tutoqbasic.html ou encore télécharger gratuitement le deuxième Espiozine disponible sur www.espionet.com, contenant un tutorial complet sur ce langage (le reste du zine est d'ailleurs très intéressant aussi, oui bon d'accord j'arrête ma pub et on continue).

ET EN PHP

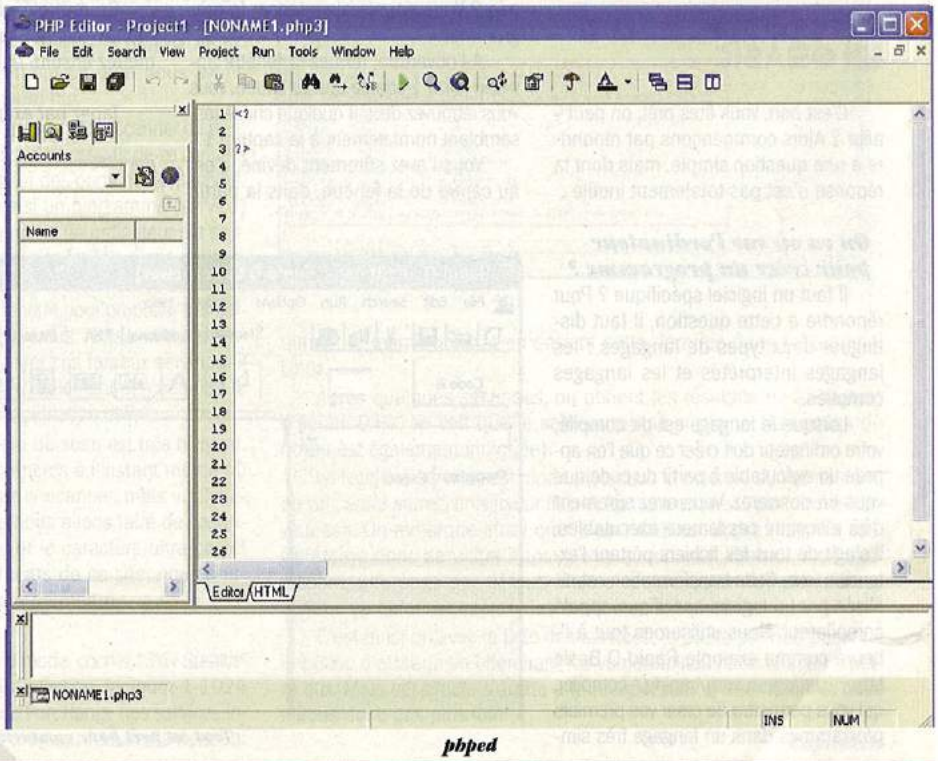
Maintenant que les exécutables n'ont plus de secrets pour vous, nous allons nous pencher sur le cas des langages interprétés et particulièrement sur PHP. Le PHP est l'un des langages les plus utilisés sur le Web : forums, guest books, sites complets sont réalisés dans ce langage.

En effet, c'est un langage simple et très puissant, et c'est pour cela que j'ai choisis de vous le présenter aujourd'hui (évidemment, si j'avais choisis un langage très compliqué et peu utile ça n'aurait pas intéressé beaucoup de monde lol).

Le PHP a pour particularité d'être exécuté par le serveur web, c'est donc très pratique lorsque vous créez votre site : il suffit d'uploader vos fichiers avec l'extension .php et ils seront automatiquement interprétés par le serveur de votre hébergeur (s'il propose php, bien sûr).

Mais pour s'entraîner et découvrir le langage, il est bien plus pratique de l'exécuter en local, sur votre propre machine. Il suffit pour cela d'installer le programme EasyPHP (qu'on trouve par exemple sur www.telecharger.com), et de placer vos pages dans le dossier www du répertoire d'installation que vous avez choisi pour EasyPHP. Pour accéder à coucou.php, il faudra alors entrer l'url : http://localhost/coucou.php.

Bien, maintenant que les présentations sont faites, nous allons pouvoir commencer. Pour éviter le bloc note, très pratique mais assez moche, nous allons nous servir de phped, à télécharger sur www.freelogiciels.com (voir illustration).



phped

Vous pouvez remarquer les petits <? et ?>. Cela signifie tout simplement *début du programme php et fin du programme php*. Je vous rassure tout de suite, on ne va pas se borner à étudier trois fonctions cette fois ci. Maintenant que vous êtes de vrais codeurs, on va pouvoir s'attaquer à un petit projet. Oui bon d'accord, un tout petit projet : une page permettant de vérifier le mot de passe d'un utilisateur.

Je vous donne tout le code maintenant, nous allons l'étudier après :

```
<?
if ($pass == "programmation") {
  print ' Bravo vous avez trouvé le bon mot de passe !! ' ;
}
else {
  print 'Non, non, non interdiction
        de rentrer ! <br> ';
  print '<form method="post"
              action="pass.php">
         <input type="text" name="pass">
         <input type="submit"
                name="Submit"
                value="Envoyer">
        </form> ' ;
}
?>
```

Alors commençons par le début. L'instruction *if* réalise ce qui est entre les { } qui suivent, si la condition entre parenthèses est satisfaite. Ici, si le contenu de la variable **$pass** est égal à "programmation".

Attention, n'oubliez de mettre deux signes égal (==), c'est très important. Vous pouvez aussi remarquer qu'ici le $ se trouve avant le nom de la variable et non après, contrairement au QBasic.

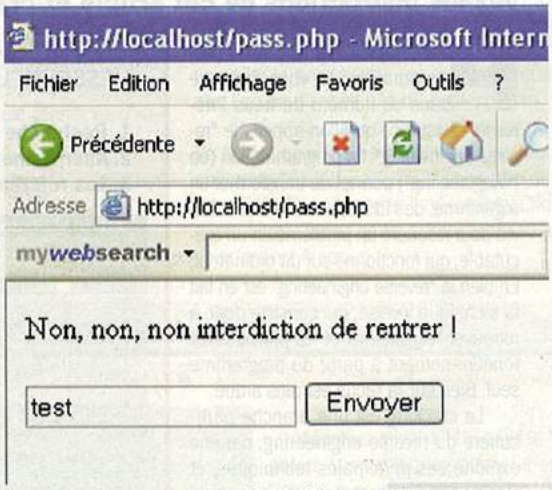
Donc, si le mot de passe est le bon, grâce à la fonction ***print***, qui vous est maintenant familière, on affiche le message Bravo vous avez trouvé le bon mot de passe.

On utilise ensuite la fonction **else**. Son rôle est très simple. Si la condition de if n'est pas réalisée, on effectue ce qui se trouve entre { et }. Cette fonction ne s'utilise jamais toute seule, elle doit toujours être accompagnée de **If**.

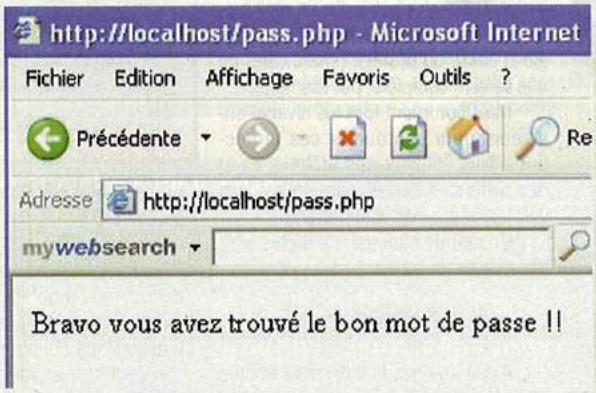
Donc, si le mot de passe est mauvais, on affiche un petit message, puis le formulaire permettant de réessayer. Je vous passe les détails du code HTML, sachez seulement que l'on crée un formulaire avec un champ appelé pass et un bouton qui, lorsque l'on clique dessus, envoie le contenu de pass à votre script (qui devra impérativement s'appeler pass.php, si vous voulez lui donner un autre nom il faut aussi changer action="pass.php" pour y indiquer le nouveau nom).

Et voilà, votre script est prêt à fonctionner. Vous pouvez, comme je vous l'ai dit tout à l'heure, l'exécuter en local grâce à EasyPHP ou le mettre sur votre site perso pour montrer au monde entier que, grâce à Pirat'z, vous faites maintenant partie de l'élite du Net.

Voici les résultats obtenus lors de l'exécution du script :



Mauvais mot de passe



Bon mot de passe

Encore une fois, nous n'irons pas plus loin dans l'étude du langage. Je pense que vous en avez compris les bases de fonctionnement et que, la prochaine fois que vous croiserez un code PHP sur le Net, vous ne serez pas totalement ignorant quant à la manière de l'utiliser.

Si vous souhaitez apprendre le PHP de façon plus poussée, ce que je vous conseille vivement, vous pouvez trouver de nombreux didacticiels sur le Net, www.developpez.com, ou bien des livres spécialisés tels que *Je débute en PHP* édité chez First Interactive, particulièrement bien fait et compréhensible si vous n'avez pas déjà fait de programmation.

Le site www.codes-sources.com est également très complet pour télécharger des scripts faits par d'autres internautes et essayer d'en comprendre le fonctionnement, ce qui constitue un très bon exercice.

Le forum phpbb, téléchargeable gratuitement sur www.phpbb-fr.com, donne quant à lui une idée de la grande puissance de PHP et des fonctionnalités très utiles qu'il permet d'ajouter à votre site Web. Phpnuke (www.phpnuke-fr.org) fait également partie des outils PHP les plus répandus et permet de créer un portail très complet en quelques clics.

Cet article touche maintenant à sa fin, j'espère avoir réussi à vous montrer que la programmation est loin d'être aussi compliquée que ce que l'on pense et, pourquoi pas, vous avoir fait découvrir une nouvelle passion ;-)

Bye

Spolix

Si vous voulez un Pirat'z avec plus de code, et du bon, n'hésitez pas à nous le faire savoir ! Et si ça vous gonfle aussi.

'Z

GOOGLE DE PIGEON

Le chantage est une arme à double tranchant. En tout cas, personnellement, j'ai toujours entendu parler de maîtres chanteurs qui se faisaient prendre, et les histoires de succès semblent plutôt rares. Remarquez, ce n'est pas si étonnant. Les victimes de chantage ne doivent pas en faire beaucoup la publicité. J'en déduis donc que ça doit parfois marcher, car sinon, il faudrait vraiment être débile pour tenter certains coups, comme cet individu qui a essayé d'extorquer pas moins 100000 dollars à Google. Tout simplement en écrivant un petit programme cliquant automatiquement sur les liens sponsorisés de Google (liens apparaissant en haut, lors de certaines requêtes, pour lesquels les compagnies concernées paient), censé être indifférentiable d'un humain. Ce logiciel à la con, s'il était utilisé en masse, générerait des milliers de clics inutiles, ce qui dévaloriserait les liens sponsorisés (principale source de revenus de Google), et boum, faillite, dépression, suicide, fin du monde. La fin de l'histoire, c'est que le gars s'est fait choper. Évidemment.

METTEZ XP AU REGIME

Lorsqu'on tombe sur un petit programme sympathique, au gré de nos tribulations internautes, on essaie de vous en faire profiter. En plus, c'est promis, on ne vous donne jamais d'adresse affichant douze millions de popups. Quoi que, faites attention pour ce numéro, on est en avril après tout. Donc à vous de voir si vous irez sur www.litepc.com pour télécharger XPLite, un programme qui désactive tout un tas de composants de XP généralement inutiles, afin de gagner en place mémoire et en rapidité. Dommage que la version complète soit payante.

CRACKING POUR DEBUTANT

Vous voulez apprendre à casser vous-même des protections, mais vous pensez que c'est encore trop dur pour vous ? Pirat'z est là pour vous prouver le contraire. Suivez les instructions de cet article et crackez notre programme d'exemple !

UNE CONFÉRENCE PIRATE ?

Macrovision vient de planifier une conférence qui dévoilera comment les pirates arrivent à cracker et à diffuser les jeux vidéo sur Internet. Cette conférence aura lieu à l'E3 (l'Electronic Entertainment Expo) en mai, lors de la nouvelle édition de ce salon mythique. Le but de cette conférence est de montrer aux éditeurs de jeux vidéo comment et pourquoi les pirates arrivent à cracker leurs jeux pour leur vendre la solution miracle : SafeDisk de Macrovision (qui ne ralentit pas pour autant les hackers :-).

L'EUROPE DISTANCE LA FRANCE

Souvenez-vous... Il y a bien longtemps, l'Europe adoptait l'EUCD (European Union Copyright Directive), censée être transposée dans la législation de chaque pays membre de l'UE avant le 22 décembre 2002. Alors qu'on attend toujours que la France s'y conforme (bon, ok, on n'est pas vraiment pressé, mais quand même, ça fait pas très sérieux), l'UE remet ça avec une nouvelle directive visant à contrer le piratage. Vu que les pays membres ont 18 mois pour l'intégrer à leur législation, on ne l'attend pas avant 2025 en France. Cette nouvelle directive a fait beaucoup parler d'elle, car elle autorise les compagnies privées (genre, les maisons de disque) à ordonner elles-mêmes des perquisitions en cas de contrefaçon. Évidemment, les internautes ont commencé à avoir chaud aux fesses en apprenant ça, mais finalement, la version finale de la directive ne vise que le piratage commercial, et laisse donc tranquille les individus qui téléchargent dans leur coin. Soulagés ? Ne vous inquiétez pas, il y aura d'autres lois pour vous, les maisons de disque ne vous ont pas oubliés, elles !

Pour compléter l'article sur la programmation, je vous propose dans ce numéro de nous intéresser aussi à ce que l'on appelle le "reverse engineering". La programmation (ou "l'engineering") permet de transformer un algorithme, des idées, une marche à suivre pour résoudre un problème en un exécutable, qui fonctionne sur un ordinateur. Eh bien le "reverse engineering" est en fait la technique inverse, qui consiste donc à retrouver l'algorithme, et les principes de fonctionnement à partir du programme seul. Bien sûr, la tâche est plus ardue.

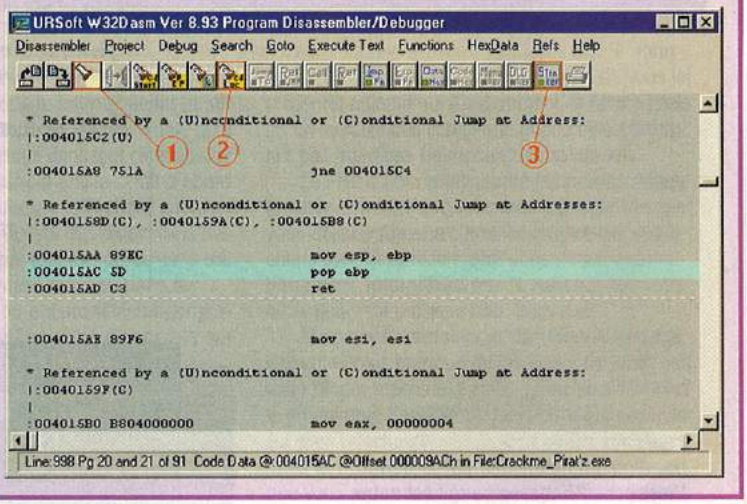
Le cracking est une branche particulière du reverse engineering, car elle exploite ses principales techniques, et s'en sert afin de contourner ou supprimer les protections d'un logiciel. On cherche à créer un crack, c'est-à-dire un petit programme qui permet de transformer un logiciel limité ou protégé (shareware) en une version complète, par exemple.

Mais comment font les reverse engineers pour contourner ces protections ? Ils utilisent des techniques et des outils spécifiques, dont nous allons voir les bases dès maintenant.

Un peu de courage, c'est plus simple que ça en a l'air ;-)

L'ESSENTIEL DE WINDASM

1. Recherche dans le binaire,
2. Aller à une adresse,
3. Les références, dans le code, à des chaînes de caractères.



PREMIERS PAS

Avant de nous lancer corps et âme dans l'explication concrète des techniques employées par les reverse engineers, nous allons nous attaquer à un programme d'étude (aussi appelé crackme, nom explicite), spécialement conçu dans le but d'enseigner ces techniques. Vous pouvez le télécharger sur notre site http://piratz.fr.st.

Pour arriver à nos fins, nous allons utiliser plusieurs outils :

- un désassembleur (WinDasm v8.9 : http://protools.cjb.net/),
- un éditeur hexadécimal (UltraEdit : http://www.ultraedit.com).

Le désassembleur permet de transformer l'exécutable, qui n'est qu'une suite de 0 et de 1 aux yeux de l'ordinateur, en un langage plus compréhensible par l'homme, mais très proche de la machine. J'ai nommé l'assembleur. Ce langage comporte des instructions simples, mais qui permettent de tout faire (opérations arithmétiques, modifications de la mémoire, interaction avec les périphériques, etc).

L'éditeur hexadécimal, quant à lui, nous servira à modifier le programme, mais nous ne nous intéresserons à la chose que plus tard.

Tout d'abord, on lance le programme. Il nous demande un mot de passe. On entre donc un mot de passe au hasard, et on valide. Il nous affiche à l'écran : "Bad password". Donc le programme sait que notre mot de passe n'est pas valide (logique, il a été créé pour ça). Maintenant, regardons ce qu'il a dans le ventre, grâce au désassembleur.

DÉSASSEMBLAGE

Lancez WinDasm v8.9, puis dans le menu "Disassembler" cliquez sur "Open a File to Disassemble". Sélectionnez l'exécutable, et validez. Le désassembleur travaille, et affiche un résultat dans la fenêtre interne. Pour continuer dans de bonnes conditions et afin que vous ne soyez pas perdus, je vous ai ajouté une légende des boutons de raccourcis de WinDasm (voir encadré).

On sait que le programme vérifie si le mot de passe est le bon, mais où le code qui ferait cette vérification se trouve-t-il ? Et bien nous avons un indice : le texte "Bad password". Il est en effet contenu dans le programme, il y a donc bien moyen de le retrouver. Et WinDasm va nous aider. Cliquez sur l'icône des String Data References (icône 3 dans la capture d'écran) : une fenêtre apparaît, qui liste toutes les chaînes contenues dans le programme. Si on cherche un peu, on trouvera celle-ci : "Bad password : %s !! Try again". Double-cliquez dessus, vous atterrissez là où le texte est appelé. Vous tombez donc sur un morceau de code, comme dans la capture en bas de page.

