

HACKADEMY #1 MAGAZINE HORS SÉRIE SURF SESSION

HORS SÉRIE

Apprendre le hacking par soi-même

Plus de 80 sites exclusifs
et outils à connaître

Tous les bons spots de hack

L 12890 - 1 H - F: 5,00 € - RD



ANONYMAT • CONFIDENTIALITÉ • RÉSEAU • ATTAQUES ET SÉCURISATION
MOTS DE PASSE • E-ZINES • ADMINISTRATION • DÉVELOPPEMENT



EDITO

Au final, il arrive parfois que Google nous montre ses limites en ne nous proposant pas véritablement ce que nous recherchions.

Ce hors série s'adresse donc à tous ceux qui aimeraient enfin trouver rapidement et simplement, le site, le document ou l'application qui pourra les débloquer sur un problème précis.

Regorgeant d'une multitude de véritables cavernes d'Ali Baba que nous vous avons dénichées, ce magazine est le résultat d'un long et interminable périple dans les entrailles du Net.

Sans pour autant être un guide complet, il pourra vous accompagner partout afin de vous aider à trouver ou à retrouver au premier coup d'œil, le site ou le programme qui correspond le mieux à vos attentes.

En effet, ces derniers sont rangés selon quatre grandes catégories : Anonymat & confidentialité, Hacking, Administration & développement et The Dark Side, divisées elles-mêmes en plusieurs sous-parties. Vous aurez ainsi la joie de découvrir que ces sites sont également rangés par ordre alphabétique et sont, pour la majorité, accompagnés d'exemples ou de captures d'écran, ce qui rend le parcours du guide plus simple et plus agréable.

Redécouvrez alors les références en la matière, puis découvrez les quelques véritables mines d'or dont peu connaissent réellement l'existence...

Sur ces dernières lignes, il ne me reste qu'à vous souhaiter, chers lecteurs, une excellente lecture.

NitryX

Greetz : RiSbo, Alias, Redils, Crak_crik, FreZz, KLoe, BeuBeu, dvrasp ainsi qu'à tout The Hackademy Team !

Sommaire

p.3
Anonymat
et confidentialité

p.14
Hacking

p.67
Administrateur
et développement

p.80
The Dark side

THE HACKADEMY MAGAZINE HORS SÉRIE

est édité par DMP,
26 bis rue Jeanne d'Arc
94160 St-Mandé
Tél.: 01 53 66 95 28

Rédacteur en chef :
NitryX

**Conception
graphique :** Weel

Illustration :
Lechatkitu

**Directeur de
Publication :**
O. Spinelli

IMPRIMÉ EN CE
Commission paritaire
en cours
ISSN en cours

© DMP 2005

Anonymat & Confidentialité



1 - Anonymat & Confidentialité

Des proxies anonymes et publics à la cryptographie, voici quelques pages de liberté pour ceux qui n'aiment pas être surveillés.

Anonymat.org

Vous pensez avoir déniché un bon proxy ?? Apparemment il a l'air rapide, mais le plus important est de tester son efficacité au niveau de son anonymat. Rendez-vous alors sur anonymat.org !

Grâce à ce site, vous pourrez en effet savoir si votre proxy est vraiment efficace. Le site vous renverra alors automatiquement toutes les informations qu'il a pu se procurer sur vous lors de votre connexion à son serveur, comme votre adresse IP, votre hôte, votre système d'exploitation et bien d'autres...

Un des points majeurs de ce site se situe également au niveau des rubriques « Annuaire » et « Outils » qui référencent une multitude de sites et d'outils concernant votre anonymat et la protection de votre vie privée sur le Web.

Anonymat.org est donc un site qu'il vous faudra garder sous la main lorsque vous voudrez tester l'efficacité de votre proxy !

LANGUE : Français

URL : <http://www.anonymat.org>

Anonymizer.com

Anonymizer.com est l'une des références en matière d'anonymat sur Internet. Étant basé sur une optique commerciale, nous ne nous intéresserons ici qu'à l'aspect gratuit du site.

En effet, anonymizer.com vous propose de surfer anonymement sur le Web.

Rappelons qu'à la base, la méthode la plus simple pour surfer anonymement est de trouver un proxy http et ensuite de configurer comme il se doit votre navigateur web.

Mais c'est ici que anonymizer.com se révèle intéressant. Il va vous permettre de surfer anonymement et cela, sans configurer la moindre adresse de proxy dans votre navigateur.

Ce qui se révèle très pratique lorsque vous n'avez pas de proxy valide sous la main.

Il vous suffit d'entrer l'adresse du site désiré dans le formulaire prévu à cet effet et votre connexion est alors relayée par les serveurs proxies d'anonymizer, ce qui revient à la même chose qu'un proxy anonyme classique.

Pour plus de simplicité, vous pourrez même accéder à ce service en utilisant cette URL :

<http://anon.free.anonymizer.com/http://www.lesitedesire.com>.

LANGUE : Anglais

URL : <http://www.anonymizer.com>

Proxy4free

On voit souvent sur des forums des personnes désespérées à la recherche de proxies valides et efficaces. Que ceux-la se réjouissent, proxy4free.com est l'une des plus grandes bases de données de proxies au monde. En effet, ce site recense quotidiennement plusieurs milliers de proxies différents, classés selon leur type (transparent, anonymous et high anonymity) et leur localisation.

Notons qu'on ne comprend pas toujours la différence entre un « anonymous proxy » et un « high anonymity proxy ». Celle-ci réside en fait au niveau des informations renvoyées aux sites visités à travers le proxy. Le simple proxy anonyme ne renvoie pas la variable HTTP_X_FORWARDED_FOR alors que l'high anonymity proxy ne renvoie ni celle-ci, ni même les variables HTTP_VIA et HTTP_PROXY_CONNECTION aux serveurs demandés par le client. Malgré les mises à jour quotidiennes, une partie de la liste des proxies ne fonctionne pas. Pour éviter de les tester un par un, aidez-vous d'un testeur de proxies comme :

<http://www.checker.freeproxy.ru/checker/>

LANGUE : Anglais

URL : <http://www.proxy4free.com>

page 7	Name	Port	Type	Country	Last Test	
page 8	168.234.181.154	3128	transparent	Guatemala	21.07.2005	Whois
page 9	80.249.73.66	80	transparent	Algeria	21.07.2005	Whois
page 10	193.126.233.58	80	anonymous	Portugal	21.07.2005	Whois
IMPORTANT TIPS	81.72.214.52	3128	transparent	Italy	21.07.2005	Whois
LINKS	203.162.220.203	80	transparent	Vietnam	21.07.2005	Whois
LINK EXCHANGE	221.10.55.202	8080	anonymous	China	21.07.2005	Whois
TOP SITES	203.162.115.35	80	transparent	Vietnam	21.07.2005	Whois
Stay Invisible	80.249.72.161	80	transparent	Algeria	21.07.2005	Whois
Public Proxy Servers	203.162.115.36	80	transparent	Vietnam	21.07.2005	Whois
Anonymity Checker	203.162.116.87	80	transparent	Vietnam	21.07.2005	Whois
Online Proxy Checker	203.162.31.28	80	transparent	Vietnam	21.07.2005	Whois
Proxz	203.162.114.173	80	transparent	Vietnam	21.07.2005	Whois
OPrivacy.com	163.21.13.5	80	anonymous	Taiwan	21.07.2005	Whois
INTERNET UTILITIES & PRIVACY TOOLS	203.162.119.117	80	transparent	Vietnam	21.07.2005	Whois
	193.194.84.198	8080	anonymous	Algeria	21.07.2005	Whois
	61.135.158.106	80	anonymous	China	21.07.2005	Whois
	200.203.60.100	3128	transparent	Brazil	21.07.2005	Whois
	212.0.138.29	80	high anonymity	Sudan	21.07.2005	Whois
	203.162.114.138	80	transparent	Vietnam	21.07.2005	Whois
	81.199.24.18	80	transparent	Uqanda	21.07.2005	Whois

Proxychains

Qui a dit que les proxies ne servaient qu'aux navigateurs web ? Le gros reproche que l'on peut faire à tous les outils d'anonymat actuels semble être leur manque de fonctionnalités et la difficulté de leur mise en place. Une solution excellente est Proxychains.

Proxychains est un programme au concept novateur qui s'utilise de façon totalement transparente. Pour ce faire, il va intercepter les appels aux fonctions utilisant les sockets (grâce au preload de librairies) et intercaler lors de vos connexions un ou plusieurs proxies de votre choix. Les types de proxies supportés sont : http (connect), socks4 et socks5.

Étant donné qu'il intercepte toutes les fonctions de type socket, aucune configuration des logiciels utilisés n'est nécessaire et ceux-ci sont tous compatibles. Ainsi, au lieu de taper :

`ssh monordi.com` vous taperez : `proxychains ssh monordi.com`

et vous serez connecté au travers d'un ou plusieurs proxies à votre destination. Le gros point fort de ce programme est que sa configuration est relativement simple, puisqu'il vous suffit d'entrer une série de proxies valides dans votre fichier de configuration et de spécifier le mode de chaînage parmi les trois suivants : Random, Strict ou Dynamic. L'authentification sur les proxies est elle aussi gérée, et il vous suffira pour cela d'informer les champs utilisateur et mot de passe lors de la réalisation de votre fichier de configuration (/etc/proxychains.conf).

Le nombre de proxies à chaîner n'est pas limité, bien que le temps de latence augmente de façon proportionnelle au nombre de proxies utilisés. Vous pourrez utiliser ce logiciel en toutes circonstances : navigateurs internet, mails, ssh, ftp, telnet, etc. L'utilisation de proxies reste à ce jour la meilleure forme d'anonymat et de protection de la vie privée sur le Web et plus généralement sur Internet. Ce programme permet leur utilisation de façon vraiment simplifiée, alors pourquoi s'en priver ?

Ce programme en est actuellement à sa version 1.8.2 et s'adresse aux OS de type Unix, à savoir Linux, BSD ou Solaris.

OS : Linux

URL : <http://proxylabs.netwu.com/proxychains>

SocksCap

SocksCap est la solution qui va vous permettre d'être anonyme, tout comme avec proxy http mais cette fois-ci sur des serveurs FTP, IRC, ICQ, MSN et bien d'autres, en passant par un proxy sock. En effet, socksCap permet de faire passer n'importe quelle application par un proxy sock. Toute la puissance de ce programme réside dans le fait qu'il permet de faire passer une application par un proxy sock même lorsque cette application ne le propose pas dans ses options.

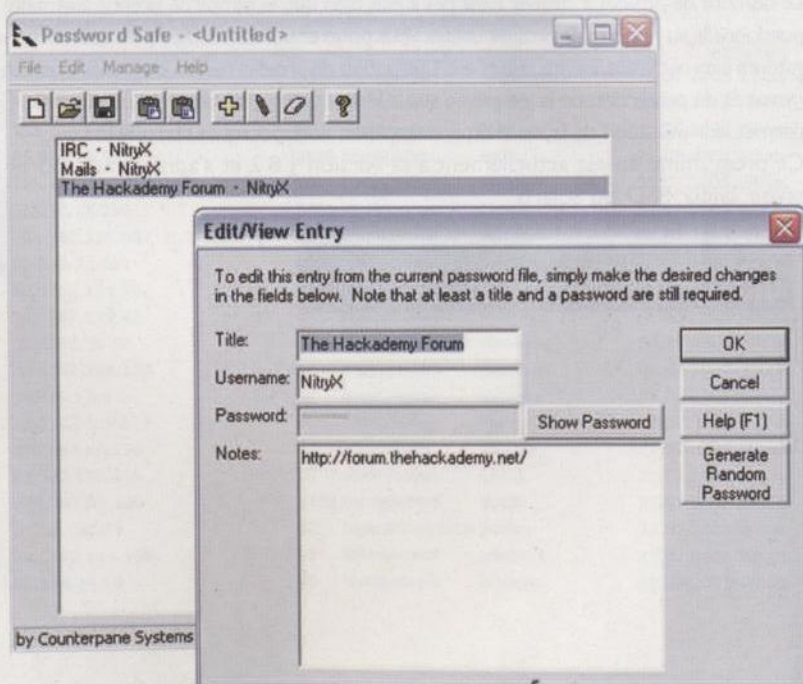
Bien entendu, tout cela se fait de manière transparente pour peu que l'application réseau soit lancée depuis SocksCap.

Dans l'exemple (cf. capture), on lance xchat (client IRC) grâce à socksCap afin de changer notre hôte et de cacher notre réelle adresse IP aux autres chatteurs. On voit également qu'il est possible de lancer votre client mail depuis socksCap, cela permet de cacher votre réelle adresse IP dans les mails que vous envoyez.

Bref, les possibilités offertes par SocksCap n'ont de limite que celle de votre imagination !

OS : Windows

URL : <http://www.socks.permeo.com>



Ars-cryptographica

Avez-vous déjà eu besoin de savoir comment fonctionne tel ou tel algorithme de crypto ? Et bien, nous voilà sur un site qui pourra répondre à la plupart de vos interrogations. À première vue, le design n'est pas la principale préoccupation du site, mais la qualité du contenu est au rendez-vous ! Tout y est. Vous pourrez comprendre, par exemple, le fonctionnement des chiffres polyalphabétiques, comme Vigenère, Trithème, Bellaso, ou bien vous lancer dans l'étude de la stéganographie. Le site est organisé comme un vrai cours. Tout est relativement bien expliqué, grâce à une présentation claire, un texte bien formulé et de nombreux schémas explicatifs. Souvent, les explications comportent une partie interactive où les algorithmes présentés sont implémentés. Pour accompagner le tout, nous n'oublions pas de souligner que des exercices pratiques vous permettront de mettre en pratique ce que vous venez d'apprendre ;)

Nous recommandons donc ce site à ceux qui voudraient en savoir plus sur les multiples aspects de la cryptographie, son histoire, ou ceux désirant comprendre en détail cet univers. C'est également une mine d'or pour les amateurs de challenges en ligne.

LANGUE : Français

URL : <http://ars-cryptographica.com>

- i. Page d'accueil
- ii. Table des matières
- iii. Comment utiliser ce cours?
- I. Introduction
 - 1. Définitions des termes courants
 - 2. Lexique de cryptologie
- II. Histoire de la cryptologie
 - 1. Chronologie des grandes figures de la cryptologie classique (avant 1950)
 - 2. Léon Battista Alberti*
 - 3. Jean Trithème
- X. Chiffres polyalphabétiques
 - 1. Tableau de Trithème*
 - 2. Chiffre de Bellaso
 - 3. Chiffre de Porta*
 - 4. Chiffre de Vigenère et variantes
 - i. Carré de Vigenère
 - ii. Règle de Saint-Cyr
 - iii. Chiffre de Vigenère*
 - iv. Décryptement du chiffre de Vigenère
 - a. Babbage/Kasiski (théorie)
 - b. Babbage/Kasiski (pratique)*
 - c. Méthode de Bazerles*
 - d. Indice de

XVII. Cryptanalyse

- 1. Principes de Kerckhoffs
- 2. Niveaux d'attaques
- 3. Techniques classiques de cryptanalyse
- 4. Comment reconnaître un chiffre?

Message clair	C	H	I	F	F	R	E	D	E	T	R
Décalage	0	1	2	3	4	5	6	7	8	9	10
Message chiffré	C	I	K	I	J	W	K	K	M	C	B

Le programme javascript ci-dessous va vous permettre de voir. Entrez un message non accenté (au besoin prétraitez le texte).

CHIFFRE DE TRITHÈME

Message clair

Message chiffré

Chiffrer / Déchiffrer / Tout effacer

Le programme javascript ci-dessous va vous permettre de voir. Entrez un message non accenté (au besoin prétraitez le texte).



Le tableau de Trithème



Les Allemands et de nombreux auteurs de l'époque 1600-1700 prétendent que c'est l'abbé Trithème qui a inventé le carré de Vigenère. Un tel tableau (voir ci-contre) se trouve bien dans *Polygraphia*, mais il l'appelle «tableau de transposition» et ne l'emploie pas de la même façon que

Vigenère. En outre, la notion de mot-clief est complètement absente de l'oeuvre de Trithème. C'est cependant bien la première fois qu'un tel tableau apparaît. Comment Trithème utilisait-il sa *tabula recta*? Il chiffrait la première lettre du message clair avec la première ligne, la deuxième lettre avec la deuxième ligne, etc. Il n'y avait pas d'alphabet clair distinct, mais la première ligne du tableau pouvait en tenir lieu. Quand il arrivait à

Bmap

Vous connaissez sûrement l'art de la stéganographie qui consiste à dissimuler un fichier dans un autre. L'intérêt de cette méthode est de permettre de faire passer des informations confidentielles à l'intérieur même d'un fichier apparemment anodin.

Pour cela, diverses méthodes sont utilisées. À commencer par la plus connue qui nécessite l'utilisation d'un éditeur hexadécimal afin par exemple d'ajouter à l'intérieur même d'une image un message secret. Ensuite, il existe une autre méthode de dissimulation d'information qui consiste à cacher les informations confidentielles à l'intérieur du slackspace. Le slackspace correspond à l'espace disque libre d'un fichier. En effet, grosso modo, le système alloue toujours un peu plus de place sur le disque dur aux fichiers qu'il ne leur en faut véritablement (dû au découpage par blocs). Cette deuxième méthode est celle utilisée par Bmap.

Illustrons maintenant l'utilisation de celui-ci par un exemple.

Ici nous allons copier la ligne correspondant au super utilisateur root depuis le fichier /etc/shadow vers le slackspace d'exemple.gif.

On regarde la taille du slackspace. Ici on va pouvoir y mettre 2ko de données !

```
nitryx:~/bmap# bmap -slackbytes exemple.gif
2006
```

Copions la ligne correspondant au root de /etc/shadow dans le slackspace de notre image :

```
nitryx:~/bmap# grep root /etc/shadow | bmap -putslack exemple.gif
stuffing block 206909
file size was: 18474
slack size: 2006
block size: 4096
```

L'opération a fonctionné !

```
nitryx:~/bmap# bmap -checkslack exemple.gif
exemple.gif has slack
```

On regarde maintenant le contenu du slackspace d'exemple.gif :

```
nitryx:~/bmap# bmap -slack exemple.gif
getting from block 206909
file size was: 18474
slack size: 2006
block size: 4096
root:$1$qEeNJPe8$gVUD.fwBNxln5pFXNhLdJ0:12877:0:99999:7:::
```

OS : Linux

URL : <http://packetstormsecurity.org/linux/security/bmap-1.0.17.tar.gz>

Burneye

Garder ses binaires secrets n'est pas chose aisée. Cependant, afin d'assurer la confidentialité d'un programme dont on ne souhaite pas dévoiler le fonctionnement, un outil formidable a été découvert par scut de la team Teso, il s'agit de burneye. En effet, burneye permet d'encrypter un exécutable au format ELF Linux sur machine Intel x86. Afin d'éviter les techniques dites de reversing, il offre plusieurs options telles que l'obfuscation qui rend le code exécutable beaucoup plus difficile à déboguer, ou encore des options telles que la mise en place d'un mot de passe afin de crypter le binaire et d'empêcher son exécution sans la connaissance de celui-ci.

La version actuelle est la 1.0.1 et à ce jour, il n'existe aucun moyen de reverser un binaire encrypté par cette méthode si l'on a oublié le mot de passe. Attention à ne pas vous brûler les yeux...

OS : Linux

URL : <http://www.packetstormsecurity.org/groups/teso/burneye-1.0.1-src.tarbz2>

```
Matrix:/tmp/burneye-1.0.1/src# ./burneye
burneye - TES0 ELF Encryption Engine
version 1.0.1
-----
usage: ./burneye [options] <program>

banner options
  -b file      display banner from 'file' before start
  -B file      display banner from 'file' on tty before start

password protect options
  -p pass      use password encryption with 'pass' as password
  -P env       first try to read password from environment 'env',
              will use password from 'env' now, too, if its there
  -i          ignore invalid entered password and execute junk
              not recommended (default: off)

fingerprinting options
  -S          SEAL mode (options F,f,t are ignored)
  -f file     use fingerprint from 'file' to protect binary
  -F         use fingerprint of current host (do not use -f and -F)
  -t num     tolerate 'num' deviations in fingerprint
  -q         be quiet about wrong fingerprint, just exit
```

Eraser

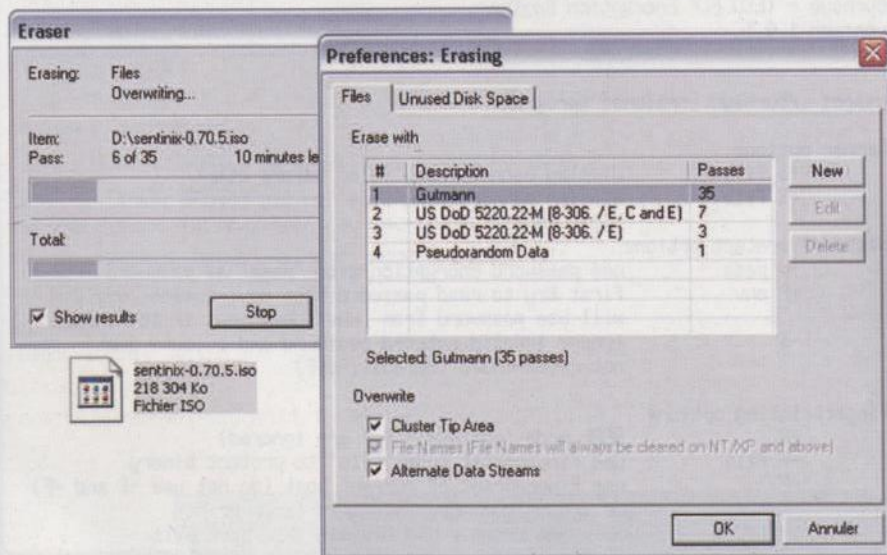
Ce programme s'est fait un nom dans le monde de la sécurité Windows. Il s'agit du meilleur outil de suppression sécurisée de fichiers. Grâce à Eraser, vous pouvez enfin supprimer efficacement vos données confidentielles. Vous savez, toutes celles que vous ne voulez absolument pas qu'un tiers puisse retrouver grâce à un logiciel tel que DiskInternals Uneraser. Pour arriver à écraser des données, un des modèles utilisé par Eraser a été élaboré à partir de l'article de Peter Gutmann ("Secure Deletion of Data from Magnetic and Solid-State Memory"). Celui-ci définit précisément comment faire disparaître toute trace magnétique d'un disque dur.

En outre, Eraser ne se contente pas d'ajouter une entrée « Erase » lors du clic droit d'un fichier. Il comporte également un gestionnaire de tâches qui pourra vous permettre de supprimer automatiquement les fichiers contenus, par exemple, dans un répertoire temporaire.

URL : <http://www.tolvanen.com/eraser/>

TAILLE : 2.7 MiB

Logiciel Libre



Password Safe

On a toujours besoin de retenir des tonnes et des tonnes de mots de passe : travail, forums, services en ligne, banques, comptes ftp, mails, etc. Password Safe permet en effet de palier à ce problème en enregistrant de manière sûre vos mots de passe dans une base de données cryptée (avec Blowfish) protégée par une phrase clé.

Un fois Password Safe lancé, on peut y ajouter toutes sortes d'entrées correspondant à des sites, des logiciels, ou pourquoi pas des informations personnelles, contenant un champ password qui sera, par la suite, masqué. Pour y accéder, il suffit de cliquer sur l'une de vos entrées pour que le mot de passe correspondant soit transféré directement dans le presse papier. Password Safe a fait l'objet de vérifications poussées afin, par exemple, de veiller à ce qu'il ne reste aucune trace d'information sensible en mémoire, après utilisation.

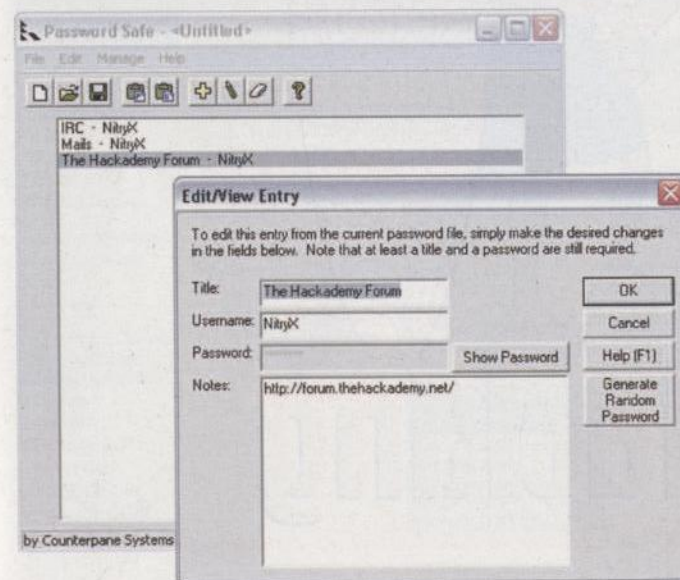
Un développeur indépendant propose une version Linux, similaire et compatible, qui n'a toutefois pas fait l'objet d'autant de vérifications : MyPasswordSafe (<http://www.semantic-gap.com/myps/>).

OS : Windows 9x/2000/XP/CE

TAILLE : 172 KiB

URL : <http://www.schneier.com/passsafe.html>

Logiciel libre





2 - Hacking

En plus des meilleurs sites pour apprendre ou se documenter sur une technique précise, une sélection d'outils toujours utiles un jour ou l'autre.

Hacking

Comment ça marche

Comment ça marche l'informatique ? Eh bien toutes les réponses sont sur ce magnifique site d'information dédié à la vulgarisation de l'informatique ! En fait, je crois qu'il s'agit du site français où l'on peut trouver le plus de documentation à ce propos. Il y a de tout : architectures, systèmes d'exploitation, histoire, lois et droit, programmation web, bases de données, langages de progs, réseaux, sécurité. Bref, y en a pour tout le monde et surtout pour les néophytes.

Les documentations sont réalisées dans des formats divers : pdf, html, doc, etc. En plus, dans la partie téléchargement, vous pouvez télécharger le site complet afin de le consulter offline (ce qui constitue une base d'informations relativement complète sur votre disque dur). Un forum est aussi à votre disposition, où vous pourrez poser vos questions. Bien évidemment, ce site est entièrement sous licence GPL ;)

LANGUE : Français

URL : <http://www.commentcamarche.net>

Dsniff

L'un des principaux problèmes que l'on rencontre quand on souhaite auditer la sécurité de son réseau en le sniffant, c'est la quantité astronomique de trafic récupéré. Il est cependant possible de remédier à ce problème en utilisant dsniff.

En effet, dsniff est un renifleur réseau de mots de passe uniquement.

Dsniff, c'est aussi une collection d'outils pour le réseau : dsniff, le filesnarf, le mailsnarf, le msgnarf, l'urlnarf et webspys permettent de surveiller passivement un réseau à la recherche de données intéressantes (mots de passe, emails, dossiers, etc.).

Mais attention, comme dit l'auteur, ce programme a été conçu afin d'auditer son propre réseau et de démontrer la faiblesse des mots de passe circulant en « clair », c'est à dire voyageant de manière non cryptée sur le réseau.

Vous l'auriez compris, la puissance de dsniff est telle que nous ne pouvons tout vous expliquer ici, le plus simple est toujours de tester par soi-même ;)

OS : Windows/Unix

URL : <http://naughty.monkey.org/~dugsong/dsniff/>

```
firewall:~# dsniff
dsniff: listening on eth0
-----
09/27/05 21:28:39 tcp 192.168.0.1.1141 -> smtp.wanadoo.fr.110 (pop)
USER nitryx
PASS 1039pJx
-----
09/27/05 21:28:44 tcp 192.168.0.1.1142 -> mail.club-internet.fr.110 (pop)
AUTH LOGIN
dHJpYm9hcmQ= [triboard]
RkZU [1039pJx]
-----
09/27/05 21:28:45 tcp 192.168.0.1.1140 -> pop.free.fr.110 (pop)
USER nitryx
PASS 1039pJx
```

ftp.zedz.net

Il n'y a pas que les simples sites qui peuvent être très intéressants sur le Net. En effet, vous avez peut-être pu constater tout au long de vos recherches que les ftp peuvent aussi être une source précieuse d'informations.

ftp.zedz.net entre parfaitement dans cette catégorie. Ce ftp regorge en outre d'une multitude de documents qui méritent le coup d'œil.

Certes, certains datent d'une dizaine d'années, mais ils restent toujours aussi instructifs et captivants.





















Vous pourriez par exemple y télécharger les dernières versions d'Open BSD ou bien des outils qui pourront vous être d'une grande aide pour effectuer de multiples tests comme le crackage de mots de passe, des tests de sécurité, l'exploration des techniques de stéganographie, le monitoring système, réseau et j'en passe...

ftp.zedz.net est donc un ftp qui mérite toute notre attention vu ses multiples aspects qui pourront nous aider à avancer dans notre quête du savoir !

LANGUE : Anglais

URL : <ftp://ftp.zedz.net>

Vers un rép. de plus haut niveau

 00-CHANGELOG.txt	3 KB 29/07/2004 13:05:00
 00-README.txt	2 KB 28/03/2005 02:27:00
 authentication	02/04/2005 02:12:00
 coast.cs.purdue.edu	30/07/2004 04:39:00
 cryptography	02/04/2005 03:40:00
 development	07/05/2005 20:00:00
 firewalls	07/05/2005 21:22:00
 host-intrusion-detection	10/05/2005 05:38:00
 host-monitoring	10/05/2005 07:47:00
 host-security	10/05/2005 07:53:00
 info	12/06/2004 00:00:00
 network-intrusion-detection	11/05/2005 02:02:00
 network-mapping	11/05/2005 04:15:00
 network-monitoring	11/05/2005 04:26:00
 network-security	11/05/2005 07:30:00
 operating-systems	02/07/2005 05:45:00
 packet-capture	03/07/2005 02:17:00
 packet-construction	03/07/2005 10:18:00
 steganography	03/07/2005 11:33:00
 vulnerability-assessment	03/07/2005 11:42:00

Google

Qui ne connaît pas le plus populaire des moteurs de recherche ? Personne, évidemment. Et pourtant, êtes-vous conscient des nombreuses possibilités offertes par ce site ? Lors d'une recherche, vous pouvez spécifier des paramètres qui parfois pourront se révéler intéressants. Par exemple, essayez de taper "allinurl: cmd.php" dans le champ de recherche ! En effet, cela vous renvoie sur un nombre impressionnant de pages possédant une adresse composée de cmd.php, qui comme beaucoup de gens le savent se résume assez souvent à un simple script php permettant l'exécution de commandes.

Donner le descriptif complet de toutes les options de Google serait futile, cependant, je vous invite à aller jeter un coup d'œil sur les diverses options de recherche avancée ou même du côté du traducteur qui peut parfois être très pratique.