Mais si on réfléchit un peu, on se dit que si le programme en arrive à afficher le texte "Bad password", c'est que le test du mot de passe est déjà effectué ! Ainsi, ce test se trouve avant l'affichage de ce texte. Remontons donc de quelques lignes dans le listing, jusqu'à obtenir quelque chose comme au sommet de la page suivante.

```
* Possible StringData Ref from Code Obj ->"Bad password: %s !! Try again
                                       ->"..."
                                       |
:0040140F 6840134000                  push 00401340
```

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:004013F5(C)
|
:00401409 83EC08                sub esp, 00000008
:0040140C FF75FC                push [ebp-04]

* Possible StringData Ref from Code Obj ->"Bad password: %s !! Try again "
                                        ->"..."
```

On observe attentivement cette ligne : "Referenced by a (U)nconditional or (C)onditional Jump at Adress : 004013F5 (C) ", soit en Français " référencé par un saut conditionnel à l'adresse 004013F5 ". Cela nous donne deux renseignements précieux : d'une part, on sait que c'est un saut conditionnel (à cause du (C)), qui nous amène dans cette partie du programme (normal, on teste le mot de passe, donc il y a une condition), d'autre part, on sait que ce saut se situe à l'adresse 004013F5.

IDENTIFICATION DE LA PROTECTION

Allons voir maintenant à quoi ressemble le saut qui nous amène au texte "Bad password". Pour cela, cliquez sur l'icône 2, et entrez l'adresse vue précédemment. Validez, et vous arrivez à quelque chose qui devrait ressembler à ceci :

```
* Reference To: msvcrt.strcmp, Ord:0282h
                                  |
:004013EB E8A0170000              Call 00402B90
:004013F0 83C410                  add esp, 00000010
:004013F3 85C0                    test eax, eax
:004013F5 7512                    jne 00401409
:004013F7 83EC0C                  sub esp, 0000000C

* Possible StringData Ref from Code Obj ->"Allright. Good Job !"
                                  |
:004013FA 6829134000              push 00401329
```

Avant le saut, on remarque l'instruction Call 00402B90. Un Call est en fait un appel à une fonction (on continue l'exécution à l'adresse en question, puis on reprend juste après le Call). WinDasm nous marque le nom de cette fonction, et dans notre cas il s'agit de "strcmp". Or, "strcmp" est la contraction, en Anglais, de "string compare", soit "comparaison de chaîne de caractères". C'est donc cet appel à la fonction " strcmp " qui va comparer le mot de passe que l'on a entré (qui est une chaîne de caractères) au vrai mot de passe. Et selon le résultat, le saut s'effectuera ou pas.

On remarque ensuite la présence d'un "test eax, eax", qui vérifie le résultat de la comparaison (stocké dans eax). Puis on arrive à la ligne fatidique : le saut conditionnel. La condition à été évoquée précédemment. Nous sommes en présence d'un saut conditionnel particulier, un JNE. JNE signifie Jump if Not Equal (saute si différent). Le saut sera donc effectué si les chaînes de caractères sont différentes, et donc si le mot de passe entré n'est pas le bon. Tout cela est très logique, si on récapitule : si le mot de passe est différent, alors on affiche "Bad password".

Si le saut n'a pas lieu, nous nous apercevons que juste après celui-ci se trouve ce texte : "Allright. Good Job !", qui indique l'entrée du bon mot de passe.

Allez, maintenant on va le cracker, ce programme !

MODIFICATION DU PROGRAMME

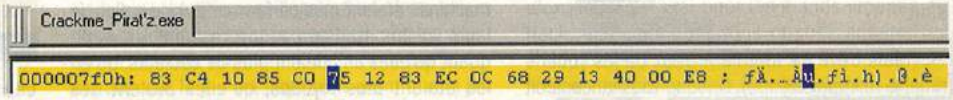
Ce que nous voulons faire, c'est forcer le programme à accepter tous les mots de passe. En d'autres termes, on voudrait que le saut conditionnel vers "Bad password" n'ait jamais lieu. Une instruction assembleur va nous y aider : NOP (No OPeration, codé en mémoire par "90"). Cette instruction indique à l'ordinateur de ne rien faire. Il ne nous reste donc qu'à remplacer le saut JNE, représenté en mémoire par "7512", par "9090", soit deux instructions NOP. Eh oui, toutes les instructions assembleur ne prennent pas la même place.

Le JNE que l'on cherche se trouve en mémoire, à l'adresse 004013F5h. Mais attention, cette adresse est en quelque sorte virtuelle. Pour modifier le programme, il nous faut savoir à quel endroit se trouve cette instruction dans le fichier exécutable. Pour cela, il faut sélectionner l'instruction et regarder en bas de la fenêtre principale de WinDasm. On obtient :

```
Line:693 Pg 14 of 91  Code Data @:004013F5 @Offset 000007F5h in File:Crackme_Pirat'z.exe
```

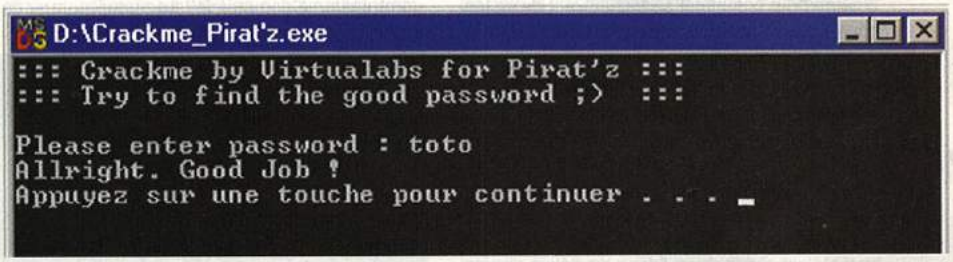
La partie qui nous intéresse est celle qui suit le " @Offset ". La valeur qui suit est en fait la position réelle du code dans le fichier (dans notre cas, c'est 7F5h). On a donc maintenant tous les renseignements pour modifier le fichier directement, sans avoir à recompiler le programme (ce qui est normalement chose impossible, vu que l'on ne dispose pas du code source).

Et c'est là que l'éditeur hexadécimal intervient. Il permet d'éditer un fichier en code hexadécimal, ainsi nous pourrons modifier le code opération "7512" en "9090" sans trop de problèmes. Pour cela, lancez Ultra Edit 32, puis ouvrez l'exécutable. Cliquez ensuite sur "Search" puis "Goto Line". Tapez cette adresse hexadécimale : "0x7F5", et validez. Vous arrivez à ceci :



Modifiez ainsi le "75" puis le "12" en "90" et "90", et enregistrez. Lancez le programme et entrez un mot de passe bidon, "toto" par exemple, puis validez. On obtient ce résultat :

Mais nous nous sommes aussi fixés pour objectif de trouver ce mot de passe. Un simple coup d'œil aux String Datas References nous donne la solution : "X22-1%344" n'apparaît nulle part dans l'affichage du programme. On en déduit rapidement que c'est le bon mot de passe, ce qu'un test sur le programme non modifié confirme :-)



Ça y est, on a trouvé le mot de passe et le programme a été modifié afin d'accepter tous les mots de passe ! Vous voyez bien que ça n'était pas plus compliqué que ça... Bien sûr, je n'explicite pas la création de crack, ce n'est pas le but de cet article. Dans le prochain numéro, je dévoilerai d'autres facettes du reverse engineering, car le cracking n'est pas le seul emploi que l'on peut en faire. En attendant le prochain Piratz, entraînez-vous bien !

Virtualabs

LA SCENE DU CRACKING

Le piratage est peut-être condamnable mais, depuis son apparition, ses usages et sa culture ont plus suscité de vocations de programmeurs de génie et d'artistes de talent que de truands invétérés. Et si l'on s'intéressait à cette vague créative ?

N'avez-vous jamais téléchargé sur un réseau FastTrack (ou sur KaZaa pour les incultes) un joli petit fichier exécutable de 150 mégaoctets environ, contenant l'un des derniers jeux venant de sortir ? Si vous lisez Pirat'Z, je suis sûr que vous êtes déjà tombé sur ce genre de choses (sans doute par hasard, n'est-ce pas ?). D'ailleurs, le piratage est l'une des activités les plus pratiquées sur Internet, soit dit en passant.

Mais trêve de morale à deux balles (quelle rime, je m'impressionne). Lorsque vous lancer ledit fichier, oh surprise ! Une curieuse musique met en vibration vos tympans, tandis qu'une sublime interface graphique se lance, offrant une débauche d'effets visuels de tous genres, alors qu'un texte faisant défiler des noms tous plus biscornus les uns que les autres (genre µa][, Kn1ghterz,ou bien encore x9x0x9x). Ensuite, après avoir lancé l'installation, en vibrant au son de l'électro la plus old-school qui soit, vous allez dans le répertoire du programme, où on vous demande de lancer un petit utilitaire DOS qui prendra presque un quart d'heure pour compléter sa tâche avant de se fendre d'un superbe "Thank you, if you like this game, go buy it !".

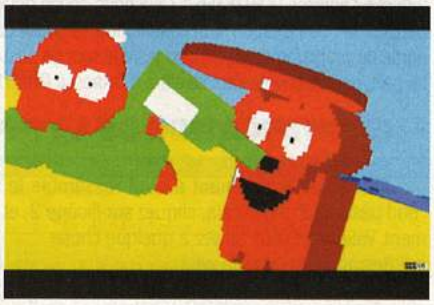
Dans ce cas, vous avez affaire a ce qu'on appelle un "release", c'est à dire un programme qui est étudié sous toutes ses formes afin de proposer le meilleur du soft en prenant le moins de place possible. De plus, le vrai release s'accompagne obligatoirement d'une superbe présentation graphique et d'une musique extrêmement stylée électro a la Juan Atkins du début des années 80. En fait, tout ceci est réalisé par une équipe de crack, en perpétuelle compétition avec les autres teams pour sortir les premiers le jeu le plus attendu (car bien sûr, les équipes de cracks balancent les jeux avant même qu'ils ne soient sur le marché), avec la meilleure musique, la meilleure compression et la meilleure interface.

AH... LES PROGRAMMES DE 3 KO !

Cette tradition n'est pas nouvelle. Dès l'Amiga et l'Atari, et même avant (pour ceux qui sont trop jeunes, voir Pirat'z N° 5) les équipes de crack rivalisaient d'audace afin de promouvoir leurs machines favorites, les amigaïstes criant que leurs machines étaient plus performantes que celles de leurs voisins ataristes, et inversement, en expliquant qu'elles affichaient plus de couleurs, qu'elles étaient plus rapides, qu'elles avaient des capacités sonores extraordinaires, qu'elles faisaient les courses et qu'elles étaient terribles au lit... Oups ! Non ptet' pas quand même, mais certains étaient à deux doigts de dire ce genre d'inepties. Et quelle est la meilleure manière de prouver que sa machine est meilleure que celle du voisin ? Tout simplement en écrivant des programmes aussi géniaux qu'inutiles !

Ces intros, cracktros, ou démos, étaient parfois distribuées toutes seules. Mais quitte à prouver que sa machine est meilleure, autant donner un programme commercial avec pour montrer ce qu'elle vaut vraiment. C'est donc une sorte de guéguerre amicale entre ataristes et amigaïstes.

Mais au fil du temps, les Amiga et les Atari ayant disparu du marché, les groupes de cracking comprirent que leur avenir était dans le release pour DOS, puis pour Windows. Mais tous ceux qui faisaient des cracktros ne voulaient pas forcément s'engager autant que les distributeurs de copies. La scène s'est donc scindée en deux groupes, les "démo" et les "crackers". En fait, le crack n'est à la base qu'une démo qui fournit un programme cracké avec son cracktro (ou l'inverse, question de point de vue). C'est pourquoi des équipes très performantes, comme par exemple CLASS (sans doute le number one avec les maîtres un peu essoufflés razor1911, encore aujourd'hui, quoique



très fortement concurrencées par les jeunes surdoués de chez MYTH) qui ont décidé de tout porter à un niveau bien supérieur aux vieux cracktros un peu débiles et des démos belles mais sans but véritable à part la beauté.

Le but à présent est de fournir des programmes ou des jeux très bons, tout en donnant un artwork très poussé. Un membre de CLASS qui créait les artworks pour les installations expliquait dans un post que j'ai dégoté après de longues et fastidieuses recherches sur les forums de sites de "scènes" cracktros tel le fameux www.defacto2.org ou bien sur www.scene.org : "Nous nous devons non seulement de faire connaître des programmes ou des jeux à des gens qui ne veulent pas risquer leur pognon à les acheter sans connaître mais qui n'ont pas non plus envie de télécharger une démo complètement bidon et qui ne représente rien. C'est pourquoi il me semble que c'est la moindre des choses de fournir un artwork de grande qualité, par respect du programme que nous distribuons. Enfin bon, en même temps c'est aussi pour montrer que c'est nous les meilleurs et que personne ne nous arrive à la cheville ;)..."

... EH BEN MOI, JE SUIS UN MYTH

On voit donc bien que le but est double. D'une part, faire connaître un programme aux gens, d'autre part, une sorte de compétition informatique entre les différentes teams. Mais il y a encore plus que cela. Ces dernières années, la politique des grandes distributions du jeu vidéo ou du software a beaucoup évolué. Désormais, les teams de crack ont une nouvelle volonté : faire la nique aux majors. D'ailleurs, lorsqu'une team de crack a été démantelée par la police il y a deux ans, quelle ne fut pas la surprise des juges quand il apprirent qu'elle était constituée à 90 % de programmeurs professionnels !

En effet, d'un point de vue purement technique, les releases comme les cracktros sont de véritables tours de force et nécessitent véritablement de solides compétences en matière d'informatique. Prenons par exemple l'assez récent GTA III : alors qu'il tient sur deux CD-ROMS à l'origine, le release pèse... 132 mégaoctets. Et il ne

manque que les musiques. Cela est rendu possible par des algorithmes qui ont été développés par et pour les crackers. Le plus connus est sans doute UHARC (pour Ultra High ARchive Compressor). Développé par une personnalité plus ou moins bidon (le site officiel qui tient sur une page ne présente aucun véritable renseignement et n'a pas été mis a jours depuis deux ans),c'est principalement lui qui permet des taux de compression aussi importants.

Les données en elles mêmes sont compressées, recompressées, converties en fonction de leur type puis reconverties (rollback) lors de l'installation. Un exemple très simple, si un jeu utilise des textures en BMP, elles sous toutes converties en PNG, puis reconverties en BMP pour que le jeu puisse fonctionner.

Et ainsi de suite, jusqu'à des techniques dix fois plus compliquées. Contrairement à ce que l'on peut penser, il ne suffit pas de lancer une simple commande et d'attendre que tout se compresse. C'est beaucoup plus complexe que cela.

D'ailleurs, une petite anecdote : chaque année est organisé sur un des sites de la "scène" un grand concours ouvert à toute team ayant au moins publié trois releases : le "32k App Contest". Il s'agit de proposer la meilleure application ou jeu possible tout en restant en dessous de la barre de 32 ko (le programme doit bien entendu n'être qu'un fichier exécutable "sans rien autour"). Le grand gagnant d'il y a deux ans était MYTH, avec son Turrican32k. Un niveau entier de turrican avec musique, effets sonores et visuels, pleinement jouable. Sachez que pour finir un niveau entier de turricanil, il faut au moins 5 minutes... Cela montre bien le haut niveau de maîtrise des teams de crack dignes de ce nom.

Et surtout, c'est une des preuves que les équipes de crack les plus importantes sont surtout formées de professionnels qui travaillent sur les jeux qu'ils crackent. Sinon, comment pourraient-ils connaître l'algorithme de compression des fichiers de GTA par exemple, alors qu'il est totalement fermé et qu'aucune information n'est disponible librement ? Ce n'est pas en bidouillant des nuits entières qu'ils y arrivent ! Le plus difficile pour les teams de crack est alors de survivre sans se faire choper...

TOUS EN PRISON ?

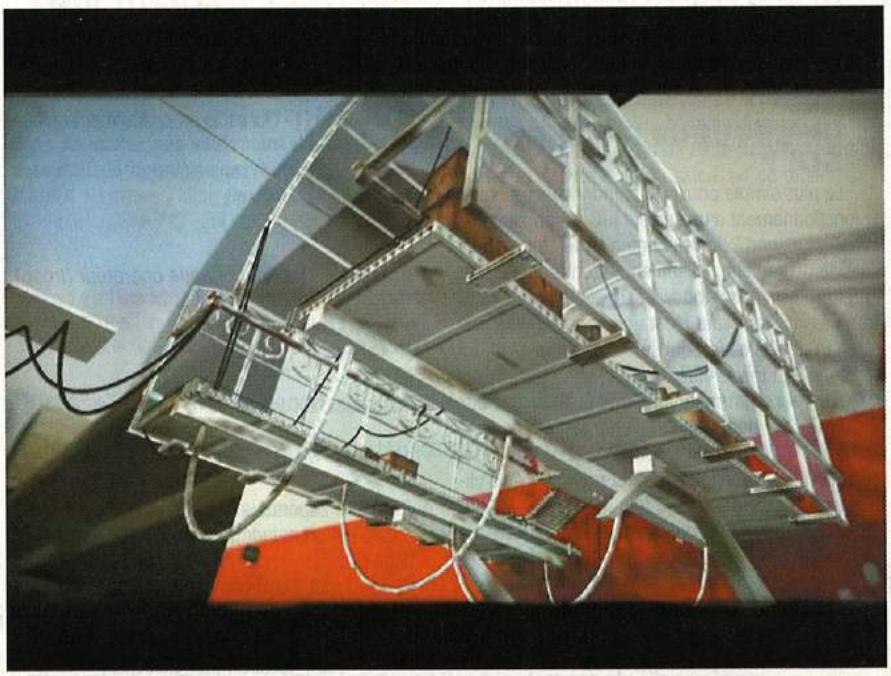
Car la pratique des teams de crack est bien évidemment totalement illégale. Des développeurs de jeux vidéos qui se sabordent eux-mêmes, dites-vous ? Bien sûr que non. Il faut savoir que le studio qui crée le jeu est payé bien avant que le jeu ne sorte : c'est le parfait contraire du cinéma. Dès lors, il devient difficile pour les majors de l'entertainement d'expliquer que lorsqu'on joue un jeu cracké, on prive les développeurs de nourriture. Car ceux qui sont vraiment fans du jeu iront l'acheter, exactement comme pour les mp3 sur Internet. On en arrive donc à la dimension idéologique des groupes de hack, dont l'idéologie pourrait se résumer à cette phrase : "Ce n'est pas parce que les gens vont essayer un jeu cracké que le marché de jeu vidéo va s'écrouler." Mais d'un autre côté, un vol reste un vol. Des petits malins s'empresseront d'ajouter à cette affirmation : "Sans doute, mais qui vole qui ?" ;)

Méfiance tout de même. Si ce que je viens d'expliquer est vrai pour les grands groupes de hack, tels ceux dont vous pourrez admirer les cracktros anciens ou récents sur DefactoZ, cela n'est en rien comparable avec les crashers qui balancent bêtement les isos sur Bittorent en les accompagnant d'un fichier texte minable se fendant d'un superbe "FUCK UNIVERSAL RULEZ" aussi constructif qu'intéressant. Ces mecs pourrissent toute l'idée des teams de crack et du cracking en général : n'importe qui peut faire un iso, le balancer sur BT ou FastTrack, et se prendre pour le Robin des Bois numérique du 21e siècle.

Etant à la fois graphiste et musicien, il m'arrive souvent de télécharger des releases de jeux qui ne m'intéressent pas du tout, juste pour voir le cracktro et l'install, pour voir de quelle inventivité et de quel humour font preuve les crackers dignes de ce nom... Entre les ASCII-arts (fichiers textes ASCII formant des logos aussi durs à déchiffrer que celui d'un groupe de black-métal) et les musiques faites au tracker dont le principe n'a pas évolué depuis 20 ans, il me semble parfois que le véritable intérêt des CLASS, des razor1911 et des MYTH est de vouloir faire perdurer une des seules traditions informatiques issues de l'Amiga et de l'Atari, dans un intégrité qui a tendance à se raréfier de plus en plus sur Internet de nos jours...

Cet article n'est en aucun cas une apologie du piratage ou une leçon de morale, il est simplement un point de vue sur des activités réelles.

KLASTEK TIMRAK



A VOIR :

www.defacto2.net **: l'archive de cracktros en tous genres.**

www.scene.org **: LE site de la "scene" (allez voir dans Jobs, EA, Team17, etc. recrutent)**

www.scenemusic.net **: écoutez cette radio online grâce à winamp et vibrez au son du tracker d'il y a 20 ans.**

DEVENEZ LE MAITRE SUR IRC

On ne s'en rend pas toujours compte, mais la majorité des sites de chat utilise un serveur IRC. Vous allez apprendre dans cet article à en faire un vous-même, et à mieux maîtriser vos séances de chat.

IRC... Ces trois lettres reviennent fréquemment sur les sites que vous parcourez ? En connaissez-vous la signification ? Savez-vous que c'est un protocole avec ses propres règles ? Avez-vous déjà imaginé devenir l'administrateur d'un serveur IRC ? Etes-vous totalement anonymes sur un tel serveur ? Cet article a pour but de répondre à ces questions en éclaircissant les divers points sombres.

QU'EST-CE QUE L'IRC ?

Tout d'abord, IRC signifie "Internet Relay Chat". Pour les personnes se répétant depuis le début de cet article "mais c'est quoi cet IRC et à quoi ça sert?!!", on peut l'introduire en le définissant comme étant un moyen simple, efficace et sécurisé de dialoguer à plusieurs en mode texte (on le nomme également comme étant le chat... j'imagine les "ahhhh, il pouvait pas le dire plus tôt ?"). Vous connaissez les protocoles http ou encore ftp, et bien IRC est également un protocole internet qui a ses propres spécifications dans la RFC 1459 pour les lecteurs avides de connaissances.

Je pense que tout le monde a déjà " tchaté " sur le Web et s'est rendu compte qu'une fois connecté, on peut rejoindre des salons toujours précédés du signe # (exemple le salon #piratz). Dans ces salons sont présents des utilisateurs avec différents niveaux de pouvoir : les @ (opérateurs ou administrateurs), les % (demi-opérateurs, ou modérateurs), les + (les voicés en Anglais dans le texte ou utilisateurs possédant l'usage de la parole, ce qui signifie qu'ils peuvent continuer à envoyer des messages même si le salon est modéré), et enfin les utilisateurs de base n'ayant aucun signe distinctif. Voyons maintenant un peu plus loin et intéressons-nous à la machine sur laquelle nous sommes connectés.

QU'EST-CE QU'UN SERVEUR OU RESEAU IRC ?

Imaginez que votre PC tourne actuellement sur un système d'exploitation quelconque (Windows, Linux ou autre), imaginez maintenant que vous lancez un programme.

A présent, faisons le parallèle avec un serveur IRC : le PC est le serveur, le système d'exploitation est le plus souvent Linux, le programme que vous lancez est un IRCd (IRCdeamon). Ce deamon IRC est aussi appelé un serveur...c'est ce deamon qui une fois lancé va gérer toutes les tâches qui découlent de l'IRC côté serveur : connexion des utilisateurs, réception des messages puis renvois de ceux-ci vers les autres utilisateurs, etc.

Ensuite peuvent venir s'ajouter ce que l'on appelle des services, c'est un programme spécifique pouvant gérer l'enregistrement des pseudos ou autres salons (correspondant à nickserv et chanserv pour les services anope).

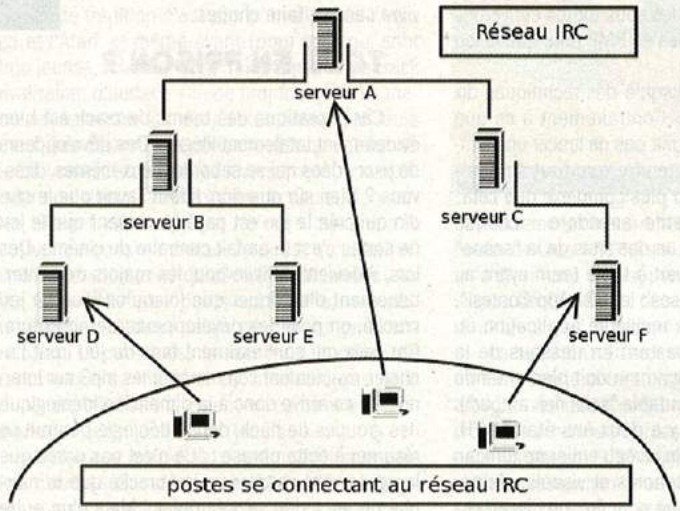
De nombreux IRCd et services existent sur le Net. Les plus connus sont sûrement UnrealIRCD et les services anope qui, associés, forment à l'heure actuelle une grande partie des réseaux IRC.

Bien évidemment, un réseau IRC est un ensemble de serveurs IRC interconnectés.

Comment sont-ils connectés ? Imaginez un arbre, le réseau est calqué sur l'architecture de ses branches (schéma).

PIRAT'Z SUR IRC

Retrouvez l'équipe de la rédaction en direct ! Pirat'z va ouvrir son salon IRC. Rendez-vous sur http://piratz.fr.st pour savoir où et quand.



L'architecture de l'IRC

Ici, le serveur A est le serveur central, mais tous les salons sont accessibles depuis le Serveur F tout aussi bien que par le Serveur D. Un réseau peut très bien n'être constitué que de deux serveurs comme six.

UN SERVEUR IRC CHEZ SOI ?

Le plus simple pour comprendre concrètement le fonctionnement d'un serveur IRC est encore d'en installer un, non ? Je vous entends déjà dire "mais j'ai pas de serveur, j'ai seulement un ordinateur et en plus il est sous Windows". Où est le problème ? Tout ce qu'il vous faut c'est une connexion au Net et un PC. L'explication qui suit s'applique aux postes sous Windows. Allez, suivez le guide :

On va commencer par installer ce fameux IRCd qui sera Unrealircd. Téléchargez-le à l'adresse http://www.unrealircd.com/?page=downloads, sélectionnez la version win32 et un miroir puis cliquez sur "download". Une fois le téléchargement achevé, vous n'avez qu'à lancer le .exe et vous laisser guider.

Maintenant le plus gros du travail arrive : vous devez avoir un fichier :
Unreal3.2\doc\example.conf. Copiez-le dans le dossier Unreal3.2 et renommez-le en unrealircd.conf. Vous obtiendrez donc un fichier Unreal3.2\doc\unrealircd.conf.

Il vous reste à l'éditer et à le modifier en fonction de vos envies. Pour cela, des explications sont données sous forme de commentaires avant chaque bloc de configuration, à moins d'être totalement anglophobe, cela ne pose pas trop de problème...

Bon d'accord, vous êtes perdu pour la configuration, voici les principaux points à modifier :

- **Bloc me{}** - *C'est ce qui définit le serveur.*