Essayez aussi www.google.fr/linux pour la version tux de Google. Sans oublier le fameux Gmail qui offre un espace de stockage d'un giga : mail.google.com

URL : <http://www.google.fr>



kernel Recherche avancée
Préférences
© Rechercher sur le Web ○ Rechercher les pages en français

Web Résultats 1 - 10 sur un total d'environ 2 980 000 pour kernel. (0,23 secondes)

Conseil : Recherche pour résultats en Français uniquement. Vous pouvez indiquer votre langue de recherche dans Préférences

Le HOWTO du noyau Linux (Kernel HOWTO)

Le HOWTO du noyau Linux (Kernel HOWTO) par Brian Ward, ward@lah.tu-graz.ac.at
Version 1.0, 5 juin 1999. (5 juillet 1999. Adaptation française par Eric ...
www.freenix.fr/linux/linux-HOWTO/Kernel-HOWTO.html - 7k - [En cache](#)

Linux HeadQuarters

Catalogued patches, distributions index, links, and an archive of the linux-kernel mailing list.
www.linuxhq.com/ - 12k - 28 août 2005 - [En cache](#)

The Linux Home Page at Linux Online

The Linux kernel provides the basic services and device drivers used by all other ... Please go to LinuxHQ for Linux kernel and development information ...
www.linux.org/

The User-mode Linux Kernel Home Page

This kernel allows developers to write and debug code using the normal process-level tools, like gdb, gprof, and gcov.
user-mode-linux.sourceforge.net/ - 22k - [En cache](#)

The Linux-Kernel Archive

Governmentsecurity

Governmentsecurity.org est un site où vous trouverez de la documentation sur de multiples aspects traitant de la sécurité. Vous pourrez consulter des articles abordant la crypto, la préservation de l'anonymat avec des informations sur les remailers. Vous aurez aussi la possibilité de lire "Le Grand Guide de l'Anonymat sur Internet" ;) Sont développés par ailleurs des textes sur la sécurité linux ainsi que sur les exploits. Cette rubrique sur les exploits est enrichie de documentation sur leurs fonctionnement et quelques codes source agrémentent l'ensemble. Plusieurs pages sur la sécurité des systèmes et des réseaux pourront vous aider à mieux appréhender ces notions. Enfin un forum est mis à votre disposition pour éclaircir les articles, les approfondir, voire aborder d'autres sujets. Notons aussi qu'une section download avec quelques softs intéressants s'offre à vous !

Governmentsecurity.org est un site en Anglais (eh oui, il faut donc maîtriser la langue), mais tout de même bien réalisé avec un contenu dynamique ! Par exemple, des icônes nous indiquent quels sont les articles les plus consultés de la semaine ainsi que les derniers publiés. Governmentsecurity.org est donc un site à garder dans vos favoris !

LANGUE : Anglais

URL : <http://Governmentsecurity.org>

Information

- [E-Mail Security](#)
- [HTTP Protocol Security](#)
- [Linux Security](#)
- [MS IIS Information](#)
- [Downloads](#)
- [Exploit Archive](#)
- [Exploit Discussion](#)
- [Database Security](#)
- [\(Common-sense Principles\)](#)
- [Places that viruses and trojans hide on start up](#)
- [Step-by-Step Guide to Using the Security Configuration Tool Set](#)
- [Improving the Security of Your Site by Breaking Into it](#)
- [Domain Name Robbery](#)
- [XDC - An .EDU](#)

Article Title	Author	Submitted
Wireless Hacking IRC Log	blacksun.box.sk	04 Feb 2003
Hacking CGI - Security And Exploitation	by b0iler	12 Jan 2003
Hacking Techniques: Issue #2 - Bouncing Attacks	Written by b0iler for http://b0iler.eyeseonsecurity.com	12 Jan 2003
Hacking With Javascript	b0iler	12 Jan 2003
AdminGuideToCracking	zen	24 Jan 2003
How to become a master Hacker	Christopher Klaus	24 Jan 2003
Hacking step by step.	phantom	24 Jan 2003
hacking the bios	anand bhaskar	24 Jan 2003
BACK ORIFICE 2000		
GUIDE FOR BEGINNERS	nexzus	24 Jan 2003
Breaking Windows 98 Passwords	unknown	24 Jan 2003

Httpport

Quoi de plus énervant que d'avoir un accès à Internet mais pas la possibilité, par exemple, de discuter sur le forum de The Hackademy ? Pas de panique car nous avons la solution. HTTPort est un logiciel des plus utiles qui vous permettra de « bypasser » un proxy HTTP lorsque votre connexion à Internet est bridée, comme c'est souvent le cas dans les entreprises. Mais ce n'est pas tout, car ce logiciel de moins d'un méga vous donnera aussi la possibilité de surfer anonymement en passant par des serveurs proxies relais. À ce sujet, vous pouvez trouver ce type de service en cherchant sur Google avec les mots clés : « free public proxy server ». Mais ce n'est pas tout ! HTTPort, c'est aussi la possibilité, pour les plus expérimentés d'entre vous, de mettre en application leurs cours de tunneling. Grosso modo, cela consiste à encapsuler des paquets à l'intérieur d'autres paquets. En général, des paquets privés dans des paquets voyageant sur Internet. Un bon petit programme donc, très peu gourmand en mémoire et en ressources, qui pourrait rendre service dans de nombreuses occasions.

OS : Windows

URL : <http://www.httthost.com>



Minithins

Minithins.net est un site au design plutôt simpliste mais qui dissimule une véritable mine d'or. C'est en effet dans la rubrique Knowledge que l'on trouve la substantifique moelle du site. Cette rubrique référence près de 250 liens ayant rapport soit à la programmation, soit aux réseaux, soit à la sécurité. Le choix des liens a été fait judicieusement afin de proposer un contenu de qualité. On y trouve bien sûr de la documentation dont on aura sûrement déjà fait la lecture, mais aussi de nombreuses autres moins connues qui méritent toute notre attention.

Dans cette même rubrique nous trouverons également des liens vers d'importants sites de sécurité, de team ou de repository.

Bien que la majeure partie des liens ne soit pas spécialement dédiée aux débutants, minithins.net reste, malgré son manque de mise à jour depuis près d'un an, un très bon site.

À noter que minithins.net est en langue anglaise. Il référence cependant quelques liens vers de la documentation française.

LANGUE : Anglais

URL : www.minithins.net

Security Related Papers

- (nearly) Complete Linux Loadable Kernel Modules - pragmatic
- A Comparative Analysis of Methods of Defense against Buffer Overflow Attacks - Istvan Simon
- A Data Mining Framework for Adaptive Intrusion Detection - Columbia University
- A Distributed Autonomous-Agent Network-Intrusion Detection and Response System - Joseph Barrus
- A Guide to Understanding Covert Channel Analysis of Trusted Systems - National Computer Security Center
- A Guide to Understanding Covert Channel Analysis of Trusted Systems (aka Light Pink Book) - NCSC
- A Pattern Matching Model for Misuse Intrusion Detection - COAST/Purdue University
- API Hijack : A Library for Easy DLL Function Hooking - Wade Brainerd
- Advanced Host Detection : Techniques To Validate Host-Connectivity - dethy
- Advantage of tcp_wrappers - Dan Langille
- An Application of Pattern Matching in Intrusion Detection - COAST/Purdue University
- An Architecture for Intrusion Detection using Autonomous Agents - COAST/Purdue University
- Analysis of Bernsteins Factorization Circuit - Arjen K. Lenstra, Adi Shamir, Jim Tomlinson & Eran Tromer
- Architectural Implications of Covert Channels - Norman E. Proctor & Peter G. Neumann
- Arming FreeBSD - Markus Delves
- Attacking FreeBSD with Kernel Modules - Pragmatic
- Attacking Windows 9x with Loadable Kernel Modules - Solar Eclipse
- Attacks on Steganographic Systems - Andreas Westfeld and Andreas Pfitzmann
- Automated Detection of Vulnerabilities in Privileged Programs by Monitoring - University of California
- Autonomous Agents for Distributed Intrusion Detection in a Multi-Host Environment - Dennis Ingram
- Backdooring Binary Object - Klog
- Backdoors - Christopher Klaus
- Being Prepared for Intrusion - Dan Farmer et Wietse Venema

Ouah.org

Ouah.org recense presque tous les meilleurs textes électroniques sur la sécurité informatique. C'est une mine d'information avec près de 700 documents sur le sujet, dont une centaine sont en français. Bien sûr, ceux-ci ont été soigneusement sélectionnés et classés par catégorie et sont accompagnés d'une description en français, précisant souvent l'origine et toujours l'auteur.

Les principaux thèmes abordés vont des différents types de vulnérabilités aux techniques d'attaque, en passant par des sujets divers comme les virus, l'assembleur, les firewalls et routeurs, les lkm ou les ids.

Ouah.org est précieux pour le débutant qui cherche à se documenter sérieusement sur les aspects les plus importants de la sécurité, surtout si l'Anglais le rebute car c'est, de loin, la meilleure collection de traductions et de textes originaux en Français. Mais c'est aussi une excellente source, actuelle, d'informations pointues pour les plus chevronnés.

À noter que ouah.org possède aussi une belle collection d'outils incontournables.

LANGUE : Français, Anglais

URL : <http://ouah.org>

Textes sur le hacking - OUAH Site

"The time has come," the Walrus said, "To talk of many things.", Lewis Carroll

Textes en français (90)	Vulnérabilités (79+1)
Buffer Overflow (90+7)	Port Scanning (16)
Format Bugs (22)	Spoofing / Hijacking (32+1)
Logging (3/2)	Denial of Service (DoS) (15)
Sniffing (31)	Firewalls / Routeurs (25)
Manuels d'assembleur (2+1)	Détection d'OS (2+4)
Backdoors / Rootkits / Trojans (27)	Loadable Kernel Modules (LKM) (39)
Worms / Viruses (2+4)	Web Vulnerabilities (37+2)
Script Kiddies (1+4)	Intrusion Detection System (IDS) (1+4)
Total == 683	

[Home] [Textes sur le hacking] [Programmes] [Forum] [Listes] [Liens]

Packetstormsecurity

Packetstormsecurity.org permet à tous de faire le point sur les dernières techniques de piratage en donnant surtout les moyens de s'en protéger. Engagé de manière claire dans le respect de votre vie privée, le site ne comporte aucun cookie (hormis pour le forum) et tous les logs et statistiques concernant votre visite sont renvoyés vers /dev/null. Le contenu, quant à lui, ne devrait décevoir personne. Le site regroupe une quantité d'informations faramineuse répartie dans quatre grandes catégories.

« Assessment », qui regroupe entre autres la base de données de toutes les vulnérabilités et exploits connus ou même les outils d'audit pour Windows et Unix. Ensuite, la rubrique « défense » regroupe les outils nécessaires à la défense de votre réseau. Continuons avec la partie « papers » qui regroupe à elle seule plus de tutoriaux que n'importe quel autre site de sécurité. Et enfin, la partie « miscellaneous » qui vous réserve également de bonnes surprises. À la carte : programmation, virus, phreaking et même humour informatique.

LANGUE : Anglais

URL : <http://packetstormsecurity.org>

The screenshot shows the Packet Storm Security website interface. At the top, there are navigation links for 'Archives', 'Forums', and 'Switch Mirror'. Below that is a main menu with categories like 'about', 'forums', 'assessment', 'defense', 'advisories', 'papers', 'magazines', 'miscellaneous', and 'links'. The main content area is titled 'Section: .. / defense /' and lists several directories:

- Directory: / UNIX Defense /**
Description: A collection of defense tools and information for use with UNIX-based operating systems.
Last Modified: Apr 2 14:59:50 2004
- Directory: / Windows Defense /**
Description: A collection of defense tools and information for use with Windows operating systems.
Last Modified: Apr 2 15:00:09 2004
- Directory: / Macintosh Defense /**
Description: A collection of defense tools and information for use with Macintosh operating systems.
Last Modified: Apr 2 14:58:35 2004
- Directory: / Cryptographic Defense /**
Description: A collection of defense tools and information related to cryptography.
Last Modified: Apr 2 14:58:58 2004

On the right side of the page, there are two sidebars: 'Last 10 Files' and 'Last 10 Advisories', both listing recent document titles and sizes.

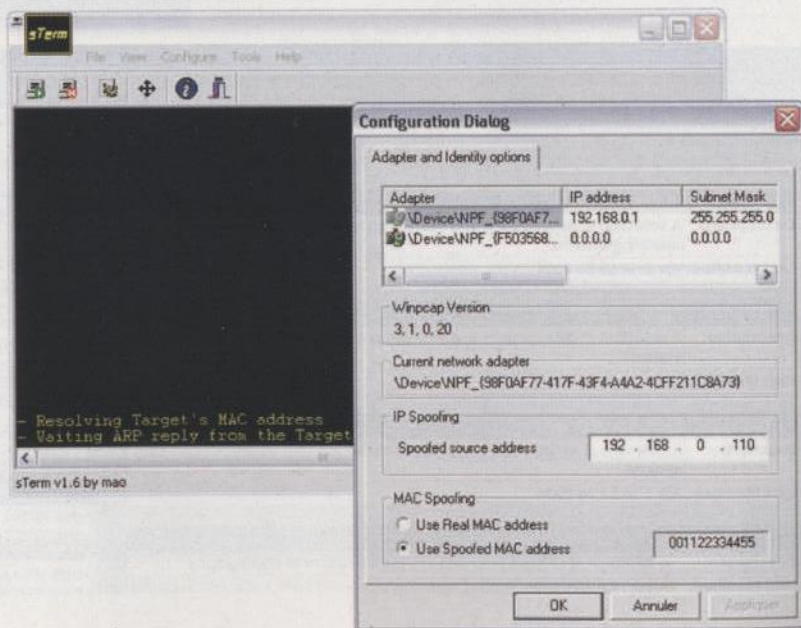
Sterm

Sterm est un outil permettant d'établir une connexion TCP en spoofant son adresse source. Ceci peut permettre de cacher son adresse IP réelle lors des tests d'intrusion et de passer outre les ACL limitant les accès à certains services TCP. Il fonctionne en faisant de l'ARP Cache Poisoning sur la passerelle et en spoofant à la fois son adresse IP et son adresse MAC afin d'être encore plus discret !

Sa configuration est des plus simples : il vous suffit de choisir l'interface réseau de la machine que vous souhaitez utiliser, puis de choisir l'adresse IP et l'adresse Mac que vous voulez simuler (ces adresses seront celles utilisées en source de vos paquets lors de votre connexion au serveur cible). Cliquez enfin sur l'icône « Connect » afin de rentrer l'adresse IP et le numéro de port sur lequel se connecter.

Mais attention, c'est un outil à utiliser avec parcimonie : après tout, si des règles de filtrage existent sur un firewall qui vous embête, pensez que c'est avant tout pour votre sécurité.

OS : Windows



<http://www.oxid.it/sterm.html>

Frenchzines

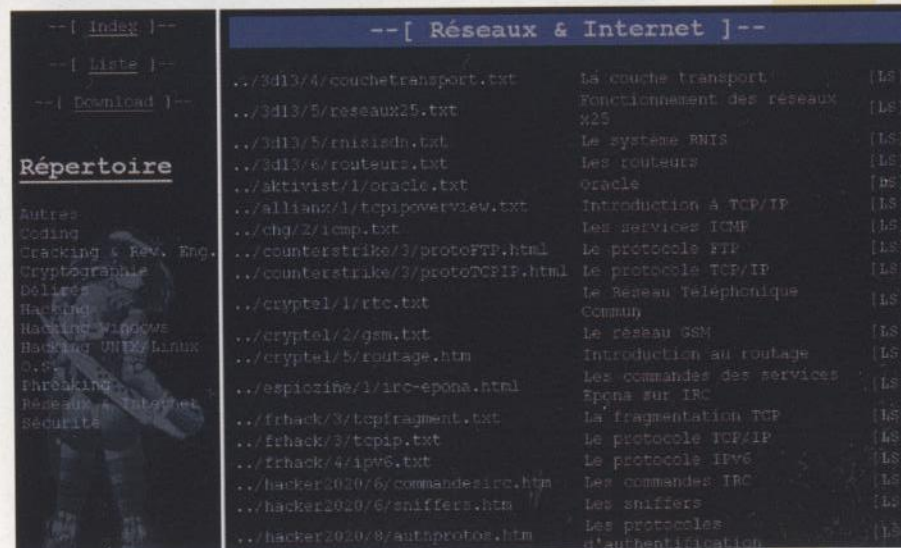
Frenchzines est un site regroupant plus de 800 e-zines francophones. Dans une atmosphère sombre mais originale, une multitude de domaines sont traités sous la forme de catégories. Il y en a pour tous les goûts. Nous citerons par exemple la programmation, la sécurité, les réseaux ou la cryptographie. Sont abordées également les techniques de backdooring, d'ARP Poisoning, de détournement de trames et bien d'autres encore.

Au-delà de son apparence, le site est doté d'une interface très pratique. En effet, les zines peuvent être classés soit par ordre alphabétique, soit par catégorie. Par ailleurs, on peut consulter d'un simple clic les multiples sujets qu'aura traité un e-zine au cours de ses différentes parutions.

Pour un plus grand confort de lecture, les textes sont au format txt ou html et sont parfois agrémentés d'images pour offrir une meilleure compréhension.

Très complet, nous qualifierons frenchzines.tk comme une des plus grandes bases de données de zines francophones. À consulter !

LANGUE : Français



L0t3k.org chzines.tk

Ô mon dieu ! Quel ne fut pas ma stupéfaction en découvrant ce site ! Un site de hackeuses qui n'ont pas froid aux yeux ! Vous avez bien lu ! L0t3k est un site (apparemment) créé par de jeunes demoiselles adeptes de l'Unix, du Backdooring et du Buffer Overflow (sans arrières pensées ;) Au programme : Linux, l'OpenSource, vie privée, programmation, sécurité, administration système, ainsi que des articles, des news, des exploits et des toolz ! Vous n'avez qu'à choisir un thème et vous obtiendrez toutes les informations relatives au sujet : articles, liens et toolz. Que rêver de mieux ? La sécurité informatique exposée dans des couleurs rose pastel, ça fait rêver... et ça change ! La seule chose qui manque à ce site est une petite série de photos des membres de L0t3k ;) Qui a dit que la sécurité était une affaire d'hommes ? Je vous déconseille de les embêter si vous ne voulez pas voir votre ordinateur partir en flammes sous vos yeux ...

URL : <http://www.l0t3k.org>

Madchat

Un site haut en couleurs et pourtant assez controversé. Les revendications « anar » et libertaires y sont peut-être pour quelque chose. La censure n'est donc pas du goût du webmaster. Pour commencer, la page d'accueil du site n'est pas statique, donc si vous réactualisez la page plusieurs fois de suite, la présentation change à chaque fois. C'est simple, mais c'est sympa et ça rend tout de suite le site plus vivant. Si l'aspect esthétique n'est pas forcément une priorité (navigation dans les rubriques en mode texte), le contenu, lui, est bien présent. Madchat, c'est l'une des meilleures sources de tutoriaux disponibles gratuitement en téléchargement. Les contributions en Français et en Anglais peuvent offrir une base non négligeable d'informations aux débutants comme aux confirmés. Parmi les rubriques les plus fournies, on trouve entre autres la sécurité admin et réseau pour les systèmes Unix/Linux. Tout ce qu'il y a à savoir sur la crypto et son utilisation. Et pour les codeurs en herbe, des infos sur la programmation sécurisée orientée réseau. De plus, si vous vous en sentez le courage et le niveau, les contributions sont bien sûr possibles. À explorer dans tous les sens.

LANGUE : Français, Anglais

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

Phrack

Qui ne connaît pas le magazine de référence Phrack, la revue des hackers écrit par la communauté et pour la communauté ? Pour les non initiés, Phrack se veut être LE magazine par excellence traitant de sécurité informatique. À l'heure actuelle, 62 phracks sont disponibles. Les articles sont chaque fois scrupuleusement sélectionnés pour vous offrir le meilleur de la documentation sur des sujets aussi divers que le hacking, le phreaking, l'espionnage, la programmation ou la cryptographie. Toutes les nouvelles techniques de hack sont présentées dans ce magazine si populaire.

Les auteurs de Phrack comptent parmi les hackers les plus connus et les plus réputés, ainsi la plupart des articles sont-ils de très haut niveau.

Pour vous y retrouver, vous pourrez rechercher une documentation particulière grâce à la recherche par auteur, titre ou commentaire. Pour résumer, Phrack vous apportera toute la documentation nécessaire pour devenir un hacker, un vrai de vrai ;)

LANGUE : Anglais

URL : <http://www.phrack.org>

Collocated Thin Server - 1657Mvds

home | about | all articles | all authors | all comments | download | search
submit article | lookback commentaries | editor in chief

Phrack 62 download (337 kb, 2004-07-13)		by anonymous author
1	Introduction (.txt)	Phrack Staff
2	loopback (.txt)	Phrack Staff
3	linuxize (.txt)	Phrack Staff
4	Phrack Profiles on road (.txt)	Phrack Staff
5	Reversing Win 9x Protection (.txt)	jamie.touler
6	Kernel Mode Backdoor for NT (.txt)	anonymous author
7	Advances in Windows Shellcode (.txt)	trapezoid
8	Remote Exec (.txt)	0x000
9	WiFi Shellcode (.txt)	0x00ff
10	Attacking Apache Modules (.txt)	and
11	Radio hacking (.txt)	shawn2k2
12	Win32 Portable Useland Proof-of-Concept (.txt)	l0g0s
13	Bypassing Windows Personal FV's (.txt)	rathe
14	A Dynamic Polyalphabetic Substitution Cipher (.txt)	vears
15	Blowing Cars for Smart Profit (.txt)	ender
16	Phrack World News (.txt)	Phrack Staff

The Hackers Choice

Porteur d'un nom qui pourrait être qualifié de déviant aux yeux de certains, thc.org (site de la team The Hackers Choice) n'en est pas moins un très bon site de hackers désireux partager au monde leurs connaissances. Pour cela, ils n'hésitent pas à utiliser les moyens les plus variés tels que les tutoriaux, les papiers ainsi que quelques outils maisons originaux, efficaces et bien-sûr sous licence GPL ! Parmi eux, nous pouvons citer AMAP ou VMAP qui ont déjà eu dans le passé, droit à quelques lignes à travers diverses publications de The Hackademy.

A ne pas oublier également que le site comporte une partie /root qui serait dommage de laisser de côté.

En parcourant cette rubrique, vous pourrez par exemple en savoir davantage sur le fameux projet Echelon de la NSA, sur la cryptographie, sur les LKM et sur bien d'autres domaines encore. Vous aurez aussi la possibilité de visiter la partie /root/phun qui contient tout les documents ... fun de la team ! ;)

LANGUE : Anglais

URL : <http://www.thc.org>



The Hacker's Choice

member since 1995

THC Papers

The members of The Hacker's Choice have published a lot of technical papers covering nearly the full palette of today's security. As a matter of fact some of the papers written in the mid and late 90s might appear a little bit dusty, but we believe you still may learn from them.

Practical SEH exploitation

Version: 1.0 Date: 2004-02-18 Language: english Size: 925b

Paper covering how to exploit the structured exception handler (SEH) on windows platforms including a step-by-step guide.

Unschärfe kryptographische Fingerabdrücke

Version: 1.0 Date: 2002-12-30 Language: german Size: 6kb

Project website: [/thc-ffp](http://thc-ffp)

Folien vom 19C3 über das Erzeugen und Nutzen von unscharfen Fingerabdrücken bei MITM-Angriffen.

Fuzzy Fingerprints

Version: 1.0 Date: 2003-09-05 Language: english Size: 42kb

Project website: [/thc-ffp](http://thc-ffp)

Introduction to the fuzzy fingerprint technique that is an extension to MITM attacks.

Top Downloaded Papers

Top 7 Downloaded Papers

- 1 Placing Backdoors Through Firewalls (35655)
- 2 Human 2 Hacker (71191)
- 3 How to cover your tracks I (56008)
- 4 Practical SEH exploitation (35316)
- 5 'Dusty' Stack Overflow Tutorial (30191)
- 6 Anonymizing Unix Systems (22381)
- 7 Hackers go corporate (20195)



Search Papers

Select Language

 Select English

Sort Order

 Sort by Date

Frsirt

Trouver de l'information à jour sur la sécurité en Français n'est pas évident. Frsirt.com (anciennement connu sous le nom de k-otik) est un site qui répond à ces critères puisqu'il est entièrement en Français et totalement dédié à la sécurité informatique. Vous aurez la possibilité de consulter sa base de données d'advisories, d'exploits ou de papers. De nombreuses news et articles sont disponibles en ligne. Ce site offre de plus, moyennant une petite participation, la possibilité de recevoir des alertes personnalisées par mail ou sms, mais aussi des exploits privés (0dayz ?!) dans le but de tester la fiabilité de votre système. Tous les exploits disponibles sont classés par date et sont mis à jour quotidiennement. Vous aurez aussi la possibilité de recevoir les advisories récents en vous inscrivant à leur mailing liste. Ce site est donc une excellente alternative à Security Focus pour se tenir informé quotidiennement des différents exploits et advisories parus, et tout ça en Français. Bref, un site à bookmarker au plus vite.

LANGUE : Français
URL : <http://www.frsirt.com>

French Security Incident Response Team

FrSIRT

Rédaction de FDS / MSDS Intelligence Economique
 32 langues, selon normes Prestations de veille et d'étude
 2001/58/CE OSHA, SIMDUT, Datops, Systèmes & Conseil

French English

Avis publics et Bulletins en vulnérabilités

- 29.07.2005 : Cisco IOS IPv6 Packet Code Execution and Denial of Service Issue
- 29.07.2005 : Linksys WRT54G Wireless Router Default SSL Certificate Issue
- 29.07.2005 : Thomson Web Skill Vantage Manager SQL Injection Vulnerability
- 29.07.2005 : Gaim libgadu Memory Alignment Denial of Service Vulnerability
- 29.07.2005 : UNG "name" and "email" Email Header Injection Vulnerability
- 29.07.2005 : PHPmyGallery "confdir" Remote File Inclusion Vulnerability
- 29.07.2005 : Simplicity of Upload "language" Remote File Inclusion Vulnerability
- 29.07.2005 : SPI Dynamics WebInspect Cross Application Scripting Vulnerability
- 28.07.2005 : Opera Multiple Cross Site Scripting and Spoofing Vulnerabilities
- 28.07.2005 : MySQL Eventum PEAR XML_RPC Remote Code Execution Vulnerability
- 28.07.2005 : FileZilla Server Zlib Library Remote Buffer Overflow Vulnerability
- 27.07.2005 : McAfee WebShield 1 User Interface Default Credential Test

Intelligence
 Télécoms
 Economie

Securityfocus

Securityfocus est, tant pour le hacker que l'administrateur, une source très précieuse d'informations. Malgré son côté un peu plus commercial depuis son rachat par Symantec (pour 75 millions de dollars), le site n'en reste pas moins intéressant. Securityfocus mets à disposition bugtraq. En effet, cette liste de diffusion à laquelle chacun d'entre nous devrait être abonné, permet de se tenir quotidiennement au courant des nouvelles vulnérabilités. L'inscription rapide est thématique. Ainsi vous pourrez vous abonner, selon vos centres d'intérêt, aux différentes listes : Linux Security News, Focus on BSD, Firewalls, Microsoft Security News, Secure Programming et j'en passe. Au total, une trentaine de sujets différents vous sont proposés, il y a donc de quoi satisfaire tout le monde ! Au-delà du côté « base de vulnérabilité et liste de diffusion », Securityfocus dispose d'un nombre intéressant d'outils. Je vous invite à aller y jeter un coup d'œil. Vous l'aurez compris, Securityfocus est une référence en la matière ! À découvrir donc, ou à redécouvrir !

LANGUE : Anglais
URL : <http://www.securityfocus.com>

SecurityFocus

Direct Marketing Services
 Databases, Lists, Broadcasting Price Match & Quality Guarantees
www.spartadata.co.uk

Network Based IDS / IPS
 IDS/IPS that can integrate with your full security solution.
www.sblsecure.com

Firewall Testing
 IDS, IPS, Firewall, SPI, VPNs, DoS Lab for Network Security devices
www.afifa.com

Home Bugtraq Vulnerabilities Mailing Lists Security Jobs Search

Vulnerabilities (Page 1 of 1)

Vendor: Apache Software Foundation
 Title: Apache
 Version: 2.0.55
 Submit

Apache HTTP Request Smuggling Vulnerability
 2005-08-16
<http://www.securityfocus.com/bid/14106>

Vulnerabilities (Page 1 of 1)

ONLINE CLASSIFIEDS

ipMonitor: Network Monitoring Software
 Securely Monitor, Alert & Recover your applications, databases, equipment, web, mail and commerce servers. Protocols include SNMP, HTTPS, FTP, SQL, SNMP TRAP, EVENT LOG, LDAP and many more. Download your free 21day trial today!

FDR SQL INJECTION XSS & MORE

The highest level of SSL encryption available, period.

Vulnerabilite.com

Voici un portail d'information très sérieux qui informe les professionnels et les passionnés depuis déjà plusieurs années. Anciennement connu sous le nom de isecurelabs.com, ce site est en perpétuelle activité. Ce qui fait que ce site nous alerte en permanence sur l'actualité de la sécurité des systèmes d'information. Des articles originaux et variés, une équipe de professionnels soudés et performants, voici la recette qui fait la réussite complète de ce site.. Vulnerabilite.com ne fait pas que livrer l'actualité, il fournit également des outils pour les professionnels tel qu'un annuaire des acteurs de la sécurité, une bible des mots de passe par défaut des constructeurs, une liste des services fonctionnant derrière chaque port d'un réseau, ou encore des solutions de sécurité pour les entreprises. Le site permet également de suivre l'actualité via un journal gratuit et téléchargeable en PDF, ainsi qu'une newsletter qui vous proposera, entre autre, toute l'information et l'actualité des derniers virus.

LANGUE : Français

URL : <http://www.vulnerabilite.com>

Le portail des professionnels de la sécurité des systèmes d'information. Inscription gratuite aux newsletters sécurité informatique.

VULNERABILITE.COM Recherche Go

Vous avez des questions ? FORUM VULNERABILITE.COM

Accueil » White Papers » Phishing

Publicité

FORUM VULNERABILITE.COM

Vous avez des questions ?

White Papers Vulnérabilités & Attaques

Deny All
rWeb : la protection totale des applications Web
Le firewall applicatif rWeb intervient en complément des dispositifs de sécurité existants afin de protéger les applications Web de l'entreprise contre les attaques non stoppées ... Publié le 27/06/2005 @ 17:22
Catégories | Firewall | Vulnérabilités & Attaques | Web Application

eEye Digital Security
How Vulnerable Is Your Network?
What assets are on your network?

Amap

Amap fait ce qu'on pourrait appeler du scanning intelligent : il se base sur les résultats de nmap (ou est capable de scanner directement les ports d'une machine) pour deviner les types d'applications qui se trouvent derrière les ports. Pour cela, il se connecte sur chacun des ports et cherche à obtenir une réponse de la part de l'application qui tourne derrière. Soit l'application lui envoie directement des informations correspondant à un protocole facilement reconnaissable (par exemple SSH ou POP3), soit il faut lui envoyer des séquences de paquets pour obtenir une réponse (par exemple pour le protocole HTTP). Grâce à cet outil, il est possible de savoir qu'un serveur FTP tourne sur le port 8765. Les administrateurs s'amuse rarement à modifier un numéro de port (surtout pour les services qu'ils ouvrent à Internet), mais il arrive que l'on souhaite identifier le service tournant derrière un port élevé... Amap fera cela très bien, très vite et très facilement ! Les protocoles supportés nécessitant un envoi sont : dns, ftp, http, jrm, ldap, ms-ds, ms-remote-desktop-protocol, ms-sql, netbios-session, ntp, oracle-tns-listener, rpc, sap-r3, smtp, snmp-public, ssl et x-windows. En ajoutant les protocoles identifiables dès la connexion, on obtient un total de 147 protocoles différents supportés !