```
me{
  name "127.0.0.1";
    /*si vous possédez un nom de domaine en .com
      .org  etc... mettez-le ici, sinon mettez votre ip
    */
  info "Serveur pour Pirat'z";
    /*choisissez un nom*/
  numeric 1;
};
```

- **Bloc admin {}** - *Qui est le propriétaire du serveur ?*

```
admin {
  "Votre_pseudo"; /* sans espaces */
  "votre_mail@fai.com";
};
```

- **Bloc oper {}** - *Pour chaque opérateur (Ircop) :*

```
oper pseudodeloper {
  class clients;
  from {
    userhost *@*.wanadoo.fr;
  };
  password "MotDePass";

  /* Ce que l'opérateur peut faire.
     Là c'est un netadmin, c'est top. */
  flags {
            get_host; can_stealth; global; local;
            services-admin; admin;
            can_wallops; can_globops;
            can_localkill; can_globalkill;
            /* ... pleins d'autres choses */
            ; can_zline; get_umodew; netadmin;
  };
};
```

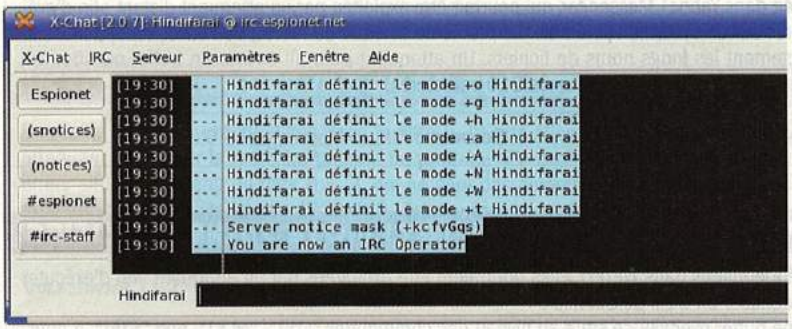
Ce sont les seuls blocs que vous ayez à modifier.... Il vous reste uniquement à vérifier, si vous avez un firewall, qu'il ne bloque pas le port 6667 (celui défini comme étant le port actif de votre IRCd dans le fichier de configuration).

Vous n'avez plus qu'à lancer l'exécutable .../Unreal3.2/unreal.exe et votre IRCd sera opérationnel !!! :) Si vous êtes déjà allé sur un serveur IRC, vous devez avoir souvenir d'avoir lu le message "pseudo is now a net-admin N". Eh bien maintenant, pseudo ne sera autre que vous !! Il vous reste donc à vous connecter au serveur et à tester votre nouvel accès net-admin...

Je vous conseille pour cela de vous servir du logiciel Xchat, qui est disponible sur les plate formes Windows et Linux à l'adresse : http://xchat.org/ (Windows version si vous êtes sous Windows évidemment). C'est un logiciel libre, et gratuit, naturellement.

Donc, l'adresse de votre serveur n'est rien d'autre que votre ip, et le port est 6667 si vous l'avez laissé par défaut dans unrealircd.conf (adaptez en fonction de la configuration).

Une fois connecté, tapez /oper VotrePseudo-Dadmin VotrePassDadmin. Et là, si tout se passe bien, vous verrez apparaître le message "You are now an IRC Operator" (voir photo d'écran).



LES COMMANDES IRCOP QUI TUENT

La commande que vous testerez en premier

KILL : syntaxe /kill (pseudo) (raison)

Effet : déconnecte du serveur l'user correspondant au pseudo.

Vous ne voulez pas seulement déconnecter un user mais le bannir du serveur ?

KLINE : syntaxe /kline (hostmask) (raison)

Exemple : /KLINE *@*.aol.com lit pas Pirat'z

Les actions forcées sur les users/salons

SAJOIN/SAPART :

Syntaxe :

/sajoin (pseudo) (salon) ou

/sapart (pseudo) (salon)

Effet : force un user à joindre ou quitter un salon.

SAMODE : syntaxe /samode (salon) (mode)

Effet : vous pouvez changer les modes du salon sans avoir le statut d'op sur ce même salon.

SANS ÊTRE IRCOP ?

Bon, là vous faites la loi sur votre réseau privé. Sur celui d'un autre, vous n'êtes que simple utilisateur. Il y a pourtant une ou deux commandes à connaître, qui peuvent vous aider.

Liste des utilisateurs

Syntaxe : /who [pseudo ou #salon ou masque]

Effet : Utilisée suivie d'un nom de salon, cette commande donne la liste des utilisateurs présents sur celui-ci. Sur certains réseaux, on peut aussi avoir des listes d'users en fonction de certains critères. Par exemple : /who *.wanadoo.fr qui donne parfois la liste de tous les abonnés connectés par ce fai.

Liste des salons

Syntaxe : /list [critères]

Effet : Renvoi une liste complète des salons présents sur le réseau. Sur certains réseaux, vous pouvez mettre des critères de recherche. Par exemple, un morceau du nom du salon, ou du topic : /list *hack* ou /list hack.

Quote list

Syntaxe : /quote list options

Effet : Cette commande est une extension de la commande LIST, elle permet d'obtenir une liste des salons filtrée grâce à certains paramètres, voici la liste des options disponibles sur certains serveurs :

< ou >nombre - liste les salons ayant un nombre d'occupant inférieur ou supérieur à nombre,

C< ou>nombre - liste les salons créés avant ou depuis il y a nombre minutes,

T< ou >nombre - liste les salons qui ont un sujet vieux de moins ou de plus de nombre minutes,

Ici on utilise /quote pour envoyer la commande brute au serveur. Sinon, votre client risque d'interférer dans les paramètres.

Vous pouvez aussi utiliser les services pour obtenir des informations. Si le serveur utilise les classiques nickserv/chanserv, vous pouvez essayer :

/msg nickserv info (nick) ou

/msg chanserv info (#salon)

Enfin, si un chat utilise une applet, vous avez probablement envie de vous y connecter avec un vrai client (mIrc, ou plutôt Xchat). Tapez : /map dans l'applet, vous apprendrez sans doute le nom du serveur à entrer à la connexion. À essayer aussi : /lusers.

IRC CONFIDENTIEL ?

C'est simple : toutes les informations transitant par un serveur ou un PC peuvent être interceptées et enregistrées... Jusque-là, vous êtes d'accord. Maintenant, il suffit de faire le rapprochement en considérant vos messages comme étant les informations et le serveur comme étant la machine hébergeant l'IRCd. Le serveur peut conserver la trace de toute information ayant transité par lui, y compris vos messages personnels, vu que l'IRC n'est pas crypté. Voir l'illustration.

Donc, rien n'est confidentiel sur IRC ? Je n'ai jamais dit ça ! Si vous voulez qu'un query soit impossible a enregistrer par le serveur, faites un dcc chat (/dcc chat pseudo). Cela créera un query direct qui ne passera pas par le serveur IRC. Ce sera une liaison directe entre les deux users (d'ip à ip). Dès lors, aucunes des informations échangées ne peuvent être enregistrées. Du moins depuis le serveur IRC où vous êtes...

En espérant bientôt vous voir sur un serveur IRC.

Hindifarai

```
⊞ Transmission Control Protocol, Src Port: 6667 (6667), Dst Port: 4
⊟ Internet Relay Chat
    Response Line: :Spolix!~nadine@192.168.0.KK0= JOIN :#Piratz

⊞ Transmission Control Protocol, Src Port: 6667 (6667), Dst Port: 4209 (420
⊟ Internet Relay Chat
    Response Line: :Bikette!~nadine@192.168.0.KK0= JOIN :#Piratz
```

Spolix et Bikette entrent sur le serveur Piratz...

```
⊟ Internet Relay Chat
    Response Line: :Bikette!~nadine@192.168.0.KK0= PRIVMSG #Piratz :lu
⊟ Internet Relay Chat
    Response Line: :Spolix!~nadine@192.168.0.KK0= PRIVMSG #Piratz :hi
```

Bikette tombe à l'eau qui reste sur le bateau ? Heu non c'est pas ça :-/ Ils se saluent