OS : Linux

URL : <http://www.thc.org/releases.php>

```

Eterm  Font Background Terminal
$ nmap -oS -f -oH results.nmap -P0 very.bad.guy.net

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-09-07 04:26 [EST]
Interesting ports on very.bad.guy.net (10.01.10.01):
(The 1183 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open      ssh
25/tcp    open      smtp
135/tcp   filtered  loc-srv
987/tcp   open      submission

Nmap run completed -- 1 IP address (1 host up) scanned in 13.243 seconds
$ ./amap -i results.nmap -o results.amap
amap v4.2 (www.thc.org) started at 2003-09-07 04:27:08 - APPLICATION MAP mode

Protocol on 10.01.10.01:22/tcp matches ssh
Protocol on 10.01.10.01:22/tcp matches ssh-openssh
Protocol on 10.01.10.01:25/tcp matches smtp
Protocol on 10.01.10.01:987/tcp matches smtp

Unidentified ports: none.

amap v4.2 finished at 2003-09-07 04:27:16
$
  
```

Engage Packet Builder

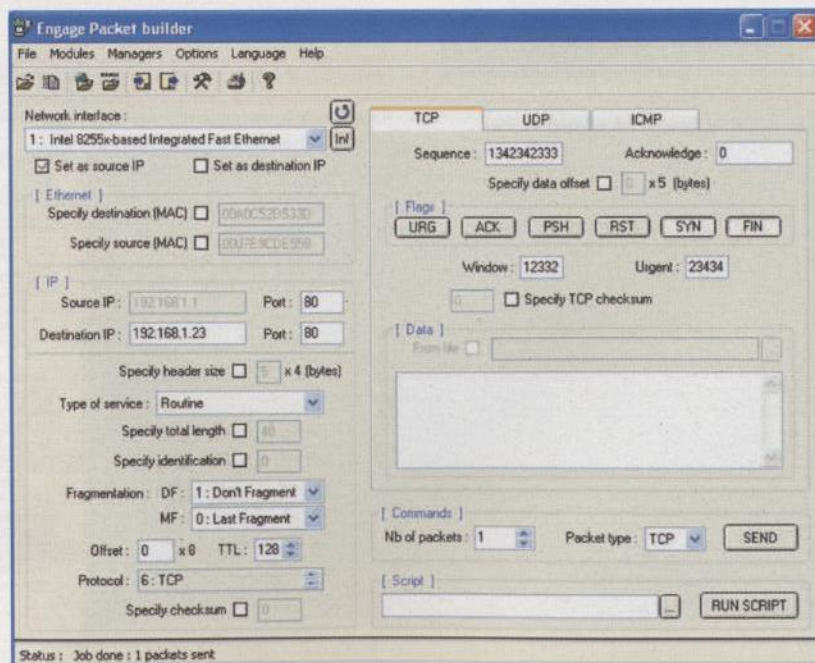
Engage Packet Builder (EPB) est un programme Windows permettant de forger les trames IP de son choix. Mais ce n'est pas tout. Là où Engage Packet Builder se distingue des packet makers traditionnels, c'est dans sa capacité à gérer des scripts. EPB gère les trois protocoles de base (ICMP, UDP et bien sûr TCP). L'interface graphique est des plus conviviales, vous aurez même la possibilité de l'avoir en Français.

Reparlons un peu de sa gestion des scripts. EBP permet en effet la création de scripts personnalisés très puissants (scripts de connexions, de syn floods, etc.). Jetez un œil aux exemples de scripts fournis avec le programme, ils détaillent toutes les commandes utilisables dans les scripts. Un programme d'installation est fourni (microsoft powered), mais vous aurez besoin de la winpcap (<http://winpcap.polito.it/>). Il y a peu de forgeurs de packets sous Windows, mais pour celui-ci, ils ont fait les choses correctement.

À essayer de toute urgence !

OS : Windows

URL : <http://www.engagesecurity.com>



Fport

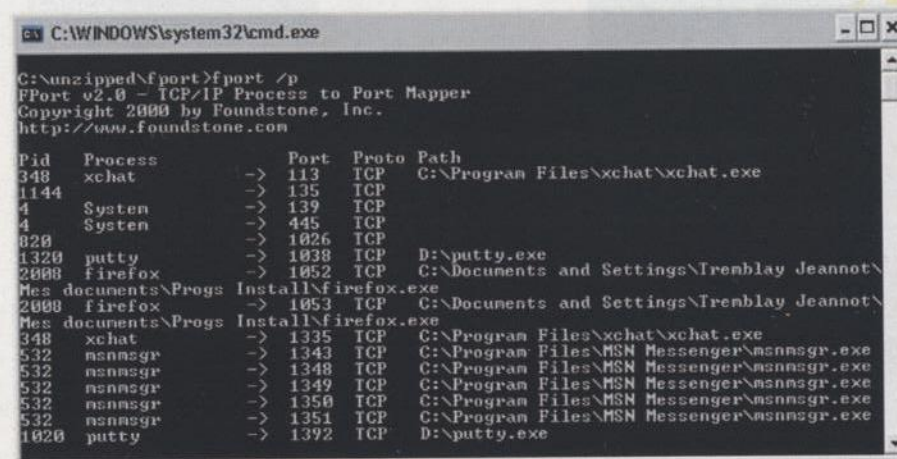
Fport est une sorte de netstat amélioré, capable de donner la liste de tous les ports ouverts sur votre machine et d'afficher le processus ou l'application qui est responsable de chacun d'eux. Cet outil est particulièrement utile pour identifier le programme responsable de l'ouverture d'un port que l'on aurait découvert en faisant scanner sa machine. On peut ainsi débusquer un trojan ou un spyware caché sur votre système.

En connaissant son nom et le chemin complet de l'exécutable, il est plus facile de le repérer dans la base de registres, par exemple. On peut également déterminer facilement quels sont les services qui sont réellement activés.

Utile pour les habitués de Linux à qui la commande netstat -atp fait cruellement défaut sur Windows.

OS : Windows NT4, 2k, XP

URL : <http://www.foundstone.com/knowledge/proddesc/fport.html>



Frameip.com

Frameip est un site dédié à la compréhension dans ses moindres détails des protocoles de communication des réseaux. Au menu, TCP/IP, UDP, ARP, ICMP, IGMP et j'en passe...

Frameip est une véritable mine d'or en la matière ! En effet, le tas d'informations présent sur ce site est très impressionnant !

Cela va de l'étude détaillée (agrémentée de schémas) du modèle OSI à l'étude du fonctionnement des VPN, tout en passant par l'étude de l'entête ARP ou par l'explication du VoIP.

De plus, le site propose une rubrique spécialement dédiée à la sécurité des réseaux TCP/IP en nous expliquant certaines attaques ou bien quelques méthodes de protection.

Ajoutons qu'il ne faut pas négliger que le site nous explique également tout l'essentiel de la programmation des sockets en C ou C++.

Nous terminerons sur l'aspect interactif de Frameip qui propose, en autres, un QCM afin de tester les connaissances que vous aurez acquises tout au long de votre visite sur le site :

LANGUE : Français
URL : <http://www.frameip.com>

<p>Général</p> <ul style="list-style-type: none"> Accueil Recherche Les News Participation Les partenaires <p>Les modèles</p> <ul style="list-style-type: none"> Toplo Osi Osi-Toplo X-200 Les Rfc <p>Les entêtes</p> <ul style="list-style-type: none"> Entête Arp Entête Ip Entête Icmp Entête Icmp Entête Tcp Entête Udp <p>Le fonctionnement</p> <ul style="list-style-type: none"> Nat Routing Sous-réseaux <p>Les services</p> <ul style="list-style-type: none"> Dhcp Dns Tcp Vpn 	<p>Entête IP par _SebF</p> <ul style="list-style-type: none"> 1 - Définition du protocole 2 - Structure de l'entête 3 - Définition des différents champs <ul style="list-style-type: none"> 3.1 - Vers 3.2 - IHL 3.3 - Service <ul style="list-style-type: none"> 3.3.1 - Priorité 3.3.2 - Délai 3.3.3 - Débit 3.3.4 - Fiabilité 3.3.5 - Coût 3.3.6 - MBZ 3.4 - Longueur totale 3.5 - Identification 3.6 - Flags <ul style="list-style-type: none"> 3.6.1 - Reserved 3.6.2 - DF 3.6.3 - MF 3.7 - Position fragment 3.8 - TTL 3.9 - Protocole 3.10 - Checksum 3.11 - Adresse IP source 3.12 - Adresse IP destination 3.13 - Options <ul style="list-style-type: none"> 3.13.1 - Copie 3.13.2 - Classe 3.13.3 - Numéro 3.14 - Bourrage 	<p>Votre IP</p> <p>193.250.32.205:2031</p> <p>Interactif</p> <ul style="list-style-type: none"> Forums Qcm Sondages <p>Groupes Nntp</p> <ul style="list-style-type: none"> fr.comp.reseaux.ip comp.protocols.top-lo linux.debian.maint.ipv6 windows.networking.toplo fr.reseaux.telecoms.pabx fr.telecoms.techniques <p>Les sockets</p> <ul style="list-style-type: none"> Winsock C - connecté C - non connecté Vb - Tcp et Udp <p>Les outils en ligne</p> <ul style="list-style-type: none"> Liste des Ports Top Udp LookingGlass Calcul des Masques Scan Tcp Whois IP <p>Les outils exe</p> <ul style="list-style-type: none"> CiscoDos.exe FrameIP.exe PingIcmp.exe
--	---	--

Guill.net

Guill.net est un site regroupant en nombre considérable des documentations intéressantes sur les réseaux. Vous pourrez y découvrir de nombreux articles relatifs aux différents protocoles connus (TCP, UDP...). Ce site dispose en plus de cela d'une grosse partie liée à la sécurité informatique des réseaux; on vous donnera des explications sur les principaux types d'attaques réseaux ainsi que sur le moyen de sécuriser votre propre réseau.

Guill.net comporte également une petite partie consacrée à l'initiation à certains langages de programmation. Vous aurez alors le plaisir de découvrir un cours complet sur la programmation réseau sous Windows en langage C.

Pour terminer, notons que ce site est également doté d'une rubrique bibliographie qui pourra vous guider dans l'achat de votre prochain livre de chevet ;)

En bref, c'est incontournable pour tous ceux qui s'intéressent de près ou de loin aux domaines informatiques que constituent les réseaux de communications.

LANGUE : Français
URL : <http://www.guill.net>

The screenshot shows the Guill.net website with a navigation bar at the top containing 'News', 'Documents', 'Forum', 'Downloads', 'Bibliographie', 'Liens', and 'Contact'. The main content area is titled 'Les protocoles réseaux' and features several highlighted boxes: 'Famille TCP/IP', 'Réseaux distants', 'RFC Request For Comments', 'Réseaux Sans Fils', 'Protocoles Sécurisés', and 'Autres protocoles'. On the right side, there is a 'Sondage' (Survey) section with a bar chart showing the following data:

Option	Percentage
RTT 56Kbps	8%
ADSL simple de 128 à 2048 Kbps	42%
ADSL + Téléphonie (+TV) de 128 à 2048 Kbps	11%
ADSL simple jusqu'à 20Mbps	12%
ADSL + Téléphonie (+TV) jusqu'à 20Mbps	23%
Autres	7%

Hping

Peu d'entre nous n'ont jamais entendu parler de Hping, et c'est bien normal. En effet, sa puissance fait toute sa popularité dans le monde de la sécurité des réseaux. Hping est un outil de création et d'analyse de trafic TCP/IP.

C'est aussi un outil complet qui peut par exemple servir à tester la sécurité de votre firewall, le fonctionnement de votre réseau, vous permettre de vous entraîner à l'OS fingerprinting, de découvrir les techniques du man in the middle, de l'idle host scanning et j'en passe...

Hping gère plusieurs protocoles tels que TCP, UDP et ICMP.

Lors de l'utilisation de Hping, il est souvent intéressant de travailler avec un analyseur de trafic comme tcpdump ou ethereal. En effet, lorsqu'on génère du trafic avec Hping il est impératif d'analyser les réactions du réseau ou du système cible.

Les fonctionnalités offertes cet outil sont donc énormes et permettent ainsi de comprendre et de maîtriser les possibilités et lacunes de TCP/IP.

OS : Unix

URL : <http://www.hping.org>

```
hzv:/# hping2 -c 6 -S -s 1337 -d 22 192.168.0.1
HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 headers + 22 data bytes
len=40 ip=192.168.0.1 ttl=64 DF id=236 sport=0 flags=RA seq=0 win=0 rtt=0,6 ms
len=40 ip=192.168.0.1 ttl=64 DF id=237 sport=0 flags=RA seq=1 win=0 rtt=0,5 ms
len=40 ip=192.168.0.1 ttl=64 DF id=238 sport=0 flags=RA seq=2 win=0 rtt=0,6 ms
len=40 ip=192.168.0.1 ttl=64 DF id=239 sport=0 flags=RA seq=3 win=0 rtt=0,6 ms
len=40 ip=192.168.0.1 ttl=64 DF id=240 sport=0 flags=RA seq=4 win=0 rtt=0,7 ms
len=40 ip=192.168.0.1 ttl=64 DF id=241 sport=0 flags=RA seq=5 win=0 rtt=0,7 ms

--- 192.168.0.1 hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0,5/0,6/0,7 ms
hzv:/#
```

Rfc-editeur.org

Qui n'a jamais entendu parler des RFC (Request for Comments) ? Il s'agit en fait de papiers techniques, d'abord soumis aux commentaires de la communauté avant de devenir la référence pour les normes de l'Internet. Tout cela est bien beau mais ces textes sont bien entendus rédigés en Anglais, ce qui n'est pas des plus commodes pour beaucoup d'entre nous. Nous avons trouvé l'adresse qui en ravira plus d'un : RFC-Editeur.org. En effet, ce site vous propose à ce jour la traduction françaises de près de 100 de ces textes de références, en de multiples formats comme pdf, html, rtf ou txt. Bien entendu, tous n'y figurent pas, mais vous pourrez aussi consulter les autres, cette fois-ci en Anglais ;)

Si vous désirez participer à ce travail, le site vous accueillera à bras ouvert. Il est aussi possible de consulter les textes en cours de traduction.

C'est peut-être également l'occasion de découvrir quelle RFC a été postée le premier avril, cette année. Traditionnellement, on découvre d'étranges protocoles à cette période de l'année (essayer « 1st april rfc » sur Google). À voir aussi : traduc.org, qui coordonne d'autres projets similaires.

LANGUE : Français

URL : <http://rfc-editeur.org>

RFC-Editeur.org		toutes les RFC traduites en Français		
	Un peu d'éthique...	OCL	73 Ko	54 Ko
RFC 1775	INFO - To be "On" the Internet Ce document attend un relecteur, contacter l'auteur si ce document vous intéresse.	Y. Bouhali	15 Ko	
RFC 1718	IETF - Le TAO de l'IETF Un guide à l'usage des nouveaux participants aux travaux de l'IETF. Ce RFC est rendu obsolète par le RFC3160 - FYI17 (aussi en vf).	Emmanuel Lescop GFSI	28 Ko	
RFC 1663	PPP-TRANS - Transmission PPP Fiable Ce document définit une méthode pour la négociation et l'usage du mode numéroté, pour fournir un lien série fiable.	Yves Lescop Lycée la Croix-Rouge - Brest	22 Ko	49 Ko 31 Ko
RFC 1692 STD 51	PPP-HDLC - PPP dans un tramage similaire à HDLC Ce document décrit l'utilisation du tramage comm-HDLC pour les paquets encapsulés par PPP.	Yves Lescop Lycée la Croix-Rouge - Brest	55 Ko	106 Ko 77 Ko
RFC 1661 STD 51	PPP - Point-to-Point Protocol Le Protocole PPP fournit une méthode standard pour transporter des datagrammes multiprotocoles au-dessus	Valéry G. Fremaux EISTI	193 Ko	212 Ko 182 Ko

Nmap

Qui ne connaît pas Nmap ? Entre nous, peu de monde. Cependant, pour les quelques-uns qui le découvrent en lisant ces lignes, sachez que ce soft pourra vous rendre une multitude de services !