```
⊞ Transmission Control Protocol, Src Port: 4210 (4210), Dst Port: 6667 (6667), Seq: 2402737218, Ack: 12729761
⊟ Internet Relay Chat
    Request Line: PRIVMSG Spolix :bon alors maintenant kon est entre nous javai un truc important a te dire
```

Un message privé est envoyé à Spolix, on peut lire tout ce qu'il contient...

Séance de sniff sur un serveur IRC !

LES DERNIERES VULNERABILITES

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

LE FAUX POISSON DE GOOGLE

Imaginez, le premier avril, Google annonce au monde entier le lancement d'un produit révolutionnaire : GMail, un service de courrier électronique gratuit proposant pas moins d'un Go d'espace libre pour stocker ses emails ! Aussitôt, gros éclat de rire sur Internet, bonne blague, haha, on a failli y croire. Du coup, Google tente tant bien que mal de convaincre les gens, mais si, mais si c'est vrai, c'est pas drôle du tout. Il aura fallu quand même attendre le lendemain pour se rendre compte qu'en effet, Google était tout ce qu'il y a de plus sérieux. Par contre, le mode de financement de GMail est loin de soulever l'unanimité. En effet, Google analyserait le contenu de vos emails afin de vous proposer des publicités en rapport avec vos centres d'intérêt. Ce qui est évidemment une atteinte assez inquiétante au contenu privé de vos correspondances, même si Google affirme que promis, tout sera automatisé et aucune information personnelle ne filtrera. Mouais, moi je suis sceptique, et je verrais bien le service devenir payant d'ici un certain temps, prenant en otage ses utilisateurs.

PIRATAGE... D'UNE STATION ESSENCE !

Un piratage pas comme les autres... En effet, plusieurs dizaines de personnes ont été arrêtées par les autorités françaises. Motif : piratage d'une station essence de Seine-et-Marne. Ces personnes avaient mis au point une bidouille sur la pompe qui délivre le carburant. Un bouton caché sur celle-ci permettait d'annuler les transactions par carte bleue. Bilan : 29 mètres cubes d'essence envolés pour un total de 27 000 euros ! Bien entendu, les coupables vont devoir rembourser, avec en prime une jolie amende !

MICROSOFT WINDOWS ASN.1 LIBRARY REMOTE CODE EXECUTION

Une vulnérabilité critique a été identifiée dans la librairie Microsoft ASN.1, elle pourrait permettre l'exécution de code arbitraire. Cette faille est provoquée par la présence d'un buffer overflow dans MSASN1.DLL. Un attaquant distant pourrait exploiter ce problème via des services de sécurité tels que Kerberos ou NTLMv2, ou via des applications utilisant des certificats. L'exploitation réussie permettra l'exécution de commandes arbitraires avec des privilèges SYSTEM..

VULNÉRABLE : Microsoft Windows NT / 2000 / XP / 2003 **SOLUTION :** MS04-007

YAHOO! MESSENGER FILENAME BUFFER OVERFLOW VULNERABILITY

Une vulnérabilité a été identifiée dans Yahoo! Messenger, qui 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

WFTPD SERVER/PRO SERVER 3.X MULTIPLE REMOTE VULNERABILITIES

Plusieurs vulnérabilités ont été identifiées dans WFTPD. Elles pourraient être exploitées par un attaquant afin d'exécuter des commandes arbitraires ou causer un Déni de Service :

1) Le premier problème, de type buffer overflow, se situe au niveau des commandes "LIST", "NLST", and "STAT". Il pourrait être exploité en envoyant un argument contenant le caractère " -" suivi d'une très longue chaîne de caractères. L'exploitation réussie provoquera l'exécution de commandes arbitraires avec les privilèges du serveur WFTPD.
2) Plusieurs erreurs sont présentes dans différentes commandes ftp, ce qui pourrait provoquer une utilisation abusive du CPU (100 %) et causer le crash du serveur.
3) Si l'option "XeroxDocutech" est paramétrée à "1", il est possible de provoquer le crash du serveur en envoyant des arguments spécifiques via les commandes "MKD" et "XMKD".

VULNÉRABLE : WFTPD 3.21 Release 1 et versions inférieures **SOLUTION :** WFTPD 3.21 Release 2

CHECK POINT VPN-1 & CHECK POINT FIREWALL-1 REMOTE VULNERABILITIES

Une vulnérabilité critique a été identifiée dans CheckPoint VPN-1 Server et ses Clients VPN. Elle pourrait être exploitée par un attaquant afin de compromettre un système vulnérable. Ce problème résulte d'une erreur de type buffer overflow, présente dans le processus d'authentification ISAKMP. Un attaquant peut exploiter cette faille en envoyant une requête spécifique "Certificate Request" pendant la phase initiale de négociation IKE, ce qui provoquera l'exécution de commandes arbitraires avec les privilèges "SYSTEM" ou "ROOT".
Plusieurs vulnérabilités critiques ont été identifiées dans Check Point FireWall-1, et pourraient être exploitées par des attaquants distants afin de compromettre un système vulnérable. Ces failles sont causées par une erreur de type format string présente dans les modules "Application Intelligence" et "HTTP Security Server". Le module Firewall-1 NG HTTP Application Intelligence (AI) est une application de type proxy dont le but est d'empêcher certaines attaques ou de détecter des anomalies dans les protocoles. HTTP Security Server, quant à lui, permet l'analyse et le filtrage du trafic. Le problème est que ces deux modules ne gèrent pas correctement certaines requêtes HTTP, ce qui pourrait être exploité afin d'exécuter des commandes arbitraires avec les privilèges "SYSTEM" ou "ROOT".

VULNÉRABLE : Check Point VPN-1 & Check Point FireWall-1 **SOLUTION :** VPN-1/FireWall-1 4.1

WINDOWS XP HTML FAKE FOLDER CODE EXECUTION VULNERABILITY

Une vulnérabilité a été identifiée dans Microsoft Windows XP. Ce problème touche l'Explorateur Windows. il pourrait être exploité par un attaquant en créant un fichier malicieux HTML contenant un code arbitraire exécutable (Virus, Trojan, ...). En renommant ce fichier en fichier.folder, il aura l'apparence d'un répertoire sous Windows XP. Ce répertoire malicieux, une fois ouvert par la victime, provoquera l'exécution automatique du code malicieux (avec les privilèges de l'utilisateur).

VULNÉRABLE : Microsoft Windows XP **SOLUTION :** Aucune solution officielle

MICROSOFT DATA ACCESS COMPONENTS BUFFER OVERFLOW

Une vulnérabilité critique a été identifiée dans MDAC (Microsoft Data Access Components), qui 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 : MDAC 2.5, 2.6, 2.7, et 2.8 **SOLUTION :** MS04-003

EXCHANGE SERVER 2003 PRIVILEGE ESCALATION VULNERABILITY

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

MICROSOFT ISA SERVER 2000 REMOTE CODE EXECUTION VULNERABILITY

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 de 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

MICROSOFT INTERNET EXPLORER FILE EXTENSION SPOOFING VULNERABILITY

Microsoft vient de publier un patch cumulatif fixant plusieurs vulnérabilités critiques présentes dans Microsoft Internet Explorer et identifiées depuis plusieurs semaines (dont la faille "URL Spoof") :
Le dispositif de redirection utilisant le manipulateur "mhtml:" peut être exploité afin de contourner la sécurité d'Internet Explorer, qui normalement interdit aux pages situées en zone " internet " de charger des pages locales. Ce dispositif de redirection peut aussi être exploité afin de placer puis d'exécuter un fichier malicieux sur un système vulnérable (le script sera exécuté dans la zone "MyComputer").

Une vulnérabilité de type Cross Site Scripting peut être exploitée afin d'exécuter un script dans une zone de sécurité liée à un autre page Web si cette dernière contient une subframe. Une variante d'une vulnérabilité corrigée peut être exploitée afin de détourner les déclics d'un utilisateur et effectuer certaines actions à son insu.

Une erreur dans le dispositif de téléchargement peut être exploitée afin d'accéder au répertoire caché d'un utilisateur, en utilisant une page HTM dont le header "Content-Type:" est invalide.

Une vulnérabilité de type "URL Spoofing", qui résulte d'une erreur dans la vérification des entrées. Elle pourrait être exploitée par un attaquant afin de cacher la vraie URL d'une fausse page en incluant les caractères "0x01" "0x00" avant le caractère @. (Ce patch supprimera définitivement la possibilité d'authentification via une URL du type http(s)://user:pass@server/page.ext.)

NOTE : Il est possible de réactiver l'option d'identification via des adresses du type http(s)://user:pass@server/page.ext en modifiant le registre Windows (à vos risques et périls) :
Aller dans :
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\
FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
(si ces clés n'existent pas, il faudra les créer).
Créer une valeur DWORD intitulée iexplore.exe (pour autoriser Internet Explorer).
Créer une valeur DWORD intitulée explorer.exe (pour autoriser Windows Explorer).
Créer une valeur DWORD intitulée nom_du_program.exe (pour autoriser n'importe quel programme utilisant ce type d'identification).
Mettre les valeurs de ces clés à 0.
Reboot :-)

VULNÉRABLE : Microsoft Internet Explorer 6 - 5.5 - 5.01 **SOLUTION :** MS04-004

HOTMAIL ET YAHOO SONT DANS UN BATEAU

Une faille est découverte. Qui coule ? Personne, car la faille est colmatée à temps. C'est ce qui s'est passé avec les webmails Hotmail et Yahoo, dont les filtres anti-scripts pouvaient être contournés (avec IE), ce qui aurait permis de lancer des attaques (genre récupérer le mot de passe de la victime, lire ses emails, etc.). Encore une fois, c'est heureusement un " gentil " qui a découvert cette faille et alerté les compagnies. Le problème, c'est qu'on imagine le nombre de " moins gentils " qui gardent les failles pour eux...

MSBLAST SOUS-ESTIMÉ

MSBlast est sans aucun doute l'un des vers les plus efficaces de l'histoire. Heureusement pour Microsoft, ses effets n'étaient pas trop radicaux (simple plantage de la machine), car les dégâts auraient pu être bien plus importants. Évidemment, sur le coup, la firme de notre ami Billou a tout fait pour calmer le jeu et minimiser l'impact de ce ver, peu reluisant pour l'image de Windows. Il n'empêche que, six mois plus tard, on apprend finalement que le ver s'est beaucoup plus répandu que ce que l'on pensait. En effet, depuis janvier, Microsoft propose, par l'intermédiaire de Windows update, un outil permettant de le détecter et de s'en débarrasser. Les statistiques indiquent que pas moins de 16 millions d'internautes ont été détectés comme infectés par le ver, tandis que 8 millions ont effectivement utilisé l'outil proposé pour l'éliminer. Quand on pense que ce ver circule depuis août dernier, ça fait quand même pas mal de machines contaminées. Auxquelles il faut rajouter tous ceux qui n'osent pas lancer Windows Update parce qu'ils ont une version piratée de Windows...

GRAVEZ VOS FILMS SUR DES S-VCD

POUR BEAUCOUP MOINS CHER QUE SUR DVD-R

La plupart des platines DVD de salon sont capables de lire les S-VCD, un format particulièrement adapté pour compresser les films destinés à être regardés sur un écran télé. Voici comment en fabriquer.

Le Vidéo CD, VCD pour les intimes, est un format vidéo assez pratique puisqu'il permet de graver sur un CD des petits films qui seront ensuite lisibles par un lecteur DVD de salon. Intéressant comme histoire, mais attention, j'ai encore mieux, j'ai le même en plus grand, plus beau, plus rapide et plus puissant : le Super Vidéo CD !

Plus sérieusement le S-VCD est une évolution du VCD développée par un comité de fabricants et de chercheurs chinois pour éviter d'avoir à payer des royalties sur d'autres technologies, principalement le DVD ($$$ quand tu nous tiens). Les caractéristiques finales du projet ont été annoncées à la fin de l'année 1998, devançant le vrai successeur du VCD (celui conçu par les mêmes développeurs) c'est-à-dire le CVD, format qui n'est plus du tout d'actualité.

Au niveau de la qualité, le S-VCD n'atteint évidemment pas le DVD (et oui, on ne peut pas diviser la taille d'une vidéo par 5 sans perdre en qualité), mais surpasse évidemment le VCD avec une résolution d'image plus de deux fois supérieure (480x576 pour le PAL et 480x480 concernant le NTSC). Un autre apport majeur du S-VCD par rapport à son ancêtre est le support des sous-titres et des surtitres, par exemple pour le karaoké (si si, le mot surtitre existe en Français).

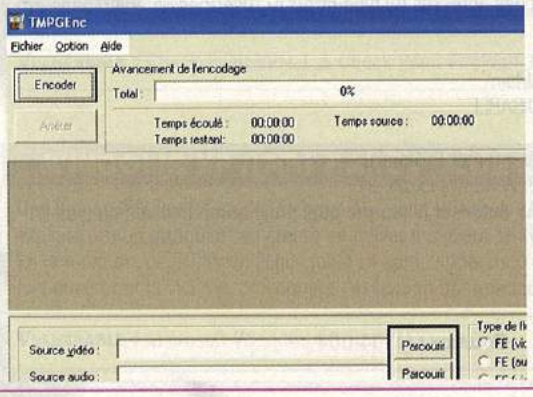
L'inconvénient principal de ce format est que l'on ne peut faire au maximum que 70 minutes de vidéo sur un CD de 700 Mo. Il faut donc prévoir deux disques pour la majorité des films et se bouger du canapé pour faire le changement au milieu du film. C'est vrai que ce n'est pas la mort non plus, ça fait un pause pipi, mais bon, c'est toujours plus agréable sans, à moins que vous ne soyez un fan de la pause pipi, ce qui est assez peu probable.

Pour l'avantage principal, j'en ai déjà parlé tout à l'heure, le S-VCD se grave, comme son nom l'indique, sur un CD. Ce qui veut donc dire qu'un simple graveur CD suffit pour créer ses films, de plus, le prix du CD-R reste encore bien inférieur à celui d'un DVD-R. Enfin cela nous donne suffisamment de raisons valables pour apprendre à créer ces fameux CD.

Ce que nous étudierons en deux étapes, selon le format de la vidéo d'origine : tout d'abord depuis un fichier avi quelconque stocké sur votre disque dur, puis depuis un DVD dans le but unique, bien entendu, d'en faire une copie de sauvegarde.

DE L'AVI AU S-VCD

Nous allons pour cela nous servir du logiciel nommé TMPGEnc. Il est disponible gratuitement sur tous les sites de téléchargement dignes de ce nom, tels que www.telecharger.com ou www.download.com pour les anglophones.

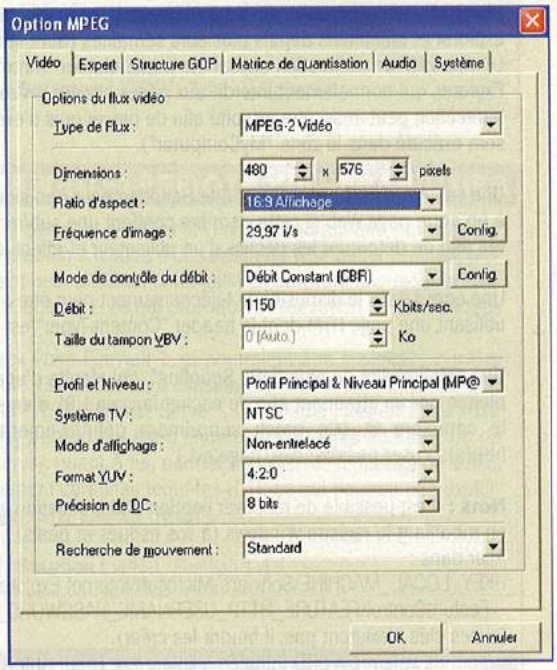


Une fois le logiciel installé, le didacticiel se lance automatiquement. Vous pouvez le fermer, comme on est des vrais de chez vrais, on va évidemment tout paramétrer nous-même. Oui d'accord, c'est vrai que ce n'est pas très dur non plus ;-)

Commencez par cliquer sur le bouton browse à côté du champ "Source vidéo", servez-vous alors de l'explorateur pour sélectionner votre fichier avi et confirmez ensuite par OK. Faites de même pour le champ "Source audio". Il est également possible de faire directement glisser le fichier vidéo dans le champ correspondant, chacun sa méthode ;-)

Le champ fichier en sortie permet quant à lui de choisir où vous voulez stocker le fichier qui sera créé et sous quel nom. Cliquez alors sur le bouton Options pour accéder aux différents paramètres. Accédez à l'onglet Vidéo, et c'est parti pour la check liste :

-type de flux : MPEG-2 Vidéo,
-dimensions : En général 480 * 576 mais 352 * 576 est aussi accepté. La qualité sera alors moins bonne mais le fichier moins gros. Vous verrez ce qui vous convient le mieux une fois que vous aurez l'habitude. Personnellement, je suis assez chiant lorsque la qualité n'est pas top, donc je préfère le 480*576, mais ce n'est que mon avis.
-ratio d'aspect : Au choix, selon vos préférences et votre télé ; 4/3 ou 16/9.



On peut maintenant passer à l'onglet Expert, et oui c'est pour nous cet onglet =) lol

Dans Ratio d'aspect, sélectionnez le ratio de la vidéo d'origine, indiquez si votre fichier avi contient un film au format 4/3, 16/9 ou encore 1/1. Le reste n'a pas à être modifié, les différentes cases en dessous correspondent à des réglages plus précis, je ne vais pas commencer à vous expliquer ce

'Z

CROTTE CROTTE CODEC

Qui n'a jamais eu de problèmes avec un fichier vidéo qui refusait de se lire, faute du codec approprié ? C'est très frustrant, surtout lorsqu'on entend quand même le son (" oh oui, oh oui "). Et le moins que l'on puisse dire, c'est que l'option " télécharger le codec " de Media Player a un taux de réussite assez proche de 0. Pour éviter les prises de tête, vous pouvez par exemple vous rendre du côté de " Codec Pack All in 1 " qui, comme son nom l'indique, regroupe la plupart des codecs populaires aujourd'hui. Ça se passe sur http://www.free-codecs.com/download/Codec_Pack_All_in_1.htm. Avec ça installé, la plupart des vidéos devraient tourner sans se faire prier. Mais s'il y en a encore qui vous résistent, tout n'est pas perdu : il existe un programme qui pourra vous aider, VideoToolBox. Ce logiciel affiche plein d'infos sur un fichier vidéo, en détectant notamment les codecs, qu'il va même télécharger tout seul comme un grand. Ah, on me susurre à l'oreille que le player de VideoLan (www.videolan.org/vlc) lit pas mal de formats aussi. À la poubelle, Windows Media Player !

LES ANCÊTRES DE LA MPAA SONT DES PIRATES

D'après Wired, alors qu'aujourd'hui la MPAA tente tant bien que mal de faire respecter ses droits, c'est bien en piratant qu'elle a fait ses débuts. Au début du 20e siècle, les réalisateurs de films ont traversé tous les États-Unis d'Est en Ouest (vers la Californie) afin d'échapper aux brevets de l'inventeur Thomas Edison. À cette époque, la distance était suffisante pour échapper à la loi, et Hollywood a pu se développer en toute illégalité, le temps que les brevets expirent (au bout de 17 ans). C'était le passage culture du numéro.

à quoi chacun correspond, sinon vous risquez de vous tirer une balle, mais si cela vous intéresse, je suis sûr que notre ami Google saura vous fournir tous les renseignements et bien plus encore.

Et voilà ! Vous pouvez maintenant cliquer sur OK et enfin sur le bouton Encoder, en haut à gauche de la fenêtre principale. Le film va alors défiler sous vos yeux au centre de la fenêtre tandis que le nouveau fichier sera créé. Cette opération peut être assez longue si votre PC est un peu vieux et le manque de Ram risque de se faire sentir si vous n'atteignez pas les 256 Mo.

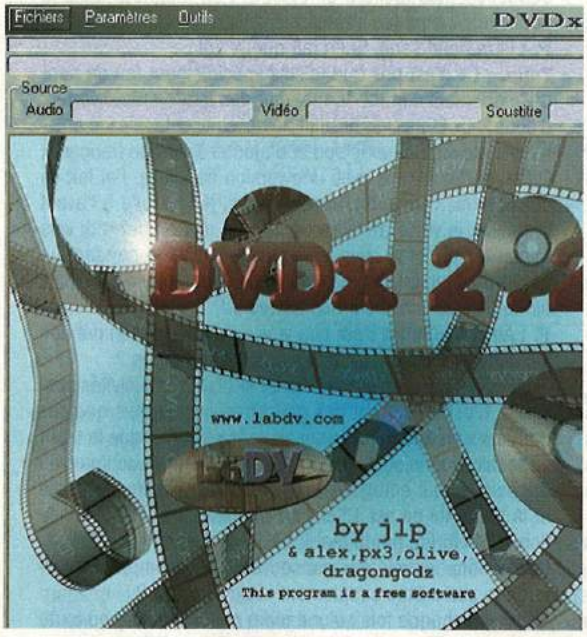
A part ces petits désagréments, tout devrait bien se passer pour obtenir votre nouvelle vidéo fraîchement encodée.

COPIER UN DVD

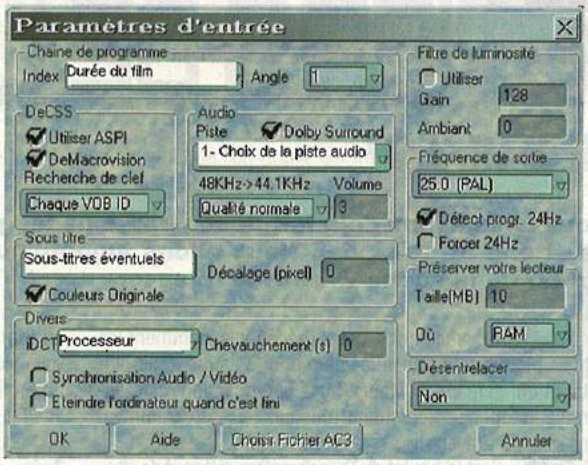
Bien, passons maintenant au deuxième cas : vous venez d'acheter le DVD du nouveau super film que vous attendiez depuis si longtemps, mais soudain l'angoisse monte en vous... Et si la petite sœur marchait dessus ? Et si le chien le prenait pour un freesbee ? Et si le voisin voulait vous le voler parce que vous avez acheté le dernier ? Impossible de faire autrement, il va falloir faire une copie de sauvegarde, seul problème, vous n'avez pas de graveur de DVD : on va donc évidemment se servir du S-VCD.

Le magnifique logiciel qui va nous permettre de réaliser cela très facilement se nomme DVDx (non messieurs, ce n'est pas un film porno, calmez-vous tout de suite). Il est téléchargeable par exemple sur www.zdnet.com (le logiciel, pas le film porno).

Une fois installé, il ne reste plus qu'à lancer le programme pour commencer.



Bon, je vous l'accorde, l'interface est d'un goût assez spécial mais on va pas en faire un plat, on va plutôt commencer par le passer en Français. Je ne vous accuse pas de ne pas comprendre la moitié de la langue de Shakespeare mais bon, dans le doute, rien ne vaut notre bon vieux François, surtout que la manipulation pour l'activer est très simple : il suffit de choisir Load language file dans le menu File, ensuite on clique sur lang_francais.txt puis sur le bouton Ouvrir. Et hop tout devient plus compréhensible d'un seul coup ;-)



Cliquez maintenant sur le bouton Ouvrir DVD, après avoir inséré votre DVD dans le lecteur évidemment. Une autre fenêtre apparaît alors avec les pistes et leur longueur. Sélectionnez simplement la plus longue (la seule qui fait plus d'une heure alors que les autres atteignent difficilement les 15 minutes). Ne vous faites pas de souci, elle contient tout de même la totalité du film ;-)

La fenêtre Input Settings s'ouvre, vous pourrez alors sélectionner la langue que vous souhaitez parmi celles disponibles sur le DVD. En effet, le S-VCD ne vous permet pas de créer des disques multi langages comme les DVD. Vous pouvez aussi choisir la qualité de la bande son, globalement, Normal Quality, est amplement satisfaisant. La case volume ne sert pas à grand-chose, en effet vous pouvez le modifier par la suite avec la télécommande de votre télé, laissez donc la valeur par défaut.

Dans la case iDCT, sélectionnez l'option correspondant à votre processeur (Intel pour Pentium ou AMD pour Athlon). La case Overlap est également intéressante, si votre film doit être gravé sur deux CD, ce qui est presque sûr, ce nombre correspond au temps en secondes qui sera répété au début du 2e CD, si vous mettez 5, les 5 dernières secondes du 1er CD seront également au début du 2e CD afin que vous ne soyez pas totalement paumé après votre pause pipi. Vous pouvez éventuellement ajouter des sous-titres grâce à la partie de la fenêtre du même nom, en revanche, ne touchez pas à la case Offset.

Validez et accédez au deuxième volet de réglages en sélectionnant Paramètres de sortie dans le menu Paramètres.

Commencez alors par choisir Super Video CD (MPEG 2) en haut de la nouvelle fenêtre. Le champ Mouvement vous permet de choisir de Normal (plus rapide, moindre qualité) à Very High (assez lent, qualité supérieure). Encore une fois, ce choix dépend de vos préférences, mais personnellement je préfère attendre un peu plus pour avoir un meilleur résultat. Mais je vous laisse faire comme vous le préférez (de toute façon, j'aurai du mal à vous en empêcher ;-) Dans Zoom, choisissez l'aspect souhaité pour votre S-VCD (4/3 ou 16/9).

Le champ Nombre d'images à encoder peut être utile pour faire des tests sans obligatoirement encoder tout le film, mais généralement cliquez sur le bouton Tout afin d'encoder le film du début à la fin.

Finissez en cliquant sur le bouton Appliquer, l'encodage peut alors commencer.

Et voilà, vous pouvez maintenant ouvrir un programme de gravure tel que Nero, choisir la fonction S-VCD, faire glisser votre fichier dans le nouveau projet et graver votre CD tant convoité et encodé à la sueur de votre front.

J'espère que vous serez satisfait du résultat.

Spolix

COUPER LE SVCD EN DEUX

S'il faut couper le fichier en deux morceaux parce qu'il ne tient pas sur un seul CD, on retourne dans TMPGenc et on suit cette procédure assez simple :

- Menu File puis MPEG Tools,

- Onglet Merge and cut,

- Type : MPEG-2 Super vidéo CD.

On clique alors sur Add, on choisit son fichier puis, en double cliquant sur son nom, on rempli les cases Range 00 :00 :00 to 00 :00 :00 par le temps au bout duquel on souhaite couper le fichier, par exemple pour un film de 1h30 que l'on souhaiterai couper en deux :

- Range 00 :00 :00 to 00 :45 :00 puis OK et Run afin de créer la première partie.

- Range 00 :45 :50 to 01 :30 :00 puis OK et Run afin de créer la deuxième partie. On remarque que les dix dernières secondes de la 45e minute sont répétées toujours pour les mêmes raisons que celles décrites tout à l'heure ;-)

LES METIERS DE LA SCENE

LE RELEASER

Nous vous avons déjà fait découvrir, dans les précédents numéros, les "métiers" de siteop et de trader. Nous allons aujourd'hui nous intéresser à un autre gros acteur de la scène warez : le releaser.

Vous savez, grâce aux articles précédents, comment les fichiers pirates sont transférés d'un bout à l'autre de la planète, et qui gère ces serveurs. Mais une question reste encore sans réponse : comment tous ces jeux, programmes, films et mp3 arrivent-ils sur le Net ?

Eh bien c'est le boulot de Thunderos, un *releaser* de divx, qui a gentiment accepté de répondre à nos questions.

PIRAT'Z : Salut.

THUNDEROS : Hi.

P. : Tu peux te présenter rapidement pour nos lecteurs, s'il te plaît ? Si ça ne te dérange pas, évidemment.

THUN. : Je ne vous dirais pas mon nom, mais je suis étudiant, âgé de 20 ans. Je suis un homme et je suis dans le warez depuis maintenant environ 2 ans.

P. : Si tu devais résumer ton rôle rapidement pour quelqu'un qui ne connaît pas du tout le monde du warez, que dirais-tu ?

THUN. : En fait, je suis chargé d'uploader (ndlr : contraire de downloader, envoyer sur le Net) les nouveaux films disponibles le plus tôt possible afin qu'ils soient disponibles en téléchargement.

P. : J'ai dit dans l'intro de cet article que les releasers s'occupaient aussi des jeux et de mp3, je me suis planté ?

THUN. : Non, non, pas du tout. Tu as raison, mais je ne peux pas tout faire. Je me charge simplement des films car je n'ai de bonnes sources que pour cela, mais de très bons releasers se chargent quotidiennement des jeux et mp3.

P. : Tu parles de "sources", qu'est ce que tu entends par là ?

THUN. : D'accord, assez de bavardages, entrons dans le vif du sujet LoL. J'appelle source les endroits et les personnes par lesquels je peux obtenir des films en exclusivité.

P. : Par exemple ?

THUN. : LoL, tu ne veux pas qu'ils finissent derrière les barreaux quand même ;) Je peux juste dire que j'ai sympathisé avec le gérant du magasin de vente de DVD zone 1 (ndlr : DVD américains) près de chez moi, qui me prête les nouveautés venues tout droit des USA dès qu'il les reçoit.

P. : Mais que gagne-t-il à faire ça ? Tu le paye ?

THUN. : Non, pas du tout, je ne lui donne pas d'argent mais ça ne lui coûte rien : je ne fais qu'emprunter le DVD le temps de la release, et je lui fourni en contrepartie les dernières auxquelles j'ai accès, et qui n'arriveront dans son magasin que plusieurs semaines plus tard.

P. : Mais comment peux-tu avoir des films qui n'existent pas encore aux États-Unis en DVD ?

THUN. : J'ai également de bons contacts ayant accès à certains festivals, où ils peuvent screener des grosses news. De mon côté, il m'est arrivé de screener certains films, mais j'essaye quand même d'éviter cette pratique.

P. : Peux-tu expliquer à nos lecteurs ce que tu signifie "screener" ?

THUN. : Bien sûr, ce terme vient de l'Anglais screen, qui veut dire écran. Cela traduit l'action d'aller au cinéma avec sa caméra et de filmer l'écran. On peut ensuite créer un divx grâce à certains logiciels. Je ne suis pas un grand fan de cette méthode pour la simple et bonne raison que la qualité finale est très moyenne. Si l'on peut s'en contenter pour certains films, comme des comédies ou autres, c'est à mon avis un véritable gâchis de regarder Matrix, le Seigneur des Anneaux ou Star Wars en screener devant son PC. Parfois, il faut savoir reconnaître le grand art et payer sa place de cinéma pour en profiter ;-)

P. : En parlant de ça, que penses-tu des nouvelles mesures de sécurité dans les cinémas ?

THUN. : Hum, à la base, l'idée n'est pas mauvaise, mais je ne pense pas qu'il soit concrètement réalisable d'avoir un agent à l'entrée de chaque salle vérifiant que les spectateurs ne rentrent pas avec une caméra.

On m'a déjà demandé, quand j'allais voir de "gros titres", d'ouvrir mon sac à dos. Je n'avais pas de caméra sur moi, mais vu le bref coup d'œil jeté par le mec et la taille des caméras aujourd'hui, il n'aurait pas vu grand-chose. En plus, ces contrôles ne sont faits que dans les grandes salles des centres commerciaux, ou des grandes villes. Mais ce n'est pas dans le budget des petits cinés de quartiers. Pourtant, il ne faut pas rêver, quelqu'un qui veut poser une caméra et screener ne va pas dans une grande salle bondée de monde, mais dans une petite où il pourra être à l'écart.

P. : Tu as déjà screené un film toi-même ?

THUN. : Ça m'est arrivé il y a un moment, mais c'est assez rare. Par contre, je fournis pas mal de bandes son, c'est beaucoup plus facile à enregistrer : un magnéto dans la poche, c'est presque impossible de se faire repérer.

P. : Et la bande son, tu en fait quoi ? LoL.

THUN. : Ce n'est pas que je sois spécialement fan de bandes son, mais comme la majorité des grands films sortent d'abord aux États-Unis, il suffit de télécharger la release américaine, de supprimer le son et d'ajouter la bande française. On se retrouve alors avec une version française. J'ai fait ça pour Matrix Revolution, par exemple : je suis allé à l'avant première, la veille de la sortie, je suis rentré chez moi vers minuit et j'ai bossé avec les mecs de ma team pendant un partie de la nuit. Le lendemain, jour de la sortie officielle, le film était disponible sur nos serveurs !

P. : Ah oui, en effet c'est une vraie course ! La compétition est serrée à ce point entre les différents groupes ?

THUN. : Oui, chacun essaye d'avoir le plus d'exclusivités possibles. C'est en sortant des gros titres en premiers que ces derniers vont être diffusés sur toute la scène, et que la team va se faire connaître. Il existe des sites comme frenchforce ou dupecheck, qui enregistrent le nom des dernières releases et la team qui en est à l'origine. Ils mettent à disposition le fichier nfo fourni par la team.

P. : Le nom des releases est souvent assez complexe, pourquoi ne pas mettre simplement le titre du film ?

THUN. : À chaque fois qu'une team release un film ou toute autre production, elle doit suivre plusieurs règles pour que la release soit "topable" (c'est-à-dire qu'elle soit admise sur les topsites, de gros serveurs de stockage et de diffusion).

Le nom de la release n'échappe pas à ces règles, voici le nom sous lequel on peut trouver le film *Kill Bill*, par exemple : Kill_Bill_Volume_1.FRENCH.DVDRip.XViD-LiQUiDE

On remarque tout d'abord le titre du film, puis la langue, puis DVDRip signifiant que la release a pour origine un DVD (en opposition au screener). Ensuite Xvid : il s'agit du codec utilisé pour compresser le DVD de 8 Go en un fichier de 700 Mo, et pour finir, le nom de la team à l'origine de la release : LiQUiDE.

RAFLE EN ALLEMAGNE

Ça chauffe chez nos voisins, où la police a arrêté une quinzaine de personnes impliquées dans du piratage de film à grande échelle sur Internet. Au total, ce ne sont pas moins de 40000 CDR et DVDR qui ont été saisis, de même que 19 serveurs d'une capacité disque totale de 38 To. Apparemment, ces pirates obtenaient leurs films directement à partir de groupes pirates allemands, qui eux aussi ont dû avoir chaud aux fesses là-dessus. Voilà qui démontre, encore une fois, que le piratage ne paie pas (et surtout le piratage commercial).

DRINK, DIE OR GO TO AUSTRALIA

On n'a pas fini d'entendre parler de l'affaire du groupe Drink or Die, qui s'était fait démanteler suite à la grande opération " anti-warez " lancée par le FBI en septembre 2001. Depuis, la scène s'en est peu à peu remise, mais pour les membres du groupe, tout n'est pas encore terminé. On vous a un peu tenu au courant, au fur et à mesure, des sentences infligées aux pauvres membres américains qui ont été promptement arrêtés, jugés, envoyés en prison et sexuellement abusés dans la douche. Oui, décidément, être membre d'un groupe pirate, c'est peut être " fun ", mais ça peut rapidement dégénérer. Mieux vaut être membre du magazine Pirat'z, au moins on n'est ni arrêté, ni jugé, ni jeté en prison, même si pour le reste, on n'y peut rien parfois. Quoi qu'il en soit, la justice US n'était pas satisfaite d'avoir envoyé croupir ces quelques malheureux, car le leader du groupe leur avait échappé, vivant en Australie. Elle a essayé d'obtenir son extradition, ce que l'Australie lui a refusé, affirmant son indépendance vis-à-vis des États-Unis. Dis, papa, c'est loin l'Australie ?

P. : Tu as également parlé d'un fichier nfo, peux-tu nous en dire plus ?

THUN. : Ce fichier est très important et est fourni avec toutes les releases sans exception. Il permet de connaître toutes les infos sur le film : les dates de sortie au cinéma, en DVD et en divx, le ratio (ndlr : 4/3e, 16/9e), la qualité de la bande audio, la résolution, le nom de CD etc...

Il sert également de signature à la team. En effet, il est souvent réalisé en ASCII et dans un style bien particulier, propre à chaque team.

Voici par exemple, pour reprendre l'exemple de tout à l'heure, celui que l'on trouve sur frenchforce pour Kill Bill de LiQUiDE (voir illustration).

```
piratz@piratz7:/tmp$ more liq-kb1.nfo

  .                      .                               .               .

   .                                                                     .
    )                  _____  | .              .      |  ____            (
   /              /       ) |/   _______  ____     /   ___|_  /    )        \
  /       ___  /       / /\  ) __  (   )    )__/ \  )   \/  __(____        \
 _/\ ___ / //        /__(___)/ (    \/    /  )__)   /\ \ __\__  \ ___ /\_
/ // // //          /  /  \        __ \  /  /  \    _)  \  \\ \\ \\ \
\_// _// _//          /   \       ) \ )  /   \        )  \ \\_ \\_/
 .  \/  \/joga_______(_______)___( \/_____(_______)_______/_______//__/  \/  .
 \  \              .  :         \___)               :   .            /  /
  )  \__________(     :                             :    )_________/  (
 .  /            )  L i Q U i D E      P R E S E N T S  (             \  .
   /          __/_____:__________/\_________________:_____\__           \
  (                   .                             .                    )
   \                                                                    /
 .  )      Kill Bill: Vol. 1                              (2003)        ( .
   /                                                                     \
  \/                                                                      \/
  /\       Theatre.date : Nov. 26th, 2003     # Screenings : .            /
    \      StOre.date.. : Apr. 13th, 2004     Video....... : rule        /
     .     ReleAse date : Fev. 16th. 2003     Audio....... : 384kbps    .
           Genre....... : Thirller            Resolution.. : awesome
           Runtime..... : 115 Min             # Discs..... : 1
           Rating...... : 8.2/10

           :: infOrmations ::
           http://www.imdb.com/title/tt0266697/
           http://www.allocine.fr/film/fichefilm_gen_cfilm=28541.html
           http://www.killbill-lefilm.com