C'est l'outil d'audit réseau rapide, discret et complet par excellence. Parmi ses fonctions, on trouve bien sûr un scanner de ports, un scanner d'IP, un détecteur de systèmes d'exploitation et même un détecteur de version de services distants (version d'Apache, etc.).

De plus, Nmap permet de scanner un serveur distant tout en camouflant son adresse IP parmi les decoy. On utilisera alors l'option -D.

Exemple :

```
# nmap -vv -D IPI,IP2,ME,IP3 -P0 IPCIBLE
```

Ainsi, la cible, ici IPCIBLE, aura l'impression de s'être fait scanner à la fois par IPI,2,3 et nous. Ceci peut être pratique si on se base sur le fait qu'un admin ne pourra analyser une quantité impressionnante de log et contacter un à un le fai de chaque IP.

Nmap, un outil à utiliser sans modération !

OS : Unix, Windows

URL : www.insecure.org

```
C:\unzipped\nmap\nmap.exe
Nmap 3.75 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sI TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF, -sX, -sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: 1-1024,1080,6666,31337
  -P Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid!Sneaky!Polite!Normal!Aggressive!Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve (default: sometimes resolve)
  -oM/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <deviceName> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features
Example: nmap -v -sS -O www.ny.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

Pof

D'abord, Pof est l'outil de fingerprinting passif le plus évolué à ce jour. Le fingerprinting passif consiste à détecter le système d'exploitation de machines dialoguant sur le réseau en ne faisant qu'écouter le trafic. Ainsi, aucun paquet n'est envoyé vers les machines, ce qui rend cette méthode de fingerprinting redoutablement indétectable ! Bien entendu, pour qu'une machine puisse être analysée, il faut qu'elle émette des paquets sur le réseau, et le résultat d'un scan de réseau est à construire avec le temps (plusieurs journées de sniff permettent d'avoir une bonne vision des différents systèmes d'exploitation qui dialoguent sur le réseau).

De plus, le fonctionnement de cet outil est d'une simplicité déconcertante. Il s'installe et se lance très simplement.

Enfin, pour permettre de rendre Pof plus fiable encore, l'auteur nous invite à augmenter la base de fingerprint en visitant la page de son site située à l'url :

<http://camtuf.coredump.cx/pOf-help/>.

OS : *BSD, Linux, Windows

URL : <http://camtuf.coredump.cx/pOf.shtml>

```
firewall:~/pOf# ./pOf -i eth0 -U -q -p
192.168.0.1:1399 - Windows 2000 SP4, XP SP1
  -> 216.239.57.104:80 (distance 0, link: ethernet/modem)
192.168.0.1:1400 - Windows 2000 SP4, XP SP1
  -> 66.102.9.104:80 (distance 0, link: ethernet/modem)
192.168.0.1:1401 - Windows 2000 SP4, XP SP1
  -> 66.102.9.104:80 (distance 0, link: ethernet/modem)
192.168.0.1:1402 - Windows 2000 SP4, XP SP1
  -> 216.166.85.97:80 (distance 0, link: ethernet/modem)
192.168.0.1:1403 - Windows 2000 SP4, XP SP1
  -> 216.166.85.97:80 (distance 0, link: ethernet/modem)
192.168.0.1:1404 - Windows 2000 SP4, XP SP1
  -> 216.166.85.97:80 (distance 0, link: ethernet/modem)
192.168.0.1:1405 - Windows 2000 SP4, XP SP1
  -> 212.27.33.225:80 (distance 0, link: ethernet/modem)
192.168.0.1:1406 - Windows 2000 SP4, XP SP1
  -> 212.27.33.225:80 (distance 0, link: ethernet/modem)
192.168.0.1:1407 - Windows 2000 SP4, XP SP1
  -> 212.27.33.225:80 (distance 0, link: ethernet/modem)
192.168.0.1:1408 - Windows 2000 SP4, XP SP1
  -> 207.68.178.16:80 (distance 0, link: ethernet/modem)
192.168.0.1:1409 - Windows 2000 SP4, XP SP1
```

Salemioche !

Le site est sérieux même s'il porte un nom plutôt amusant. Salemioche.com donne une analyse intéressante et sur plusieurs niveaux des protocoles communs comme http, smtp, ftp, irc, imap et j'en passe.

Chaque protocole est traité en plusieurs étapes. Une partie nous permet de comprendre le principe, les possibilités et les limites du protocole étudié tandis qu'une autre nous présente une session telnet où l'on peut voir comment fonctionne le protocole en fonction des diverses commandes passées grâce à ce programme (les log fournis sont très clairs grâce à un code couleur qui permet de s'y retrouver facilement). Ensuite vient une partie programmation, également intéressante, où des exemples de code nous montrent comment manier certains protocoles à travers plusieurs langages (principalement : C, C#, Java, VB). Enfin une synthèse est présentée pour clore l'analyse.

Bien entendu, si vous voulez aller plus loin sur l'étude d'un protocole, rien de tel que la RFC en Français, directement disponible sur le site.

Bonne visite !

LANGUE : Français

URL : <http://www.salemioche.com>

The screenshot shows the 'protocole HTTP' section of the Salemioche website. It includes a sidebar with navigation links like 'Comment ça marche', 'Session telnet', and 'Programmation'. The main content area contains a description of HTTP and several links to resources, including 'Comment ça marche', 'Débuter sur HTTP', 'Session telnet', 'Programmation', 'RFC 1.1 en anglais', and 'RFC 1.0 en français'.

Scapy

Il y a quelques jours, sur le salon officiel de l'Hackademy, une personne est venue en demandant quel était le meilleur langage de programmation pour débiter. Je lui ai proposé le Python qui est simple et complet pour démarrer. On m'a alors interpellé en me disant que le C était le meilleur, le plus puissant et pas si complexe que ça. Pour prouver ma bonne foi, j'ai trouvé Scapy, qui est un programme très intéressant en Python, eh oui :-)

Scapy est un outil très performant de manipulation de paquet réseau. Il permet, selon l'auteur, de remplacer hping, nmap dans 85 % des cas, arpspoof, arp-sk, arping, tcpdump, ethe-real et p0f. Scapy peut en effet générer et sniffer toutes sortes de paquets. L'avantage est qu'il permet de manipuler tout cela à un haut niveau d'abstraction, sous la forme d'objet Python sur lesquels on peut agir de manière interactive ou scriptée, assez simplement (voir la séance de sniff directement dans l'interpréteur en capture et les nombreuses démos du site).

Packages disponibles pour RedHat et Debian.

OS : Linux

URL : <http://www.cartel-securite.fr/pbiondi/projects/scapy.html>
Logiciel Libre

The screenshot shows a terminal window with the Scapy interface. The user has entered a command to sniff traffic on port 25 or 110. The output shows several packets being captured and analyzed, including a successful login attempt with the password 'toto' and a failed login attempt with the password 'tata'.

```
Echier Édition Affichage Terminal Onglets Aide
>>> a=sniff(filter="tcp and ( port 25 or port 110 )",
prn=lambda x: x.strftime("%IP.src%:%TCP.sport% -> %IP.dst%:%TCP.dport
% %2s,TCP.flags% : %TCP.payload%"))
192.168.8.10:47226 -> 213.228.0.14:110 S :
213.228.0.14:110 -> 192.168.8.10:47226 SA :
192.168.8.10:47226 -> 213.228.0.14:110 A :
213.228.0.14:110 -> 192.168.8.10:47226 PA : +OK <13103.1048117923@po
p2-1.free.fr>

192.168.8.10:47226 -> 213.228.0.14:110 A :
192.168.8.10:47226 -> 213.228.0.14:110 PA : USER toto

213.228.0.14:110 -> 192.168.8.10:47226 A :
213.228.0.14:110 -> 192.168.8.10:47226 PA : +OK

192.168.8.10:47226 -> 213.228.0.14:110 A :
192.168.8.10:47226 -> 213.228.0.14:110 PA : PASS tata

213.228.0.14:110 -> 192.168.8.10:47226 PA : -ERR authorization failed
```

Tcpdump

Tcpdump est la référence en matière de sniffer ! En effet, c'est le sniffer par excellence sous linux, le plus abouti et le plus malléable. Son utilisation est des plus simples, sa prise en main rapide et il vous suffira de lire le man (man tcpdump) pour connaître toutes les possibilités que vous offre ce soft.

Admirez, grâce à un exemple, quelques-unes de ces possibilités.

Dans le cas suivant, la passerelle, qui est donc la machine à partir de laquelle est exécuté TCPDump, filtre tout ce qui arrive de la machine 192.168.0.1 à destination d'un serveur FTP sur Internet (port 21). Grâce à l'option -X de TCPDump, nous pouvons avoir une visualisation du contenu des paquets en ASCII et en hexadécimal :

```
# tcpdump -X -s 0 src 192.168.0.1 and port 21
```

On obtient alors quelque chose du type :