           :: nOtes ::
           we r back baby
```

INTERVIEW BY SPOLIX

P. : Ok, merci pour les précisions. Ce travail te prend-t-il beaucoup de temps dans ta vie quotidienne ?

THUN. : Ça dépend des périodes, selon que l'actualité cinématographique est plus ou moins chargée. Mais en général, je compte environ 2 heures pour faire une release, plus le temps passé au ciné s'il s'agit d'un screener. Pour un simple rip d'un DVD, il me suffit de descendre à la boutique près de chez moi, de l'emprunter et ensuite c'est très rapide. Cela ne demande donc pas énormément de temps, mais il faut vraiment être constamment au taquet, prêt à bondir sur une news, au moindre coup de fil d'un pote venant de recevoir quelque chose d'intéressant.

P. : D'accord, je te remercie beaucoup pour avoir éclairé un peu nos lecteurs sur ton boulot et sur l'origine du divx qu'ils vont aller mater ou du mp3 qu'ils vont aller écouter une fois qu'ils auront fini de lire leur mag préféré. Bon courage et continue à nous fournir des bonnes news.

THUN. : Ne vous inquiétez pas pour les news, je serais toujours là ;-) Merci à toute l'équipe de Pirat'z et d'Espionet pour leur taf, vous êtes sur la bonne voie. Continuez comme ça !

@+

DON'T DO IT !

Attention ! Déjà que télécharger des films, des mp3 ou tout autre produit protégé par un copyright et dont on n'a pas les droits, c'est illégal, vous imaginez bien que les mettre à disposition, c'est un splendide moyen de s'attirer des ennuis.
Pourtant à Pirat'z, nous ne sommes pas dupes, et nous savons que ça se fait tous les jours. C'est pourquoi nous vous en parlons sans porter de jugement. C'est à vous de décider si le piratage est juste, constructif et si les risques en valent la peine.

'Z

LA FOX INFILTRÉE

On se souvient du " supplier ", qui était la source de versions piratées de films présentés aux Oscars (numéro précédent). Cette fois, c'est à la Fox que ça se passe, avec une employée qui s'est amusée à mettre sur des ordinateurs de la compagnie certains des films produits par son employeur (genre, les derniers Matrix). Elle a été découverte suite à une enquête des responsables système sur une faille de sécurité des serveurs. Morale de l'histoire : mieux vaut être responsable système pour faire ce genre de choses.

321 STUDIOS NE LÂCHE RIEN

Si vous l'aviez oublié, 321 Studios est accusé par la MPAA (l'industrie du film américaine) de commercialiser un produit permettant de copier illégalement des DVD (DVDXCopy). Ce qui est vrai, mais 321 Studios affirme vouloir seulement permettre aux gens de faire une sauvegarde de leurs DVD. Ce à quoi la MPAA a répondu (véridique) : " si vous avez besoin d'une sauvegarde, achetez un autre DVD ". En attendant, le 20 février, la MPAA a gagné le premier round, avec l'interdiction de continuer à distribuer DVDXCopy. Du coup, 321 Studios a juste enlevé le module fautif (celui qui élimine la protection du DVD), module d'ailleurs disponible peu après sur Internet. Après avoir ainsi " obéi " au jugement, la compagnie a rameuté le monde pour protester auprès du Congrès, générant plus de 100000 messages de protestation de consommateurs désireux de " sauvegarder les DVD de leurs enfants " (haha). Le pire, c'est que ça a semble-t-il marché, le Congrès devant bientôt débattre à ce sujet. Quelle perte de temps, quand on sait qu'il existe plusieurs logiciels gratuits pour copier les DVD...

ENCODER SES FILMS

WINAMP = DANGER

Malheureusement, il semblerait que Winamp devienne bientôt aussi dangereux à utiliser qu'Outlook Express. Encore une fois, on y a découvert une faille permettant à un pirate d'exécuter du code arbitraire sur un ordinateur (donc d'en prendre le contrôle) rien qu'en jouant un morceau. Une mise à jour est bien sûr d'ores et déjà disponible, mais c'est le genre de faille très dangereuse, car très rares sont ceux qui mettent régulièrement à jour un logiciel comme Winamp. Si vous avez d'autres players à nous conseiller, écrivez-nous !

MATROSKA ET VP6

Pirat'z vous l'annonce, les DivX, c'est du passé. Il existe de nouveaux formats, bien plus performants, qui permettent de tout inclure dans un fichier : les sous-titres, les bonus des dvd, et même l'affiche du film. Et bien sûr, avec une meilleure qualité.

Débuté officiellement en Mai 2003, le projet Matroska recouvre à la fois un container audio et video. Projet d'origine européenne, il est placé sous licence GNU/GPL, c'est-à-dire libre. Le projet a pour but d'offrir une enveloppe libre permettant de contenir à la fois de la vidéo, de multiples bandes sons, des sous-titres, des chapitres, des images (jaquettes), mais aussi le menu des DVD (encore en développement!). Le MKV, comprenez "Matroska Vidéo", apparaît donc comme un concurrent direct de l'AVI ou de l'OGM.

LA LOI - Il est absolument obligatoire de posséder les originaux pour faire une copie. La copie tue la création et la violation de copyright est punie par la loi. Et vous savez, depuis le temps que la loi interdit le téléchargement et la conservation de toutes œuvres sous copyright à moins qu'on possède l'original ou l'autorisation du détenteur des droits.

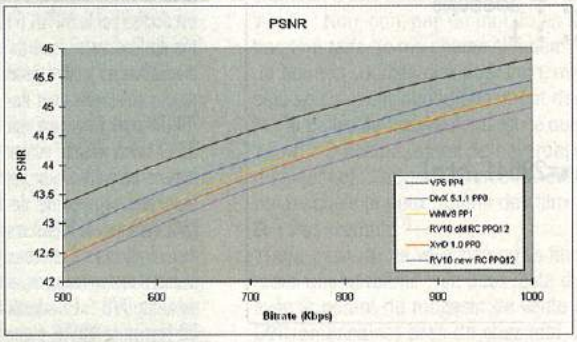
CODEC VIDÉO

Le MKV permet le choix du codec vidéo. Le mieux est encore de choisir en fonction de critères tels que le taux de compressibilité, codec libre ou propriétaire, qualité du lissage, etc. On peut ainsi comparer le VP6, le RV10, le DivX et le Xvid (voir le schéma).

Le but étant de placer un film (avec encore deux pistes son) sur 700mo, la perte de qualité liée au lissage et les faibles taux de compression des codecs Xvid et Divx nous font abandonner ce format au profit du RV10 ou du VP6.

Le choix peut paraître difficile. En effet, le rendu flou du RV10 est parfait pour une utilisation sur écran cathodique ou LCD, alors que le grain retrouvé grâce au VP6 permet une qualité d'image parfaite sur un écran de télévision. Néanmoins, les deux codecs sont égaux en qualité et le choix reste principalement une question de goût...

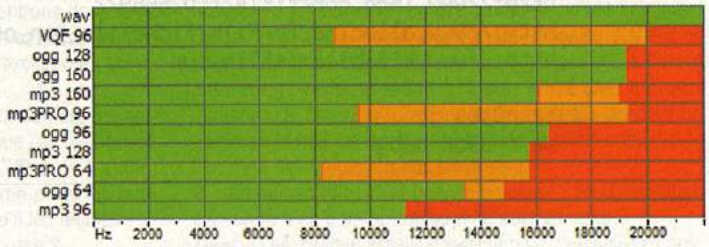
Mais la principale différence entre ces deux codecs reste la licence qui, importante pour le RV10, empêche grandement son intégration dans les platines de salon.



Comparaison des différents codecs, sur un trailer de 128 secondes. Le test PSNR indique le niveau de qualité par rapport à la source. Il s'agit d'un test mathématique dont les mesures sont exprimées en dB.

CODEC SON

De manière générale, le MKV contient deux pistes son. Le codec le plus connu est le mp3, mais c'est aussi l'un des moins bon. Nous allons donc le comparer au ogg vorbis, qui possède des taux de compressibilité plus important et est libre d'utilisation. En effet, le mp3 a tendance à détruire les fréquences de sons inaudibles à l'oreille humaine, tout comme le ogg, mais celui-ci possède plusieurs tables de compressions suivant les données à encoder. Ils se basent donc tous deux sur une compression destructive de l'information (contrairement à wav ou aiff, par exemple). Voir le tableau (en vert : respecte le format de l'original ; en oranga : ne respecte pas la forme de l'original, mais cependant un son proche la remplace ; en rouge : ne respecte pas la forme de l'original, un son très mauvais le remplace ou aucun n'est émis).



Comparaisons des codecs audios

DIVX, XVID, VP6, MKV, OGM ?

Pour ceux qui sont perdus au milieu de toutes ces normes et noms de formats, voici une petite mise au point.

Un film contient plusieurs pistes, de types différents (son et image), et différentes meta-informations (sous-titres, chapitrage, etc.). De la même manière que tout tient sur un DVD, on aimerait tout mettre sous la forme d'un fichier unique. C'est tout de même plus facile à manipuler. C'est là qu'intervient le choix d'un format, le *conteneur*. avi en est un, au même titre que Matroska ou ogm. Ou encore : mpeg, quicktime, asf, ...

Le conteneur permet de mêler plusieurs types de contenu, principalement des flux audio/video (streams). Mais ces composants peuvent aussi être codés et compressés dans des formats divers. Pour le son, on connaît bien le mp3 ou ogg vorbis, ou encore realaudio, ac3. Pour la video, on a le choix entre les différentes versions de mpeg, wmv, real video, vp6, et j'en passe.

Alors qu'est-ce que c'est qu'un DivX ? Comme xvid, c'est en fait un codage plus ou moins compatible avec certaines versions de mpeg4. Les premiers logiciels permettant de faire tenir un dvd sur un cdrom sont devenus rapidement populaires. Ils utilisaient une première version du codec divx. C'est pourquoi, par abus de langage, on désigne par le terme de divx des films compressés quel que soit le format utilisé. De la même manière, on a tendance à dire ogg, à la place de ogg vorbis, alors qu'ogg est le nom du projet de développement open source de codecs audi/video, dont vorbis.

FAÇON HI-TECH

Le test a été réalisé en compressant dans tous ces formats un fichier d'origine non compressé (format WAV), passant par toutes les fréquences de 200 Hz à 22000 Hz, soit toutes celles audibles à l'oreille humaine. Les fichiers ainsi créés sont comparés à un graphique créé avec cooledit, retraçant les fréquences émises par le fichier.

Comme vous pouvez le constater, le OGG est plus performant, quel que soit le bitrate. De plus, il permet l'encodage des sources aussi bien en stéréo qu'en surround ou 5.1. Cela permet d'encoder des concerts ou des films ne possédant qu'une bande son tout en gardant les six canaux... et une qualité au niveau de la vidéo.

Bref, l'utilisation d'ogg permet donc d'encoder avec des bitrates plus faibles pour la même qualité que le mp3, d'où un gain de place.

LES AUTRES INFORMATIONS

Les bandes son et la vidéo représentent la partie la plus importante du MKV, avec 99 % de la taille totale du fichier final. Le reste des fichiers à inclure ne dépasse pas 1 Mo.

Il existe différents formats de sous-titres, la principale différence entre eux reste la taille finale du fichier en sortie. Les fichiers IDX reprennent les images de sous-titres inclues dans les fichiers VOB, ce qui donne un fichier en sortie de plus de 5 Mo, trop gros pour l'utilisation que nous voulons en faire. Nous utilisons donc des fichiers au format SUB ou SRT. Ces fichiers sont tout simplement des fichiers texte, et la différence se situe surtout au niveau de la syntaxe.

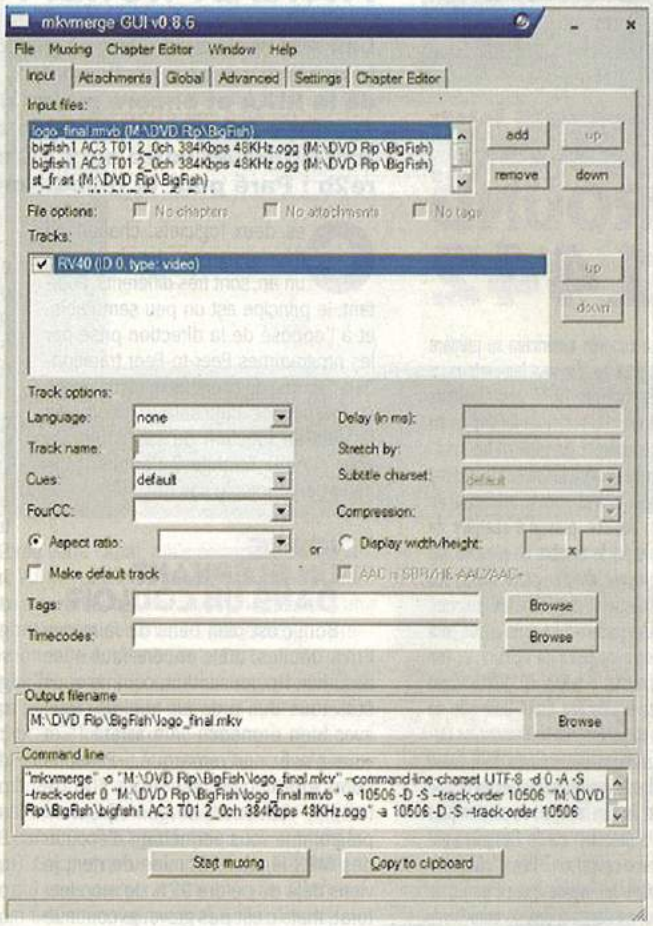
RmFactory, la GUI pour le tout en un du MKV

Pour les écrire, on se base sur un logiciel de reconnaissance des caractères (OCR), qui scanne les images de sous-titres contenues dans les fichiers VOB du DVD. Les fichiers SUB ou SRT ont une taille de sortie d'environ 100 Ko. Cela permet d'inclure au minimum deux langues, voire plus...

Une fois fini, il faut récupérer les bonus, c'est-à-dire les chapitres et la jaquette du film. Les chapitres se trouvent dans le DVD, du moins les temps ! Ils sont enregistrés dans un fichier texte et font à peine 1 Ko. Ensuite, il ne reste qu'à nommer les chapitres. Mais là, il n'y a qu'une solution, recopier les noms inscrits sur la boîte du DVD ! De la même manière, la jaquette se récupère au format JPEG sur Internet ou en scannant la boîte du DVD.

MULTIPLEXAGE

Une fois tous ces fichiers créés, il ne reste plus qu'à les muxer, c'est-à-dire les réunir dans un fichier unique, le fichier MKV. Cette opération dure en moyenne trois minutes. Une fois le fichier fini, vous pouvez le lire avec la plupart des lecteurs, à condition de posséder les bons codecs.



MKVToolnix, le logiciel de muxage

Dans les versions à venir, le matroska devrait contenir les menus des DVD, mais on ne sait toujours pas quand, ni sous quelle forme. Néanmoins, le projet est en constante évolution. Dans les mois à venir, on devrait aussi voir apparaître des platines de salon capables de lire ce conteneur, mais il est par contre peu probable que celles-ci décodent les codecs tels que le RV10, notamment à cause de sa licence.

Il est donc conseillé de relier son ordinateur à son téléviseur soit par un câble, soit par infrarouge si votre ordinateur est éloigné de votre téléviseur. En effet, ces deux solutions restent toujours moins chères qu'une platine de salon...

By Epsil & String
de team-mrt.org

Pour les **CODECS** et les **FILTRES MATROSKA**, un seul site : http://satsuki.yatoshi.free.fr/, un pack mis régulièrement à jour et qui ne créé pas de conflits.

MKVTOOLNIX se trouve à cette adresse :
http://www.bunkus.org/videotools/mkvtoolnix/

Quant à **RMFACTORY**, c'est ici :
http://www.rmfactory.fr.tc

Un grand merci à Zedude de rmfactory et Sagitaire, txtman, et la Team-MRT.

LE PEER2PEER QUI VIENT VERS VOUS

iRATE ET KONSPIRE2B

Les accrocs au P2P ont parfois la vie dure. C'est qu'il n'est pas toujours facile de trouver tout ce que l'on veut, de gérer de multiples téléchargements, de se cacher de la RIAA et encore moins de sa maman qui appelle à table. Que diriez-vous d'un système tel que tout arrive tout cuit dans votre assiette, avec un minimum d'intervention de votre part ? C'est justement ce que nous proposent iRate et konspire2b ! Paré pour la révolution dans la distribution de fichiers ?

ÉTATS-UNIS VS KAZAA, ROUND 1442

Le congrès américain se prépare à prendre d'assaut les partageurs de fichiers MP3 sur plusieurs fronts. Un projet de loi circule en ce moment qui rendrait les poursuites contre les fautifs beaucoup plus faciles pour le ministère de la Justice, puisqu'il suggère de réduire le nombre de preuves. On propose, dans ce projet de loi, des sanctions plus strictes pouvant aller jusqu'à 10 ans de prison pour les partageurs de fichiers... (on exagère à peine ici). Tout se met en branle aux États-Unis afin de poursuivre plus facilement les utilisateurs de logiciels P2P, étant donné que les industries du disque et du film mettent de plus en plus de pression sur le Congrès pour faire cesser ce " fléau ". Maintenant, on espère que ce projet de loi ne donnera pas de mauvaises idées à notre cher gouvernement français. Remarquez, de toute manière, ce ne sont pas les idées qui semblent lui manquer, mais plutôt la volonté de les mettre en application. Inutile donc de trop s'inquiéter pour l'instant de ce qui se passe chez nos amis ricains.

PIRATES POUR MASTERCARD

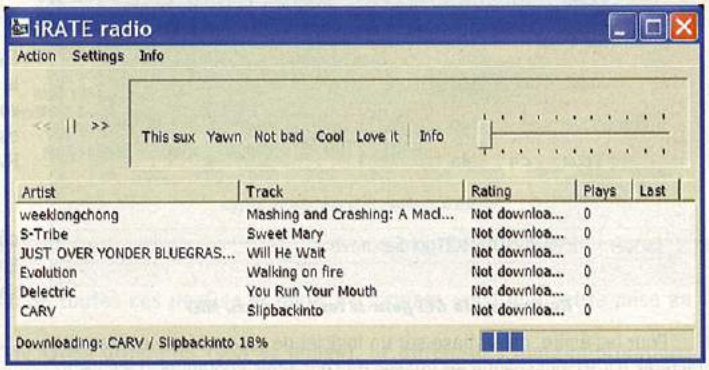
De nos jours, beaucoup de sites de commerce se font pirater pour récupérer des numéros de cartes bancaires, et en particulier de MasterCard. La société a donc engagé une équipe de hackers blancs dont le but est de trouver des failles sur ces sites pour pouvoir les " boucher " et éviter les vols de numéros. Ce projet, intitulé Site Data Protection, semble bien fonctionner car plus d'un millier de sites a déjà été " rustiné ". Le coût de cette action est encore indéterminé, mais MasterCard espère bien recevoir des aides de la part des banques.

Ces deux logiciels, chacun en développement depuis environ un an, sont très différents. Pourtant, le principe est un peu semblable, et à l'opposé de la direction prise par les programmes Peer-to-Peer traditionnels : au lieu de chercher quelque chose en particulier, l'utilisateur reçoit des fichiers en fonction de ses goûts. Ça vous semble étrange ? Commençons donc par étudier le cas de ...

iRATE, UN ÉLÉPHANT DANS UN COULOIR

Bon, c'est bien beau de faire des titres débiles, mais encore faut-il les assumer. Heureusement, comme vous êtes tous des pros en anglais, vous avez bien prononcé "Aïe arrête !" et vous n'avez rien remarqué... Passons donc aux choses sérieuses : iRate (http://irate.sourceforge.net) est un programme vous permettant d'écouter des MP3 légaux. Là, mine de rien, je viens déjà de perdre 92% de mon lectorat, mais c'est pas grave, je continue quand même. iRate se présente comme une petite radio (d'où le nom complet "iRate radio"), qui joue de la musique téléchargée sur des sites HTTP proposant des MP3 libres. Jusque-là, rien de bien extraordinaire... là où la chose devient intéressante, c'est que iRate vous permet de donner une appréciation à chaque morceau, de façon à ruiner définitivement la carrière de pauvres artistes sans le sou contraints de donner leur travail pour se faire connaître. Il y a même un autre intérêt à la chose (si si) : le programme centralise les votes de tous les utilisateurs, et en fonction des goût communs que vous avez avec d'autres internaute (et d'un savant calcul statistique), téléchargera des MP3 qui "devraient" vous plaire. C'est-y-pas beau le progrès ?

Ça vous branche ? Commencez donc déjà à installer la bestiole, car d'une part l'installation peut s'avérer un peu lourde, et le téléchargement des morceaux prend aussi parfois un certain temps. Rendez-vous dans la section "Download" du site, et téléchargez ce qu'il faut pour votre système d'exploitation (iRate est compatible Windows, Mac, Linux et Amstrad CPC). En cas de problème, lisez le guide "Getting started" dans la section "Documentation". Sous Windows, vous aurez besoin de Java installé : avec Microsoft qui a tendance à bouder de plus en plus ce langage, vous devrez peut-être l'installer vous-mêmes (allons, un peu de courage, ce n'est pas beaucoup plus difficile que de décompresser un film porno, et ça vous le faites sans rechigner, bande de petits galopins !). Avec Java en place, l'installation se fait très simplement par l'intermédiaire de Java Web Start, qui se déclenche en double-cliquant sur le fichier téléchargé. Au démarrage, vous voilà devant une fenêtre on ne peut plus laide, tandis que le téléchargement démarrera de lui-même.c



Une fois un premier MP3 téléchargé, votre nouvelle radio commencera enfin à jouer (il ne s'agit pas ici de streaming), et vous pourrez lui attribuer une note en cliquant sur l'une des appréciations au-dessus. En attendant, étudions un peu le fonctionnement de iRate. Tout d'abord, vous êtes identifié sur le réseau par un login / mot de passe, et donc loin d'être anonyme (c'est ce système de compte personnel qui permet de garder en mémoire vos préférences musicales). Mais l'auteur s'engage à ne pas donner ces informations à des tiers.

À part ça, l'algorithme proprement dit permettant de rechercher les internautes ayant les mêmes goûts que vous n'est pas très détaillé, c'est donc en l'expérimentant que vous verrez s'il vous convient ou non. Après avoir donné vos notes aux premiers MP3 de la liste de départ, vous recevrez en priorité de la musique pour laquelle le programme a "deviné" que vous allez aimer (avec de temps en temps un morceau choisi aléatoirement pour donner aux nouveaux MP3 une chance d'être notés, et vous ouvrir à de nouveaux genres).

Pour ce qui est de la provenance de ceux-ci, il s'agit donc uniquement de sites HTTP préprogrammés : le côté P2P, distribué n'est ici présent que pour la notation, pas pour la propagation des fichiers (cependant, le projet évolue vite, et c'est peut-être pour bientôt). Inutile non plus d'espérer trouver de la musique piratée, puisque tout est ici parfaitement légal. Ce qui a au moins l'avantage de laisser la RIAA en dehors de tout ça. Par les temps qui courent, c'est quand même un bon point ;)

Alors, iRate va-t-il remplacer Kazaa et Cie ? Sûrement pas pour ceux qui cherchent les dernières nouveautés musicales à la mode, mais pour quelqu'un désireux de découvrir de la musique "alternative" gratuite, c'est vraiment à essayer ! Car souvent, le problème avec ces MP3 amateurs, ou distribués sur le Web, c'est qu'il faut chercher longtemps avant de trouver quelque chose qui nous plaise : grâce au système de iRate, inutile de chercher, vos futurs coups de coeur viennent à vous !

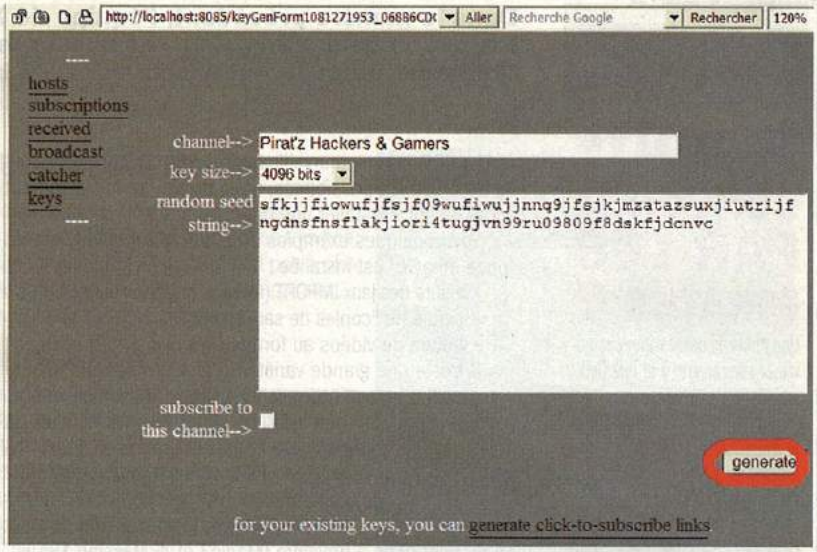
Parmi les inconvénients, outre l'interface assez basique et l'obligation d'installer Java (pour la version Windows), on notera le taux de transfert pas toujours top, la rareté des chansons en français, l'absence d'informations sur les autres utilisateurs (combien ? qui vote pour quelle chanson ?), et l'impossibilité de diffuser facilement ses propres créations (il faut passer par un site externe connu d'iRate, ou contacter l'auteur).

KONSPIRE, OH MAN !

C'est ce que je me suis exclamé en découvrant konspire2b (http://konspire.sourceforge.net) récemment (qui pourtant existe depuis presque un an). Comment un tel programme est-il passé inaperçu ? Avant de chercher des réponses à cette question existentielle, une petite mise au point sur le vocabulaire : konspire2b est le nom du protocole, tandis que le programme lui-même est plus simplement nommé kast. Comme iRate, kast est compatible avec la plupart des systèmes d'exploitation récents (sauf l'Amstrad CPC). Par contre, ses auteurs n'ont pas voulu utiliser Java, pour des raisons de simplicité et de performances. En fait, et ça fait d'ailleurs un peu bizarre au début, kast utilise une interface web : on lance un exécutable qui est juste une sorte de petit serveur web auquel on se connecte en ouvrant l'adresse http://localhost:8085 dans son browser.

Ok, j'ai dit que iRate était laid, mais à côté de kast c'est Bill Gates (ou tout autre personnage hautement sexy que vous aimez). En théorie, il est très simple de faire des skins, puisque tout est en HTML, mais les deux skins proposées par défaut sont, euh, rustiques, pour rester poli. (*ndlr : rien que pour embarasser l'auteur, nous avons subrepticement remplacé sa capture minable par une belle page d'accueil, avec une skin digne de ce nom*). Enfin, avant d'étudier un peu les fonctionnalités pas toujours intuitives de kast, mieux vaut bien expliquer son principe. L'idée est de vous permettre de distribuer des fichiers sur votre propre canal ("channel" en anglais), un peu comme si vous gériez une station de radio. Lorsque vous envoyez un fichier, tous les "auditeurs" (ceux qui sont abonnés à votre canal) le reçoivent et se le partagent entre eux. kast sert à la fois d'émetteur et de récepteur : vous pouvez émettre sur votre canal (ou vos canaux), mais bien sûr également recevoir sur les canaux que vous écoutez (ce qui est souvent l'utilisation principale d'un tel programme).

Tout se fait finalement très simplement à partir de l'interface web que vous ouvrez dans votre navigateur. En cliquant sur "subscriptions", on peut s'abonner à un canal existant. Pour cela, il faut avoir la clef de réception de ce canal : typiquement, cette clef sera téléchargée à partir d'un site web public. En cliquant sur "broadcast", vous pouvez envoyer un fichier (ou tous les fichiers d'un répertoire) sur l'un de vos canaux. Il faudra bien sûr avoir d'abord créé un tel canal, ce qui se fait dans "Create channel" ou "keys" (selon la skin choisie) : entrez un nom de canal, choisissez une taille de clef, tapez n'importe quoi dans la boîte de dialogue pour avoir une clef bien aléatoire, et voilà, un clic sur "generate" et quelques calculs plus tard, vous êtes prêt à émettre !



Ok, vous avez créé votre canal, mais comment faire pour avoir des auditeurs ? Il y a plusieurs solutions à cela. La première consiste juste à commencer à envoyer ("broadcast") un fichier : lorsqu'un broadcast commence, est émis un "prebroadcast" qui annonce le fichier à venir. Or, tous les utilisateurs de konspire2b sont susceptibles de recevoir ce prebroadcast (vous pouvez voir ceux que vous avez reçus en cliquant sur "catcher"). Si quelqu'un le remarque et pense que le fichier en question pourrait être intéressant, il va peut-être s'abonner au canal... Une autre solution consiste à faire la pub de son canal sur son site web, en donnant la clef de réception de votre canal (qui est générée au moment de la création de celui-ci). Sachez qu'une autre clef a été créée : la clef d'émission, qui vous permet d'être la seule personne à pouvoir diffuser un fichier sur votre canal. Enfin, il existe un système de recommandation : vous pouvez vous faire recommander par le propriétaire d'un autre canal, afin de faire de la pub pour le vôtre (évidemment, il faudra convaincre le propriétaire en question que vous en valez la peine).

Le système de konspire2b est particulièrement adapté à la diffusion de gros fichiers qui ne sont pas sensés être archivés (car une fois que tous les abonnés d'un canal ont reçu un fichier, celui-ci ne se propage plus, et il n'est pas possible de récupérer d'anciens fichiers). En cela, il se rapproche pas mal de BitTorrent : si vous voulez en savoir plus sur les différences entre les deux, plusieurs pages y sont consacrées sur le site officiel. Une autre question qui revient assez souvent est celle de l'anonymat : si le propriétaire du canal peut rester anonyme (il est très difficile de savoir qui est la source principale), les utilisateurs ne sont absolument pas protégés. Et il n'est pas évident qu'il soit légal de participer (même passivement) à la propagation de fichiers potentiellement illégaux, donc faites attention à ce qui circule sur les canaux auxquels vous avez souscrit.

En soi, konspire2b est donc une idée très originale et prometteuse, qui malheureusement est restée pour l'instant assez confidentielle. Espérons qu'avec cet article, nos millions de lecteurs de par l'univers (on a étendu notre diffusion jusqu'à Uranus depuis le dernier numéro) lanceront leurs propres canaux... et pourquoi pas un canal Pirat'z prochainement ? Restez branchés sur http://piratz.fr.st, il paraît qu'on va diffuser des anciens numéros !

EtVid

ÉMIGREZ AU CANADA

La justice canadienne n'est pas du côté des maisons de disques. En effet, 29 internautes étaient poursuivis par ces dernières pour avoir téléchargé gratuitement plus de mille chansons par l'entremise de logiciels d'échange de fichiers musicaux. Le juge a acquitté les accusés pour manque de preuves tangibles et parce qu'il n'est pas illégal, en théorie, de partager des fichiers via Internet. De plus, le juge a déclaré qu'il était difficile d'identifier l'adresse IP à partir des pseudonymes auxquels elle se rattache. Bien fait !

P2P RIME AVEC GLANDER

On savait qu'Internet nuisait grandement au rendement des employés. Une nouvelle étude a démontré que 36 % des 300 personnes interrogées utilisaient des logiciels de P2P au bureau, en se souciant très peu de ce qu'il adviendrait si la RIAA poursuivait l'entreprise pour laquelle ils travaillent. Internet et les spams sont des fardeaux pour les entreprises, mais le partage de fichiers l'est encore plus. En effet, 70 % des sondés ont avoué y sacrifier au moins 15 minutes par jour, une plus faible proportion d'entre eux y consacre une heure.

LIBERER LA PUIS

Dans le numéro précédent, l'équipe de Xavbox nous avait donné ses conseils sur les puces pour XBox. Que les possesseurs de PlayStation ne soient pas jaloux ! Voici tout ce qu'il faut savoir avant de bidouiller sa PS2.

La PS2 est une merveilleuse console de jeux regorgeant de nombreuses possibilités, mais pour y avoir pleinement accès, il faut y installer une puce.

Voici quelques exemples de possibilités lorsque que la "puce miracle" est installée :

- lecture des jeux IMPORT (tous les originaux de tous pays),
- lecture de "copies de sauvegarde",
- lecture de vidéos au format Divx (voir Pirat'z n°6).

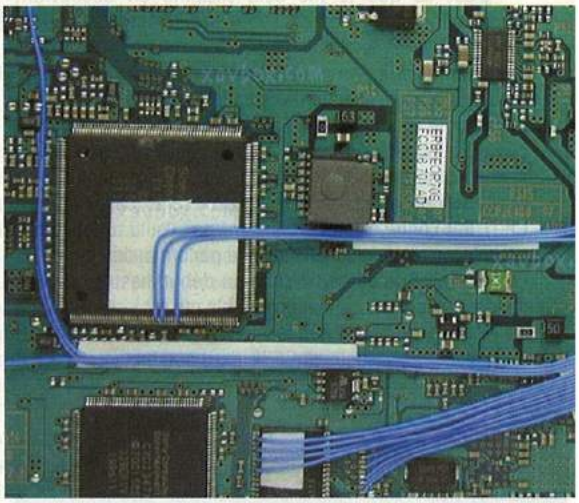
Il existe une grande variété de puces pour PS2, chacune ayant des caractéristiques techniques différentes, dont la compatibilité, les fonctionnalités apportées à la console, et notamment le voltage utilisé. Nous ne traiterons ici que des puces fonctionnant en 3.3V, qui est le seul voltage n'altérant pas la console (le bios de la PS2 étant conçu pour supporter une tension de 3.5V max). Toutes les puces fonctionnant en 5V sont donc à proscrire (Magic3 et 4, Messiah XS...).

Il existe d'autres méthodes, sans puce, pour booster sa console : le "Swap Magic" et le "Flip Top", pour une utilisation plus aisée, disponibles sur le site Internet Puces-et-Consoles.com. Même si elles ne remplacent pas une puce, ces techniques restent fiables (lire l'encadré).

Vous vous êtes enfin décidé à mettre une puce dans votre PS2 ? Si vous êtes bricoleur et plutôt doué pour la réalisation de soudures minutieuses, installez la puce vous-même. Mais si vous n'êtes pas très doué en électronique ou si vous préférez opter pour la sécurité : renseignez vous auprès d'un magasin spécialisé ou faites appel à un poseur, comme ceux inscrits dans la rubrique "Poseur de puces" de www.xavboxps2.com" (France - Belgique - Suisse - Canada).

PREMIÈRE ÉTAPE

S'ASSURER DE LA FIABILITÉ DU BLOC OPTIQUE. En effet, si la lentille du bloc optique commence à avoir des faiblesses, la pose d'une puce peut alors rendre la lecture de DVD-R impossible. Il faut procéder aux tests suivants :



- Insérer un des médias suivants dans la console puis appuyer sur " Reset " :
  - jeu Playstation sur CD (face noire),
  - jeu Playstation 2 sur CD (face bleue),
  - jeu Playstation 2 sur DVD (face blanche).

Si ces trois types de médias démarrent directement sans afficher le navigateur de la PS2, vous pouvez poser la puce. Si le navigateur apparaît, c'est signe que le bloc optique commence à avoir des faiblesses de lecture. Il est possible de le nettoyer avec de l'alcool à 90 °, mais sans rien obtenir de miraculeux : cela ne fonctionnera pas longtemps, tout comme le fait de mettre la PS2 en position verticale plutôt qu'horizontale, fera durer la lentille un tout petit peu plus longtemps. Pour savoir comment changer le bloc optique, reportez-vous à l'encadré.

SANS PUCE, AVEC LE «SWAP MAGIC»

Si vous ne voulez vraiment pas mettre de puce, il existe un système permettant de lire vos copies de sauvegarde. Mais attention, cette méthode est beaucoup moins fiable qu'une puce et vous ne pourrez peut-être pas tout lire. De plus, il faut savoir que cette méthode peut endommager le mécanisme, car il faut ouvrir le tiroir de la PS2 (en appuyant sur Eject) puis dévisser la façade du tiroir.

Pour l'utiliser, il faut démarrer avec le "Swap Magic", puis forcer sur l'ouverture du tiroir (à l'aide du "slide card" fournit avec). Ensuite on insère la copie de sauvegarde que l'on veut lire...

Pour une utilisation plus aisée, il est fortement recommandé d'utiliser le "Flip Top", vous préserverez ainsi la durée de vie du mécanisme d'éjection du tiroir.

Attention, ce système n'est pas l'équivalent d'une puce, mais évite d'avoir à faire des soudures toutes petites.

DEUXIÈME ÉTAPE

RECONNAÎTRE LA VERSION DE SA PS2 AFIN DE CHOISIR SA PUCE. Vous pourrez définir la version de votre PS2 au moyen des différentes petites caractéristiques suivantes, mais principalement en relevant le numéro SCPH situé sous la console :

PS2 v3	SCPH-30004 (+ 10 vis sous la console) Seules les V3 possèdent 10 vis, toutes les autres versions n'en disposent que de 8, les 2 vis manquantes étant remplacées par une grille d'aération
PS2 v4	SCPH-30004 (+ 8 vis sous la console) SCPH-35004 SCPH-30004R (uniquement 2 vis dans l'Extension Bay)
PS2 v5 et v6	SCPH-30004R (+ 3e vis dans l'Extension Bay) SCPH-35004R (+ 3e vis dans l'Extension Bay)
PS2 v7 et v8	SCPH-39004 On différencie la V7 de la V8 au moyen des trois derniers chiffres du numéro inscrit sur le bios ; s'il se termine par 090, il s'agit d'une V8 (version non commercialisée en France)
PS2 v9, v10 et v11	SCPH-50004

X-BOÎTE CONVOITÉE PAR LES PIRATES ?

Une nouvelle assez compréhensible et surprenante à la fois (lol) : les sondages réalisés permettent de constater qu'environ 60 % des possesseurs de la console de Billou y ont intégré une puce et un disque dur avec, par la même occasion, une plus grande capacité de stockage. Ce " PC " peut ainsi lire les jeux et DVD gravés, les divx, les mp3 ... Le prix, peu onéreux, et la facilité de la pose de la puce ont ainsi permis une hausse spectaculaire des ventes de la Xbox partout en Europe.

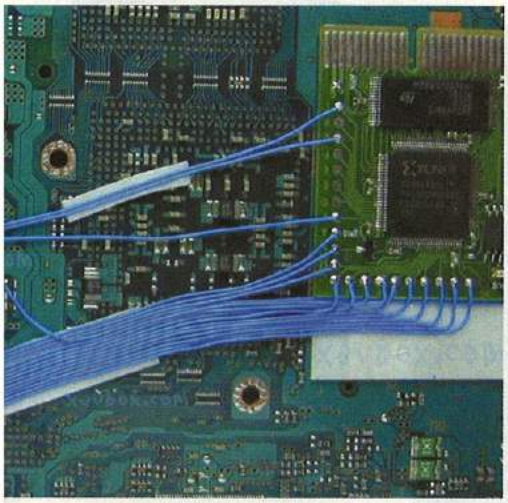
CHAÎNE SMS

Une chaîne SMS a circulé en Belgique sur le réseau du fournisseur en téléphonie mobile Proximus. Ce fournisseur avait lancé en février une promotion qui comprenait 60 SMS gratuits. Alors si vous recevez une message ou l'une de ses variantes qui ressemble à ceux-ci : " Proximus : vu le succès de la promotion des 60 SMS gratuits durant trois mois, prolonge ! Envoyez ce SMS à 5 personnes Proximus et bénéficiez de 180 SMS en plus durant 3 mois ", évitez de relancer la chaîne sinon bye-bye les 0.75euros !

STOCKAGE DE LIVRES, DVD, ETC.

Le célèbre revendeur on-line est suspecté de piraterie audiovisuelle, terme très à la mode en ce moment. Selon l'A.E.D., Alapage.com revendrait des DVD de zone 1 (alors que la France est en zone 2) ce qui n'a pas l'air de beaucoup plaire à ces messieurs des autorités. Allez les gars, soyez forts ;-)

SANCE DE SA PS2



La VRipper Gold

QUATRIÈME ÉTAPE

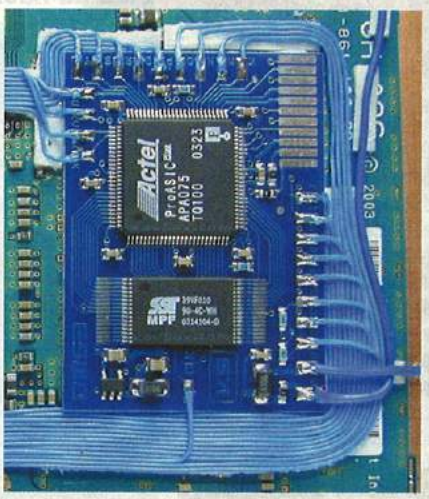
POSER LA PUCE. Préparation requise :
- un fer à souder équipé d'un panne très fine, 15W maxi, de préférence ne chauffant pas à plus de 300W afin de ne pas griller les composants,
- une bonne dose de patience...

CINQUIÈME ÉTAPE

UTILISER LA PUCE. Chaque puce ayant des modes de fonctionnement bien spécifiques (comme de devoir appuyer deux fois sur le bouton reset pour lire une copie de sauvegarde d'un jeux Playstation, etc) il demeure indispensable de se reporter au manuel de la puce en question afin de savoir comment utiliser la console "pucée".

Par Xavier et Pedro93

de xavboxps2.com
Rendez-vous sur leur site pour d'autres infos sur la PS2 !



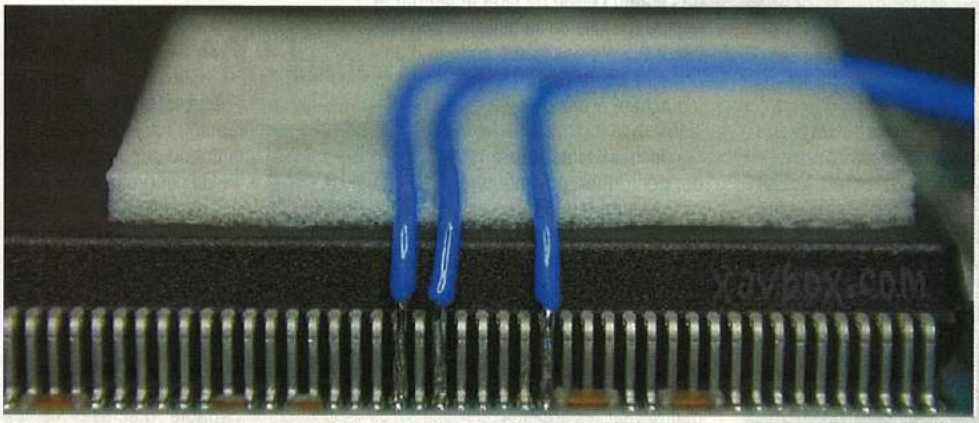
La DMS3 v9

Ce sont les dernières versions commercialisées avec le ventilateur silencieux et le port infrarouge.

TROISIÈME ÉTAPE

CHOISIR LA PUCE. Deux solutions pour choisir votre puce : soit opter pour la même que celle d'un ami satisfait de la sienne, soit la sélectionner à partir des caractéristiques techniques et modes d'utilisations qui vous séduiront le plus.

A titre d'information, voici quelques noms de puces, dont la renommée n'est plus à faire : Ripper 2 (existe en versions Lite, Deluxe, Gold), Messiah 2 pro, DMS3, MXL2, Magic V, F-14, Blue Chip, (liste non exhaustive).

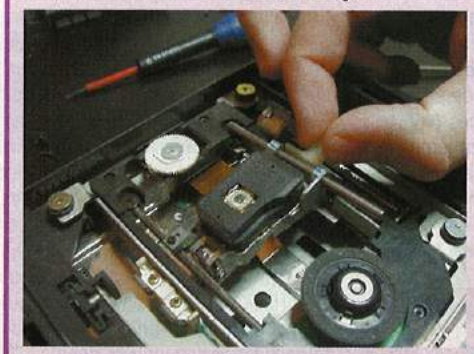


Attention à la précision des soudures

TRUCS ET ASTUCES

Lorsqu'on ne joue plus avec la PS2, il est recommandé de l'éteindre au moyen de l'interrupteur se trouvant au dos de celle-ci.
La PS2 est loin d'être un lecteur multimédia, la lecture de Divx, de MP3, de DVD et de RW restent possible, cependant elle sollicite intensément le bloc optique, ce qui l'use prématurément !
Il faut également savoir que les PS2 v9 sont plutôt fragiles, ce qui fait que très peu de poseurs de puces ne veulent garantir cette version...
Cependant, la PS2 remplit pleinement son rôle de console de jeux et reste une référence dans ce domaine !

CHANGEMENT DU BLOC OPTIQUE



Vous avez testé la lentille, et avez conclu qu'elle ne fonctionnait pas bien ? Voici comment la changer. Tout d'abord, il faut savoir qu'il existe trois types de lentilles différentes, selon le modèle de votre PS2 : un modèle vient de chez Sanyo, les deux autres de chez Sony.
Il faut commencer par démonter le capot de la console, le cache du lecteur DVD, puis faire glisser le tiroir pour avoir accès à la lentille. Elle se démontera assez facilement. Mais prudence : pour retirer la nappe, il faut écarter les deux extrémités du connecteur à l'aide d'un petit tournevis plat. Il est à noter également que pour démonter le bloc optique, il faut se munir d'un tournevis Torx n°6.