```
[..]
00:34:03.145837 192.168.0.1.2698 > ftperso.free.fr.ftp: P 44:56(12)
ack 182 win 65205 (DF)
0x0000 4500 0034 31d3 4000 8006 0b30 c0a8 0001   E..41.@....0...
0x0010 d41b 28fc 0a8a 0015 dc77 67ee 7b1d 4ffe   ..(.....wg.{.O.
0x0020 5018 feb5 e852 0000 4357 4420 6e69 7472   P...R..CWD.nitr
0x0030 7978 0d0a                                     yX..
[..]
```

On voit clairement que la commande FTP "CWD nitryx" (la commande FTP "CWD" correspond au "cd" sur une machine unix) a été lancée par 192.168.0.1 sur le serveur.

Bien entendu, cela reste un exemple. Il y a en effet des utilisations de tcpdump bien plus intéressantes que celle-ci. Par exemple, auditer votre réseau pour découvrir ce qui y transite ou non en « clair » sur (donc non-crypté), vérifier l'efficacité de votre forgeur de paquets et j'en passe...

TCPDump est donc un outil que tout le monde devrait avoir sous la main afin de mieux comprendre, par exemple, le fonctionnement de son réseau.

OS : Linux

URL : <http://www.tcpdump.org>

1st security center

1st Security Center Pro est un programme que tout administrateur Windows devrait posséder. Il permet en effet de combler quelques lacunes de l'OS de Microsoft, notamment au niveau de la gestion des permissions des utilisateurs. Il offre donc la possibilité d'empêcher les éventuelles actions malveillantes ou tout simplement aux parents de limiter l'accès à leurs enfants.

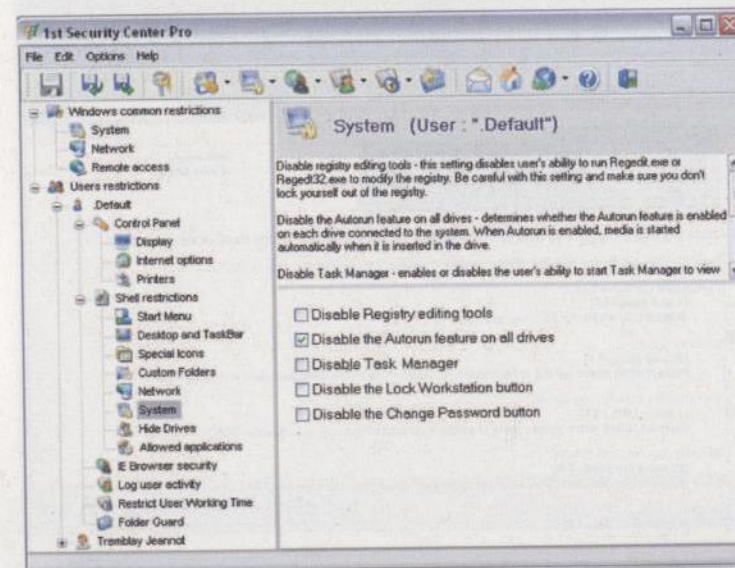
L'application de règles différentes pour chaque utilisateur est un point essentiel sur lequel j'aimerais retenir votre attention : deux utilisateurs peuvent ne pas avoir les mêmes libertés sur le système.

Ainsi, 1st Security Center Pro est capable d'effectuer de multiples actions. Des utilisateurs peuvent se voir restreindre l'accès au panneau de configuration, aux dossiers ou même à l'éditeur de registre. Il peut également masquer des menus d'administration dans Internet Explorer ou dans le menu démarrer ainsi que rendre invisibles certains lecteurs dans le poste de travail.

Bien entendu, ce n'est pas la peine de préciser que l'interface de gestion est protégée par un mot de passe.

OS : Windows

URL : <http://www.1securitycenter.com>



Hsc

Le site de cette célèbre société de conseil en sécurité informatique est très intéressant par le nombre de documents techniques de référence qui y sont publiés. Par les temps qui courent, il est très rare qu'une société commerciale fournisse les codes sources de ses travaux et interventions publiques. HSC est de celles-là. Et elle propose des supports de cours ou des articles sur le Net en libre accès. Les sujets abordés sont par exemple les "mécanismes d'authentification HTTP/HTTPS", "Bases de données et sécurité" ou "Fonctionnement des PKI".

Vous y trouverez également des outils en open-source développés pour leurs tests d'intrusion tels que Wifiscanner (wardriving), babelweb (tests d'un serveur web), ssltunnel (établissement d'un tunnel ppp par dessus une connexion ssl) et bien d'autres choses utiles en libre téléchargement. Comme quoi toutes les boîtes de sécurité ne font pas que se gaver de la recherche en sécurité réalisée gratuitement par des hackers. Tout cela est présenté de manière claire et un index permet d'accéder rapidement aux documents concernant un thème particulier. Un bel exemple qui, nous l'espérons, sera pillé par les autres entreprises de sécurité... du point de vue de la philosophie du site bien sûr ;)

LANGUE : Français

URL : <http://www.hsc.fr>

Cabinet de consultants en sécurité informatique depuis 1998 - Spécialisé sur Unix, Windows, TCP/IP et Internet

HSC
Hervé Schauer Consultants
Consultants en Sécurité Informatique

Vous êtes ici : Accueil > Ressources > Supports de cours

Services

- Domaines de compétences
- Conseil & Expertise
- Installation & Configuration
- Veille en vulnérabilités
- Audit & Evaluation
- Tests d'intrusion
- Tests de vulnérabilités (TSAR)
- Assistance Technique
- Formations

Conférences

- Agenda
- Interventions passées
- Tutoriels

Ressources

- Index thématique
- Bibles
- Présentations
- Cours
- Articles
- Outils (téléchargement)
- Veille en vulnérabilité

Supports de cours

Voir aussi...
• Formations

Cette page donne accès à certains de nos supports de cours, que nous avons choisi de rendre publics. Pour plus de détails sur nos formations, veuillez consulter [cette page](#) ou nous contacter .

Fonctionnement des PKI
[4 avril 2003 - 11]

Support du cours Fonctionnement des PKI .

Sécurité Solars
[22 avril 2002 - 11]

Présentation ayant servi à la réalisation du support de notre formation Sécurité Solars .

Introduction à la cryptographie
[9 février 2001 - 11]

Support utilisé entre autres dans la partie 4 du cours Sécurité des réseaux TCP/IP .

Sécurité des réseaux TCP/IP
[25 novembre 1999 - 11]

Support des deux premières parties du cours Sécurité des réseaux TCP/IP .

Sécurité Linux
[9 décembre 1999 - 11]

Hide Folder

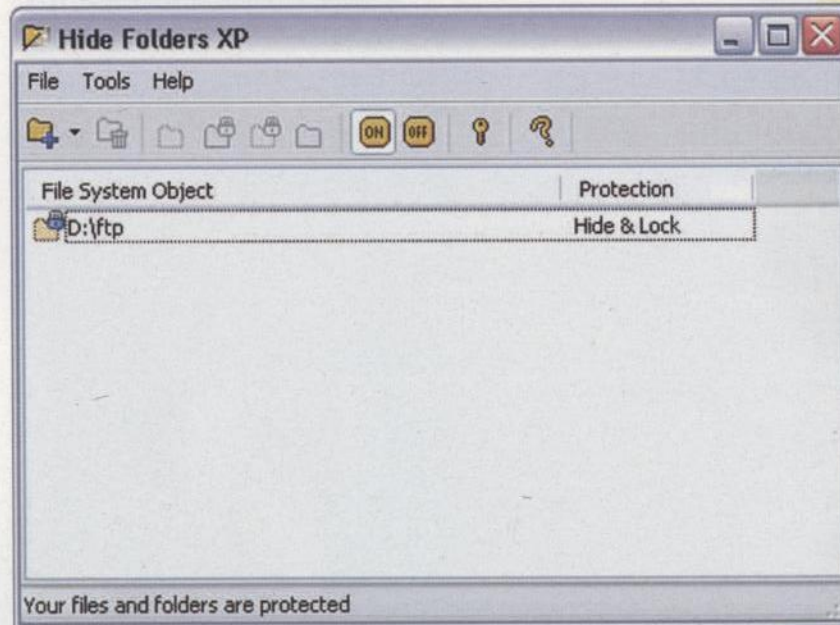
La plupart des utilisateurs ont des dossiers et des fichiers personnels sur leur ordinateur qu'ils ne veulent pas partager avec d'autres personnes susceptibles d'utiliser leur machine. Ceci pourrait inclure l'information financière, administrative, des mots de passe (cf. Password Safe - Pour enregistrer en sécurité vos mots de passe sur votre ordinateur), des lettres, des notes personnelles, des numéros de série et une foule d'autres données privées et personnelles.

La meilleure manière de protéger ces informations est de faire des dossiers spécifiques dans lesquels résident les données et disponibles uniquement pour vous. En un clic de souris, ceux-ci sont devenus invisibles. C'est-à-dire qu'il est impossible de les retrouver, d'accéder aux informations qu'ils contiennent et même de les supprimer (même en enlevant directement le dossier de niveau supérieur).

Un bon moyen donc, de préserver sa vie privée dans l'univers Microsoft Windows.

OS : Windows

URL : <http://www.fspro.net>



Linux-sec.net

Personnellement, j'adore ce site ! Plutôt axé sur le contenu que la présentation, il regroupe toutes les informations dont vous avez besoin pour améliorer ou vérifier la sécurité de votre linux. Car linux-sec est un portail qui se révélera une mine d'or pour vos ressources en matière de sécurité. Avec des centaines de liens vers tous les sujets touchant de près ou de loin à ce thème. Au hasard de nombreuses rubriques, vous pourrez trouver par exemple (attention, prenez votre souffle ;) toutes les distributions, les patches kernel, les dernières vulnérabilités, les stats des attaques, les outils de sécurité (firewall, IDS, monitoring, tracking...). Et ce n'est qu'une partie seulement :) De nombreux conseils et astuces sont aussi disséminés sur le site et au fil des pages on peut apprendre à mieux connaître son OS préféré. Linux-sec a de quoi satisfaire les plus exigeants et permet de trouver rapidement les meilleurs sites sur tous ces sujets.

LANGUE : Anglais
URL : <http://www.linux-sec.net>

The screenshot shows the website interface for Linux-sec.net. On the left is a navigation menu with links for 'Hardening - Tightening', 'Security Policy', 'Hardening HOWTO', 'Linux Distros', 'Distro Patches', 'Kernel-Patches', and 'Dedicated Servers'. The main content area is titled 'Kernel Hardening' and includes a search bar and a list of links under 'Minimum Kernel Hardening' such as 'Kernel.org Linux Kernel Sources', 'Download, Compile and Install the latest kernel', and 'Apply Additional Kernel Security Enhancements'.

Linuxsecurity.com

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

LANGUE : Anglais
URL : <http://www.linuxsecurity.com>

The screenshot shows the website interface for Linux Security.com. It features a search bar at the top, a navigation menu with 'News', 'Advocates', 'Resources', and 'Newsletters', and a main content area with 'HOWTO/FAQS' and 'Resources' sections. The 'Resources' section lists articles like 'Networking in NSA Security-Enhanced Linux' and 'Apache 2 with SSL/TLS'. There is also a sidebar with 'Guardian Digital' and 'Free Encryption Software'.

MBSA

Attention ! Microsoft a enfin créé un outil qui permet à n'importe qui de configurer correctement son système d'exploitation Windows, de rechercher et d'installer efficacement les mises à jour manquantes et de repérer ses erreurs de configuration. Le but : pallier le manque de sécurité sur les systèmes Windows installés par défaut.

C'est un programme qui analyse la configuration du système pour y mettre en évidence les problèmes les plus courants, comme par exemple les mots de passe trop simples ou inexistant, la configuration des mises à jour automatiques, le type de système de fichier ou encore le nombre d'administrateurs sur l'ordinateur ainsi que d'autres subtilités moins connues.

Le rapport présenté à la fin de l'analyse est intéressant et même pédagogique. En effet, il donne non seulement le résultat, positif ou négatif, des nombreux tests, mais aussi le détail des ressources analysées et les explications nécessaires à la compréhension et éventuellement à la correction du problème.

Il est intéressant de noter que MBSA pourra analyser votre ordinateur mais également ceux de votre réseau, simplement en précisant le nom de domaine et la plage IP à analyser !

OS : Windows 2K, XP, 2003

URL : <http://microsoft.com/technet/security/tools/mbsahome.msp>

Nsa.gov

La plus grande agence gouvernementale américaine livre au grand public ses connaissances en matière de sécurité informatique sur son site Internet. Alors que certains proclament l'insécurité des systèmes Microsoft et la force des systèmes Open Source, la NSA, elle, l'affiche fièrement comme le système d'exploitation de toute l'administration américaine, et ce depuis longtemps. La NSA, qui possède depuis le début le code source de Windows, connaît bien le système et a appris à le rendre suffisamment fiable pour l'administration américaine.

Sur ce site, on nous propose alors des guides de configuration pour Windows XP, 2000 ainsi que Server 2003 (et pas des moindres, par exemple un document de 143 pages pour la sécurité de Windows XP).

Du côté Web (serveurs et navigateurs), vous trouverez le guide du légendaire Microsoft IIS, d'IE 5.5 et même de Netscape.

Bien entendu, d'autres termes sont abordés.

En tout cas, pas moins d'une quarantaine de guides de sécurité et de fichiers de configuration sont disponibles. Cependant, aucun logiciel libre n'est à l'affiche...

LANGUE : Anglais

URL : <http://www.nsa.gov/snac/>

PC Security Test 2005

Vous voilà devant votre nouveau système fraîchement refait et configuré. Il est à jour et vous avez dépensé des centaines d'euros pour le protéger. Mais comment être sûr d'être paré contre les attaques de base ? Eh bien, voici un logiciel qui répondra à vos attentes ! PC Sécurité Test va simuler différentes attaques simples pour évaluer la fiabilité de vos outils.

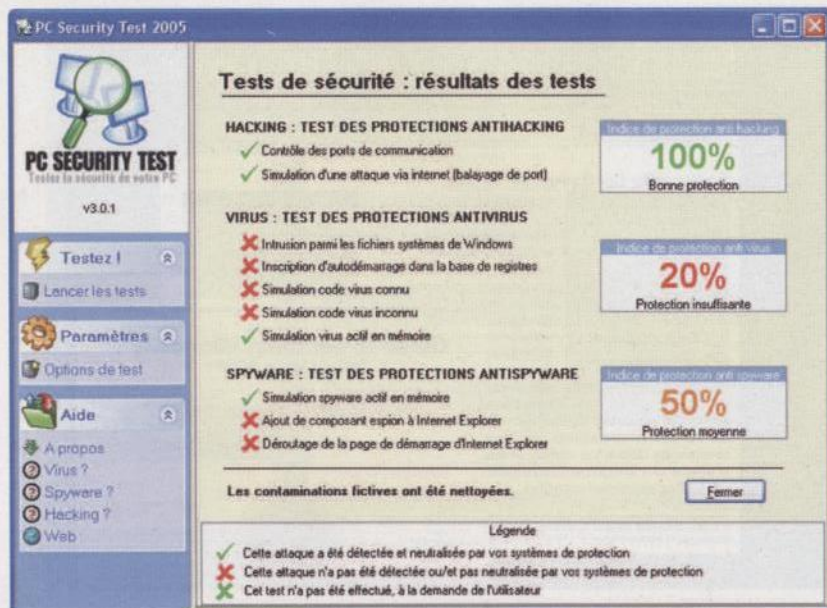
Au menu : contrôle et scan des ports, inscription dans la base de registre, simulation de code de virus connus (signature) et inconnus (euristique) et changement de configuration de votre navigateur web préféré (ajout de composants à Internet Explorer et changement de la page de démarrage ;>)

Le logiciel est en Français, vraiment simple d'utilisation et relativement pédagogique. Vous ne risquez pas d'être perdu. Une rubrique d'aide est à la disposition de ceux qui voudraient en savoir plus.

Ce logiciel n'a pas la prétention de tester toutes les techniques connues, mais seulement les plus utilisées. Redoutable pour convaincre quelqu'un en deux clic qu'il devrait changer de protection... ou de système d'exploitation ;)

OS : Windows

URL : <http://www.pc-st.com>



Portsentry

PortSentry est un programme qui fonctionne sous de multiples Unix. Il s'adapte aux comportements de chacun d'eux. Son unique objectif est de prévenir les tentatives d'intrusion sur un système.

Quand un pirate veut s'attaquer à une machine, il va souvent commencer par scanner les ports de sa cible à la recherche de services potentiellement vulnérables. C'est dans cette configuration qu'intervient PortSentry. Lorsqu'il détecte le scan, il bloque immédiatement toute communication de la machine équipée de PortSentry avec la machine attaquante. Pour y parvenir, il peut par exemple créer une règle de firewalling et ajouter une entrée dans /etc/hosts.deny. Tout cela, bien entendu, logué dans /var/log/messages. Pour les plus paranos d'entre nous, il est également possible d'exécuter une commande lorsqu'un scan est détecté. Par exemple `ifconfig -i eth0 down ;`

PortSentry marque ainsi un point essentiel par rapport aux programmes passifs qui se contentent seulement de détecter les scans en cours.

OS : Linux

URL : <http://sourceforge.net/projects/sentrytools/>

```
1127844068 - 09/27/2005 20:01:08 Host: 192.168.0.1/192.168.0.1 Port: 636 TCP Blocked
1127844108 - 09/27/2005 20:01:48 Host: 192.168.0.1/192.168.0.1 Port: 389 TCP Blocked
1127844350 - 09/27/2005 20:05:50 Host: 192.168.0.1/192.168.0.1 Port: 389 TCP Blocked
1127844484 - 09/27/2005 20:08:04 Host: 192.168.0.1/192.168.0.1 Port: 636 TCP Blocked
1127845071 - 09/27/2005 20:17:51 Host: 192.168.0.10/192.168.0.10 Port: 100 TCP Blocked
1127845198 - 09/27/2005 20:19:58 Host: 192.168.0.10/192.168.0.10 Port: 100 TCP Blocked
```

```
hzt:/home/nitrix# hping2 --scan 100-200 -a 192.168.0.10 -S 192.168.0.1
Scanning 192.168.0.1 (192.168.0.1), port 100-200
101 ports to scan, use -V to see all the replies
-----
|port| serv name | flags | ttl | id | win |
-----
All replies received, Done.
Not responding ports: (100 ) (101 hostnames) (102 iso-tsap) (103 ) (104 acr-nema)
(105 csnet-ns) (106 poppassd) (107 rtelnet) (108 ) (109 pop2) (110 pop3) (111 sunrpc)
(112 ) (113 auth) (114 ) (115 sftp) (116 ) (117 uucp-path) (118 ) (119 nntp)
(120 ) (121 ) (122 ) (123 ntp) (124 ) (125 ) (126 ) (127 ) (128 ) (129 puidg)
(130 ) (131 ) (132 ) (133 ) (134 ) (135 loc-srv) (136 ) (137 netbios-ns) (138 netbios-dgm)
(139 netbios-ssn) (140 ) (141 ) (142 ) (143 imap2) (144 ) (145 ) (146 ) (147 ) (148 )
(149 ) (150 ) (151 ) (152 ) (153 ) (154 ) (155 ) (156 ) (157 ) (158 ) (159 ) (160 )
(161 snmp) (162 snmp-trap) (163 cimp-man) (164 cimp-age) (165 ) (166 ) (167 ) (168 )
(169 ) (170 ) (171 ) (172 ) (173 ) (174 mailq) (175 ) (176 ) (177 xdmcp) (178 nextstep)
(179 bgp) (180 ) (181 ) (182 ) (183 ) (184 ) (185 ) (186 ) (187 ) (188 ) (189 ) (190 )
(191 prospero) (192 ) (193 ) (194 irc) (195 ) (196 ) (197 ) (198 ) (199 smux) (200 )
hzt:/home/nitrix#
```

Rootkithunter

RootKit Hunter est un logiciel libre qui permet de détecter la présence de certains rootkits sur les systèmes unix. Pour y parvenir, ce script bash effectue une longue série de tests. D'abord, il y a un test d'intégrité (md5) des fichiers importants – notamment des binaires utilisés par le script même – en fonction d'une base de données de divers systèmes et leurs différentes versions (surtout pertinent sur les systèmes propriétaires). Ensuite, il cherche des fichiers connus pour être utilisés par certains rootkits. Enfin, RkHunter détecte des anomalies dans les permissions des fichiers, des ports ouverts, ou même des LKM et KLD suspects. RootKit Hunter s'adapte à l'OS testé et effectue les tests les plus appropriés. Sur Linux par exemple, le programme compare le contenu de /proc avec la sortie de ps.

Complémentaire à chkrootkit (www.chkrootkit.org), cet outil peut s'avérer très utile si vous craignez que votre système ait été compromis. Mais n'oubliez pas que ce genre de tests ne pourra que vous prouver que vous avez bien été piraté, mais certainement pas l'inverse.

OS : unix

URL : <http://www.rootkit.nl>

```

/usr/bin/du [ OK ]
/usr/bin/file [ OK ]
/usr/bin/find [ OK ]
/usr/bin/head [ OK ]
/usr/bin/kill [ OK ]
/usr/bin/login [ OK ]
/usr/bin/lsattr [ OK ]
/bin/netstat [ BAD ]
/bin/ps [ OK ]
/bin/sh [ OK ]
/bin/su [ OK ]
/usr/bin/chatr [ OK ]
/usr/bin/wc [ OK ]
/usr/bin/wget [ OK ]
/usr/bin/whereis [ OK ]
/usr/bin/who [ OK ]

```

[Press <ENTER> to continue]

Check rootkits

* Default files and directories