La petite vis est à conserver car elle n'est pas fournie avec la lentille neuve. Il y a également deux petits points de soudure à enlever, qui représentent la protection de lentille.
Ensuite, on remet en place le bloc optique, et on essaie. Si ce n'est pas parfait, il y a une petite molette blanche, juste à côté du bloc optique. Il suffit de la tourner un tout petit peu (mais attention, dans la majorité des cas, c'est inutile).

CONSOLES : TRICHER A LA DURE

On connaît le coup des manips à faire avec sa manette pour avoir un nombre de vies illimité ou des armes bonus. Cependant, il existe depuis longtemps des accessoires pour tricher encore plus efficacement, et d'une manière qui relève un peu plus du hacking.

À quoi ça sert de tricher ? Eh bien, tout d'abord à débloquer le joueur, sortir d'un niveau trop dur pour lui. Qui d'entre nous n'a pas connu l'envie de jeter le jeu par la fenêtre à cause de sa difficulté trop élevée ? Qui n'a pas laissé au fond d'une armoire ou revendu ce même jeu acheté à prix d'or ?

Tricher permet aussi de débloquer des niveaux supplémentaires, des personnages ou des armes nouvelles, parfois même des modes multi-joueurs et surtout de finir le jeu. Sans oublier, bien entendu, le plaisir de frimer devant les copains...

Si l'on admet que tricher est utile, on pourra tricher de deux façons différentes : premièrement, en effectuant une combinaison de touches sur la manette de votre console. Vous trouverez sur Internet des tas de sites qui vous donneront ces astuces (voir les liens plus bas), mais la deuxième méthode, la plus radicale et la plus complète, consiste à utiliser un accessoire spécialisé.

Sans faire de publicité pour un produit quelconque, il existe plusieurs gammes de produits sous des marques différentes. Les produits ACTION REPLAY de la société DATEL pour l'Europe, la gamme CODE BREAKER ou bien GAMESHARK et GAME GENIE aux USA. Tous ces accessoires se déclinent en plusieurs modèles, en fonction des consoles.

Toutes les consoles ont eu droit à leur accessoire pour tricher : Nintendo NES, SNES, Sega Megadrive (Genesis), Sega Master System, Nintendo 64, Dreamcast, Gameboy, Gameboy Advance, Gamecube, Playstation 1, Playstation 2, Xbox. En fait, les fabricants ont suivi la sortie des consoles de très près pour proposer leurs produits à la vente.

COMMENT ÇA MARCHE ?

Tout est dans la mémoire ! Lorsqu'un jeu vidéo fonctionne sur votre console, des endroits spécifiques dans la RAM sont utilisés pour stocker des informations importantes telles que le nombre de vies restant au joueur, les munitions, le niveau du jeu, les armes, etc. L'accessoire de triche est capable d'écraser ou de bloquer ces valeurs avec d'autres, ce qui permet de jouer avec un nombre de vies infinies, des munitions illimitées, etc. Reste à savoir à quel endroit de la mémoire se trouve ce que l'on cherche à gruger. C'est assez simple, il suffit de dire qu'à un certain moment, il nous reste trois vies, par exemple, puis plus tard une de moins, etc. Certains dispositifs sont ainsi capables de scanner la mémoire et de déterminer les emplacements cherchés par recoupement. On a déjà vu ce principe similaire pour PC, avec MemHack, dans Pirat'z N°1 (pour ceux qui l'ont perdu, cet article a été réédité dans notre dernier hors-série).

Le gros avantage, par rapport aux codes manettes, c'est la puissance. Les codes manettes ont été prévus par les programmeurs (pour faciliter leurs tests lors du développement), tandis que les codes triche sont infinis puisque l'on peut trouver soi-même les valeurs adéquates : en effet, les modèles les plus récents et surtout les plus évolués permettent de se connecter au PC et de lancer des recherches de codes via une connexion sur le PC !

DÉTOURNEMENT DE PRODUIT

Ce fut alors au tour des hackers de détourner le produit de son utilisation originale. Pour pouvoir lire des cd gravés sur la Playstation, les pirates avaient découvert qu'il suffisait de brancher une cartouche Action Replay à l'arrière de la console sur un connecteur disponible et de faire quelques manipulations... cela avant que soient inventées les puces...

En effet, au démarrage, l'Action Replay affiche un menu qui permet de choisir le code triche voulu. Une fois celui-ci sélectionné, il faut mettre le cd de jeu qui se lance avec les codes en mémoire. Mais l'astuce trouvée a été d'ouvrir le capot sans que la console le détecte. En fait, pour éviter la détection, on ajoutait un simple ressort !

Mais un tel succès a bien entendu fait des jaloux, et des tas de copies plus ou moins bonnes ont vu le jour... L'une d'elles porte le doux nom explicite de "psx hacker", et est livrée avec un ressort...

'Z

UN JEU D'INFILTRATION INFILTRÉ !

Project IGI2, le fameux jeu d'infiltration et de discrétion, vient d'être exploité ! Alors que le jeu vient juste d'être interdit en Chine (ouf pour eux lol), Luigi Auriemma, un pirate parmi d'autres, vient d'y découvrir une faille. L'exploit vise les commandes employées par les administrateurs gérant des parties distantes. Grâce à celui-ci, le pirate peut contrôler le PC en lui envoyant des commandes DOS. Petit conseil, ne jouez plus trop on-line à ce jeu, mais bon, rien ne vaut un bon firewall !

WITTY

L'EXTRA-TERRESTRE

Un nouveau virus a débarqué dans le monde électronique. Il se nomme Witty et s'attaque aux logiciels RealSecure et BlackIce. Ces deux softwares ont le point commun d'avoir été programmés par la société ISS. Petit bémol seulement, les clients de cette société s'attendaient à être aidés par ISS, seulement celle-ci n'a, dans 90 % des cas, même pas daigné lever le petit doigt. Motif invoqué : pas de contrat de service après vente. Seulement Witty est différent des autres virus, il possède une commande de destruction, il est donc bien plus féroce qu'ET !

HACK PAR IRC

Un lien diffusé sur IRC est directement responsable de " l'intrusion " d'un virussounet, un petit virus, baptisé à l'occasion : Tagdoor. Il utilise la faille Windows MS03-032, ce qui n'est pas une surprise. Cependant Microsoft avait déjà remarqué cette faille en mettant en ligne un patch qui visait à servir d'énième rustine. Alors si vous voyez ce lien : www.divx.dc***b.com, évitez de cliquer dessus, car il lance le téléchargement de loi.htm qui est en fait un exécutable loi.chm. On joue sur les lettres du côté des fourbes de chez Tagdoor !

LES MISES À JOUR

Notez le ressort !

Un accessoire de triche, par définition, n'est jamais à jour, puisque de nouveaux jeux sortent en permanence. Il est donc souvent complété par un site Web. Mais le plus intéressant et la grande mode, c'est de connecter l'Action Replay à votre PC par un port série, un port parallèle ou même un port USB. Dans ce cas, un logiciel livré avec le produit permet de fabriquer vos propres codes de triche.

Et chose curieuse, les pirates ont utilisé la même méthode pour craquer la PS2... avec l'Action Replay. Dans le cas de la Playstation 2, on n'utilise plus un ressort mais on force l'ouverture du tiroir du lecteur de CD/DVD avec un morceau de plastique (méthode dite du SWAP).

Sur la cartouche Action Replay pour PSX, on trouvait même un bios de remplacement (CAETLA) qui permettait de lancer des exécutables sur la première Playstation en les envoyant depuis le PC... ou bien, avec le dispositif adéquat, on pouvait faire des recopies d'écran de la console vers le PC...

Encore plus fort, les pirates ont craqué l'Action Replay et autres compatibles, entre autres sur la PS2 et sur la Dreamcast, ce qui permet d'utiliser le logiciel sans la pseudo carte mémoire livrée avec. Cette carte servait en fait de protection contre la copie.

C'est en partie pour cette raison que la plupart des fabricants n'accordent pas de licences à ce genre de produits. Ils n'ont aucun intérêt à voir leur console détournée ou piratée (quoi que...).

LES ÉMULATEURS

Enfin, le comble du succès, c'est l'incorporation des ces fonctions de triche directement dans les émulateurs, que ce soit pour SNES ou même Playstation...

CONCLUSION

Il n'y a aucune raison de ne pas acheter ce genre de produits, hormis les cartes mémoires qui sont vendues avec un CD permettant d'avoir quelques codes pour tricher. Ce genre de produits est à éviter, même si le prix est très attirant, car la compatibilité avec les logiciels de jeux existant est désastreuse, et vous n'allez pas pouvoir l'utiliser... correctement. Sinon, j'ai passé des heures, voire des journées, à trouver les vies infinies grâce à ce genre de produits. Pour un bidouilleur, c'est un bonheur total, puisque futile :-)

Par l'équipe
de metagames-fr.com

Dreamcast Utilities

DC BootCD

File	Game	Size	Author
	Action Replay CDX Dreamcast v3.0 [French/MacOS]	57 KB	-
	GameShark CDX v3.3	806 KB	E
	Boot Loader v1.2 [+ Covers] - DiscJuggler Format	2,4 MB	-
	Utopia DC BootCD v1.1 - DiscJuggler Format	1.0 MB	UTP

Liens utiles

Pour les codes accessibles à la manette, un lien vers ETAJV : Encyclopédie des Trucs et Astuces pour Jeux vidéos
http://www.jeuxvideo.com/dletajv.htm
Cette encyclopédie est disponible pour presque toutes les consoles et même pour votre PC.
Visitez aussi http://www.codejunkies.com

DERNIÈRE MINUTE

Quelques infos de dernière minute juste avant de boucler votre mag préféré. Tout d'abord, la news exclusive du numéro a disparu au profit de celle-ci. Tant pis. Sinon, le virus NetSky dont on vous parle par ailleurs semble plutôt bien fonctionner, puisque plusieurs sites visés ont déjà été mis hors service. Enfin, une bonne nouvelle du côté des croûtons du Sénat, qui ont décidé de revoir un peu la LEN, et notamment d'enlever l'obligation de surveillance du contenu des pages perso par les hébergeurs. Enfin un peu de bon sens.

UN PROCÈS BIEN DE CHEZ NOUS

Un homme de 60 ans a comparu pour avoir téléchargé et gravé des films grâce à Kazaa. L'homme a été pris en flagrant délit (il téléchargeait Taxi 3) par les gendarmes du Morbihan qui ont débarqué chez lui en décembre dernier. Ils ont trouvé près de 200 CD sur lesquels des films piratés avaient été gravés. Selon un avocat parisien, il s'agirait du premier procès de ce genre en France. Le sexagénaire serait coupable, outre d'avoir téléchargé les films, de les mettre à la disposition des autres internautes. Cet homme n'est pas le seul à devoir comparaître devant les tribunaux puisqu'ils sont au nombre de six. L'un des avocats de la défense blâme sévèrement les fournisseurs d'accès haute vitesse qui font la promotion de la rapidité de téléchargement de leurs offres. Il reconnaît tout de même que leurs clients sont fautifs, mais " qui n'a pas un seul MP3 sur son ordinateur ? ", a-t-il interrogé. Un autre avocat a pointé du doigt les logiciels de téléchargement comme Kazaa qui sont accessibles à tous. Même débat et peu de nouveauté, vous ne trouvez pas ?

COURRIER DES LECTEURS

Tenez, je vais être bref, pour une fois. Notre adresse reste le bon vieux piratgamez@yahoo.fr, sur laquelle vous pouvez poser toutes vos questions les plus débiles, et recevoir des réponses qui ne le sont pas moins. Le message du mois: ne soyez pas timide, n'hésitez pas à nous dire quels articles vous avez aimés, détestés, transformés en papier toilette... Ce n'est qu'avec votre aide qu'on pourra continuer d'améliorer le mag!

Salut, juste pour faire gagner 1 seconde aux nouveaux-nés: www.whatismyip.com marche aussi pour obtenir son adresse IP (juste pour gagner le mot address:p). Sinon j'ai un pote qui veut mettre en place un serveur qui fera entre autres proxy. Son IP sera dynamique et moi je voudrais bien pouvoir m'y connecter quand je veux. J'ai pensé à plusieurs méthodes mais toutes sont assez tordues. Si tu pouvais me dire comment tu ferais, ça serait cool. Merci pour votre super mag et bon crack.

CLEMTB

Hehe, bonne remarque pour l'adresse... Pour ton problème d'IP dynamique, il existe des logiciels prévus pour publier son IP (cherche "ip publishing tools" sur Google, tu en trouveras un paquet). Si j'avais à le faire à la main, j'aurais un hébergeur gratuit proposant du php (genre Free), et le serveur appellerait automatiquement un script php en donnant son adresse IP. Cette adresse serait alors dispo sur une autre page du site.

Salut! Je voudrais d'abord vous dire que votre mag est super bien. J'ai lu votre article sur Linux et je me demandais si on pouvait avoir, sur le même ordinateur, Linux et Windows en même temps, car j'ai un ami qui a Windows 2000 et Windows XP en même temps et il n'a aucun problème. Merci et continuez de faire votre magazine.

LEGEND KILLER

En effet il est tout à fait possible d'avoir à la fois Linux et Windows en même temps. Il est conseillé d'installer d'abord Windows, puis Linux. Si tu le fais dans l'autre sens, il est possible que Windows écrase le menu de boot de Linux (qu'il est ensuite possible de restaurer plus tard bien sûr, mais bon, autant s'éviter cette petite difficulté si on le peut).

Salut, je suis un fidèle lecteur de Pirat'z et je tenais à vous dire que je vous adore (malgré la hausse du prix). En tant que script kiddie je me pose plusieurs questions depuis quelque temps. J'ai essayé subseven2.2 ou hackatack2000 mais ces logiciels sont tous en anglais! Ne connaîtrais-tu pas une version française? De plus je trouve que le serveur de SS2.2 est très difficile à configurer. J'ai aussi essayé netbrute scanner sur le site de mon collège car je voulais changer mes notes! (ben oui sinon ma mère me supprime l'ADSL) mais cela n'a pas marché! Je me demandais si tu pourrais lui faire un petit crash disk!! Voici l'adresse du college: http://www.college-<xxxx>.org/. S.T.P. c'est une question de vie ou de mort! Au revoir Pirat'z et merci pour tout!!!!! :)

RODOLPHE

Malheureusement je ne suis jamais tombé sur un de ces logiciels en français. Une bonne raison pour travailler son anglais! Mais par contre, tu peux trouver sur internet des tutoriaux en français (il suffit de chercher sur Google), comme http://www.yacapa.com/article-62.html. Quant à hacker ton lycée, tu imagines bien qu'on ne peut pas se le permettre, c'est complètement illégal. Il est de plus peu probable que tu puisses avoir accès aux notes à partir du serveur web (ou alors, ça serait vraiment une grosse erreur de la part des administrateurs système). A+ et travaille bien à l'école!:P

Salut à vous! Merci à vous pour la fraîcheur et la pertinence de vos articles, n'hésitez pas à dire du mal des gens, surtout quand c'est mérité (ex: Billou). Ma question sera basique pour vous. J'essaye en vain de passer à Linux mais après l'installation pour le premier redémarrage j'arrive à rentrer le login mais pas le mot de passe. En fait le curseur reste figé et impossible d'écrire. Donc impossible d'utiliser Linux. Merci pour votre réponse et vive Linux et Pirat'z et puis moi aussi.

CARO

Voilà qu'on nous encourage à dire du mal des gens maintenant. Comme si on était du genre à faire ça, nous (sifflement innocent). Bon, la réponse à ton problème devrait être très simple: sous Linux, le curseur ne bouge pas lorsque tu entres ton mot de passe. Ça évite de dévoiler sa longueur à quelqu'un qui regarderait. Il faut donc juste que tu le tapes en aveugle, puis un coup sur Entrée, et ça devrait fonctionner. C'est vrai que c'est très basique, mais ça peut effectivement perturber les habitués de Windows. Sache aussi qu'un hors-série Linux est en préparation !

Où est-ce que je peux télécharger un virus pour l'envoyer à quelqu'un d'autre?

PATRICIA

Désolé, mais nous ne donnons pas directement ce genre d'adresse, qui pourrait être considérée comme illégale (même à quelqu'un signant "Patricia"). Il est déjà trop facile de trouver des virus à télécharger sur le net en cherchant un peu sur Google...

Salut Khan, alors, on s'occupe de ceux qui ne comprennent pas les articles de votre mag? Il se trouve que je fais partie de ces gens-là. Bon, en gros, je ne comprends rien à l'article sur le décryptage / cryptage du numéro 6. Pourrais-tu m'expliquer les grandes lignes de l'article autrement please?

THIBAULT

L'idée est très simple, mais si elle a échappé a un lecteur, il y en a peut-être d'autres qui voudraient de l'aide. Le codage consiste juste à décaler chaque lettre, mais au lieu de prendre un décalage fixe, on décale par la lettre qui précède. Pour la première lettre, puisqu'il n'y a évidemment pas de lettre précédente, on choisit une lettre au pif (c'est la clef), que seuls l'expéditeur et le destinataire du message doivent connaître. C'est tout.

Ci-joint une petite photo pour te remercier de m'avoir répondu! J'espère qu'elle te plaira.

RODOLPHE

Tiens, c'est bien la première fois qu'un lecteur m'envoie une image de c** pour me remercier. Je vous le dis tout de suite, autant que ce soit la dernière, la boîte aux lettres du mag' exploserait bien vite. Envoyez-moi plutôt ça sur mon email perso !

Salut, je voulais vous demander s'il y avait un moyen de lire les DivX sur PS2 sans modchip. J'ai vaguement entendu parler d'un fichier que l'on rajouterait sur les CDs pour qu'ils puissent être lus par la PS2. Merci d'avance et longue vie au mag!

UN LECTEUR

Voilà, c'est malin, j'avais préparé une belle réponse, pour finalement me rappeler au dernier moment que tout a été expliqué à ce sujet dans le numéro précédent. C'est ça la force de Pirat'z: répondre aux attentes des lecteurs avant même de les connaître!

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.com

Puces et consoles. Bon site de vente pour les puces, consoles prémodifiées et autres accessoires : www.puces-et-consoles.com

-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