```

Rootkit '55808 Trojan - Variant A'... [ OK ]
Rootkit 'AjaKit'... [ OK ]
Rootkit 'aPa Kit'... [ OK ]

```

Securemac.com

Une fois n'est pas coutume ! En effet, tout au long de ce hors série, nous parlons beaucoup de la sécurité Windows ou Linux, mais ces fameuses machines communément appelées Mac y ont aussi leur place !

Securemac est l'une des références en la matière ! Ceux possédant un mac vont être comblés ! Au menu : virus, cryptographie, sécurité système, réseau et même physique ! Le site propose également des outils à télécharger comme des anti spyware, des outils pour sécuriser OS X, des antivirus, des firewalls, des outils d'analyse réseau et bien d'autres encore... En première page, toute l'actualité de la sécurité mac visible en un coup d'œil.

De plus, bien que les papiers ne soient pas nombreux, ils ne restent pas moins intéressants et très instructifs, même si vous ne tournez pas sur le système en question.

Bref, Securemac est une véritable mine d'or pour les amateurs de l'OS à la pomme. Un site à visiter donc, et à conserver dans vos bookmarks !

LANGUE : Anglais

URL : <http://www.securemac.com>

* Conventions
* Feedback Form

New Mac Security News

Macintosh Security CD, T-Shirts, and Security books



Mac OS X Security

* Root Shell in 4 steps with setuid apps
* sudo buffer overflow exploit + fix
* Disable Single User Boot Mode
* Malevolence - Dumping Passwords
* nidump security
* Startup Security - Open Firmware Password Protection

Mac OS X Network

We just added the following Data to our Site:
6.29.2005 News

Proxify Dashboard Widget allows you to safe securely through the Proxify network allowing for stripping of advertisements and protection of the user while surfing. Some other features include surfing in text only, remove cookies, remove scripts, hide referral information and other encoding options.

6.8.2005 News

New security update is available for Mac OS X downloadable from the Software Update system preference panel.

6.2.2005 News

QuickTime 7.0 contains a security bug where a maliciously crafted **Quartz Composer object** can leak data to an arbitrary web location. Apple has released QuickTime 7.0.1 which addresses this issue, users should upgrade.

With the release of Mac OS X 10.4, the version of FileVault included addresses an issue discussed in this **FileVault advisory**. Mac OS X 10.4 allows the user to securely delete the data, however the issue still remains 10.3.9.

5.26.2005 News

Clam Anti-Virus (ClamAV Mac OS X) is affected by a command execution vulnerability as described within

Security + OS

* ATEase
* DistLock
* PowerBook Security Control Panel
* Empower Pro
* FileGuard
* FreeGuard
* FoolProof
* Deus Lock Master
* OnGuard
* Keys Off
* LockOut
* MacOS Algorithm
* Modern Security
* Password Key
* PGPUam
* PPE
* Shift Key Suite
* Stealth Signal
* SuperLock Lite
* SuperLock Pro
* Web-Confidential

Macintosh Viruses

* Agax 1.3
* Disinfectant
* Sophos Anti-Virus
* Norton AntiVirus
* Nav 7 Nav 6 Nav X
* Virex - Oct

Sentinix

Sentinix est une distribution Linux principalement destinée à la détection d'intrusions et au monitoring réseau. Cette distribution regroupe les plus grands programmes en la matière. On ne citera ici que les plus connus, Snort pour la détection d'intrusions et Nagios pour le monitoring réseau.

D'abord, on ne signalera aucun problème lors de l'installation de la distribution, qui s'effectue rapidement et simplement.

En outre, la configuration de ses outils et le monitoring sont facilités grâce à l'interface web (cf. capture). Vous aurez alors la chance de pouvoir y trouver des schémas et graphiques pour une meilleure visualisation des différents événements.

Enfin, ajoutons que grâce à Nagios, vous pourrez toujours garder un œil sur vos serveurs ou vos stations de travail et être immédiatement prévenu si l'un d'entre eux tombait en panne. Sentinix est donc une distribution que devrait utiliser tout administrateur réseau soucieux de l'intégrité de son domaine.

URL : <http://www.sentinix.org>

Nagios

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Status Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map

- Service Problems
- Network Outages

- Trends
- Availability
- Alert History
- Notifications
- Log File

- Comments
- DownTime

Status Summary For All Host Groups

Host Group	Host Status Totals	Service Status Totals
Windows Workstations (winworkstations)	1 UP	1 OK
Beowulf Servers (beowulf-servers)	1 DOWN 4 UNREACHABLE	0 CRITICAL
Linux Servers (linux-servers)	6 UP	1 OK 18 PROBLEM
Mail Servers (mail-servers)	1 UP	1 OK 3 PROBLEM
Novell Servers (novell-servers)	4 UP	10 OK 2 WARNING
NT Domain Servers (nt-domain-servers)	3 UP	10 OK
NT Web Servers (nt-web-servers)	3 UP	21 OK 1 CRITICAL
Printers (printers)	2 UP 1 DOWN	4 OK 1 CRITICAL
	1 UP	1 OK

Securite.org

En ne pouvait espérer mieux ! Un annuaire sur la sécurité. En effet, securite.org recense plusieurs centaines de sites dédiés à la sécurité informatique. La présentation du site est ce qu'il y a de plus simple mais aussi de plus pratique, et sa consultation des plus agréables. Chaque site de l'annuaire dispose d'une description écrite mais aussi d'indications visuelles nous permettant de connaître la qualité (grâce à des étoiles) et la langue d'un site dès le premier coup d'œil.

Securite.org se partage en quatre grandes catégories : Sécurité, Crypto, Linux et Réseau. Celles-ci sont par la suite divisées en sous-catégories afin d'affiner votre recherche et de trouver les sites qui correspondent le mieux au sujet qui vous intéresse. Notons également que l'outil de recherche rapide peut parfois rendre service.

Outre son côté « annuaire », securite.org dispose également de quelques dossiers qui pourront parfois vous apprendre quelques notions intéressantes.

Enfin, pour couronner le tout, sachez que le site est également disponible via HTTPS :

LANGUE : Français

URL : <http://www.securite.org>

Accueil Ressource : Tout ce qui concerne la sécurité

Vous êtes dans : Sécurité OK

Les sous-catégories :

- Administration
- Attaques Distribuées
- Audit
- Authentification
- Autopsie
- BoF
- ChaineFormat
- Divers
- E-zine
- Firewalls
- GSM
- IDS
- Information
- Java
- People
- PotDeMiel
- Societes
- Systemes
- ViePrivee
- Virus
- Vulnerabilites

Rechercher dans la base : Rechercher

IT Security Cookbook ★★★★★ Guide sécurité traitant des menaces et des analyses de risques ainsi que de la marche à suivre pour créer une politique de sécurité. Ce site fournit aussi des informations techniques pour sécuriser de nombreux systèmes.
<http://www.boran.com/security/> [Document HTML]

Pages sécurité de Loria ★★★★★ Très intéressantes évaluations de produits de sécurité (firewalls, IDS, analyseur de logs, etc.)
<http://www.loria.fr/services/moyens-info/securite/> [Document HTML]

Projet CID ★ Base de données de menaces, d'attaques, de défenses et de contremesures.
<http://all.net/CID/overview.html> [Document HTML]

eXperts

Interview

SSM

System Safety Monitor est un outil qui va permettre à tout administrateur Windows de vraiment contrôler l'activité de son système. En effet, SSM est capable de superviser les processus, le registre, les services ou les fichiers tels que win.ini et system.ini.

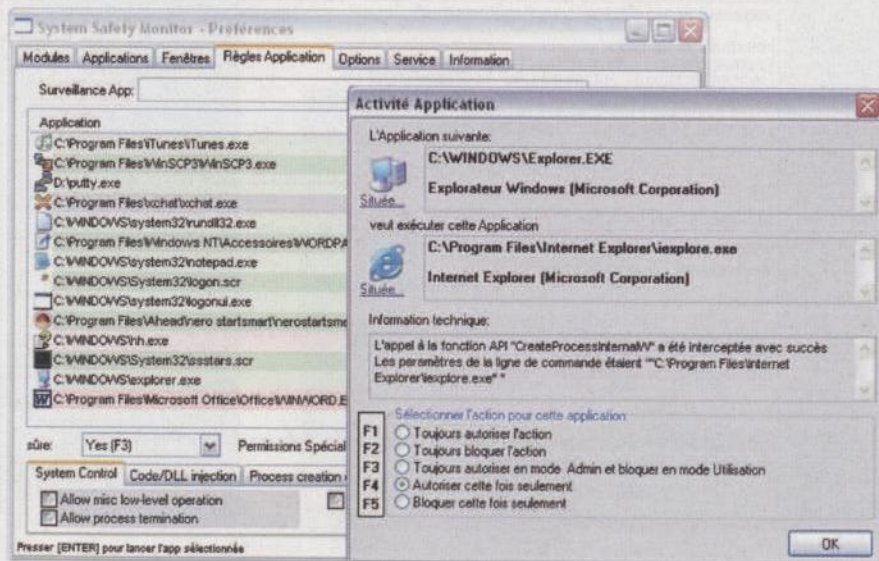
Ensuite, grâce à SSM, il est possible d'accepter ou de refuser toute action qu'un programme souhaiterait effectuer. Par exemple, Explorer.exe aimerait lancer un programme douteux; vous pouvez alors immédiatement bloquer son exécution.

Enfin, nous porterons notre attention sur une autre possibilité majeure que nous offre ce programme. SSM va pouvoir filtrer les entêtes de vos fenêtres grâce à une blacklist que vous aurez pris le soin de compléter. Cette option est très pratique, surtout si vous ne possédez pas d'anti-popup ou que vous souhaitez protéger l'accès à un dossier.

Si vous vous référez au numéro précédent, vous pourrez constater que le duo IstSecurityCenter/SSM se révèle être d'une grande efficacité et donne alors la main sur la quasi-totalité du système.

OS : Windows

URL : <http://kormushkin.narod.ru/>



Tripwire

Ce logiciel open source est en priorité destiné au monde *nix et fera le bonheur de tous les administrateurs et root en tout genre. Il est intéressant de noter qu'une version commerciale est également disponible pour les systèmes Solaris, Windows NT, HP-UX et IBM AIX. Tripwire est un programme qui permet de vérifier en temps réel la modification des fichiers les plus importants sur votre système.

C'est donc un contrôleur d'intégrité qui compare les propriétés des dossiers et des fichiers contre l'information stockée dans une base de données précédemment produite lors de l'installation. Tous les changements sont notés, y compris ceux qui ont été ajoutés ou supprimés, avec la possibilité d'être averti directement par mail. De plus, les dossiers contenant les informations (bases de données, rapports...) sont cryptés, ce qui permet d'en assurer la confidentialité. C'est un outil qui devrait être installé juste après la mise à jour de votre système pendant le processus d'installation de votre distribution, afin de garantir que les fichiers marqués ne soient pas déjà corrompus.

OS : Linux

URL : <http://www.tripwire.org>

```
Section: Unix File System
```

Rule Name	Severity Level	Added	Removed
Invariant Directories	66	0	0
* Tripwire Data Files	100	1	0
Other binaries	66	0	0
Tripwire Binaries	100	0	0
Other libraries	66	0	0
Root file-system executables	100	0	0
System boot changes	100	0	0
Root file-system libraries (/lib)	100	0	0
Critical system boot files	100	0	0
Other configuration files (/etc)	66	0	0
Boot Scripts	100	0	0
* Security Control	66	0	0
* Root config files	100	0	0
* Devices & Kernel information	100	98	49

Total objects scanned: 26254
Total violations found: 148

Windowsecurity.com

Windowsecurity est un site en Anglais traitant uniquement, comme son nom l'indique, de la sécurité touchant à Windows. Le site est organisé selon deux parties principales. En première partie, une section Antivirus qui nous présente les derniers virus qui hantent les réseaux, les risques de se faire infecter et surtout les différentes manières de s'en prémunir. Une multitude d'articles nous aide alors à mieux nous protéger.

En seconde partie, une section comportant des textes sur des domaines aussi distincts que la sécurité sous Win 2003, les serveurs web sous Windows, la détection d'intrusions et bien d'autres encore...

Tout le monde y trouvera son compte, y compris les débutants, car les textes proposés requièrent des niveaux de compétence divers.

Nous ajouterons également que ce site est mis à jour régulièrement. Nous pouvons donc, dès la page d'accueil, consulter les derniers articles disponibles.

Windowsecurity est un site au contenu très varié qui ne demande qu'à être visité par tous ceux qui désirent améliorer leur sécurité.

LANGUE : Anglais

URL : <http://www.windowsecurity.com>

Anti Virus Section

Articles & Tutorials

- Authentication, Access Control & Encryption
- Content Security (Email & FTP)
- Firewalls & VPNs
- Intrusion Detection
- Misc Network Security
- Viruses, trojans and other malware
- Web Server Security
- Windows 2003 Security
- Windows Networking
- Windows OS Security
- Wireless Security

Authors

- Email Security Test
- Event Log Scan
- Links
- Message Boards

Anti Virus section

Virus Warnings

HIGH RISK

MyDoom.L (Jul 26)

MEDIUM RISK

Bagle.AK (Aug 31)
MyDoom.M (Aug 16)
Lovgate.AJ (Jul 08)
Zafi.B (Jun 14)
Netsky.B (Feb 18)
Swen.A (Sep 18)

LOW RISK

Bagle.AI (Aug 09)
Bagle.AH (Jul 19)
Bagle.AF (Jul 18)
Bagle.AE (Jul 16)
Netsky.Q (Mar 30)
Netsky.P (Mar 25)
Netsky.D (Mar 01)

NORMAN
Virus Warnings

Anti Virus White Papers

- **Remote user security: Your IT's Achilles heel? (By Sophos) - Aug 26, 2004**
Remote working has radically altered employment practices within the new economy, but the benefits (such as employee flexibility and increased productivity) need to be balanced against the problems of managing teleworkers. In particular, companies need to make sure that remote PCs remain properly protected against computer viruses and other security exposures.
- **Windows Scripting Host - disabling .VBS association (By Norman) - Jan 22, 2004**
Windows Scripting Host (WSH) is a part of some of Microsoft's 32 bits


Winsec.epfl.ch

Ce site, suisse et francophone, vous propose de vous donner les bases et les moyens pour sécuriser votre machine fonctionnant sur un système Windows 32 bits. Vaste programme ! Sur le site, vous trouverez cinq rubriques principales. La première vous donnera, en tant qu'administrateur ou utilisateur, les principes de base pour utiliser votre machine de manière sécurisée et vérifier son intégrité. N'oublions pas que la première insécurité vient souvent d'une configuration par défaut ou d'une utilisation peu sérieuse de la machine ;) Vous pourrez aussi y découvrir les derniers bulletins sur les virus actuellement offensifs sur les systèmes Windows ainsi que des conseils pour vous en prémunir. Le site possède aussi des pages outils, patchs et spam, qui vous permettront de télécharger et d'installer les outils les plus efficaces pour sécuriser votre poste.

Winsec.epfl.ch est donc un site qui permet de faire rapidement un tour d'horizon de votre sécurité Windows en vous donnant les moyens de l'améliorer rapidement et efficacement.

LANGUE : Français

URL : <http://winsec.epfl.ch>



WINDOWS SECURITY

MSFT Security Support:
Christian Raemy
Tél: 32223 / mail

Windows @ EPFL

Procédure en cas d'infection / Disinfection procedure

Si vous êtes infectés par un virus, voici les quelques étapes communes à effectuer pour se désinfecter et se protéger au maximum d'une future attaque:
If you are infected by a virus, here is common steps for disinfect your computer and protect it against futures attack:

(Pour pouvoir effectuer la plus-part des points suivants, il est nécessaire de disposer des droits administrateurs sur votre machine, si ce n'est pas le cas, contactez votre administrateur informatique)
(For execute most of following steps, it is necessary to have administrators rights on your computer, if it is not the case, contact your administrator)

- Lancez **WindowsUpdate** pour contrôler les dernières mises à jour disponibles (patchs) et, le cas échéant, les installer automatiquement.
- Lancez **Stinger** pour contrôler et nettoyer votre machine.
- Installez le dernier anti-virus VirusScan 7.1 grâce à **MSU** ou si vous utilisez un autre produit, vérifiez que votre anti-virus soit à jour et planifiez les mises à jour automatiques.
- Vérifiez que les comptes locaux **administrateur** (ou **administrateur**) et **guest** possèdent bien un mot de passe et que ce dernier ne soit ni vide, ni trop simple (1234, admin, etc...) car beaucoup de virus rentrent dans votre machine comme cela.
- Launch **WindowsUpdate** to control the last updates available (patches) and, if necessary, to install them automatically.
- Launch **Stinger** to control and clean your machine.
- Install the last anti-virus VirusScan 7.1 by **MSU** or if you use another product, check your anti-virus is up to date and schedule automatic updates.
- Check the local administrator account (or administrator) and guest do not have a blank password or too simple as: 1234, admin, etc... because some virus use this way to infect your computer.

Pour certains virus, des actions supplémentaires sont peut-être nécessaires. Un article spécifique est dans ce cas disponible, il suffit de consulter la rubrique **Alertes Virus** à gauche.
For some virus, additional actions are perhaps necessary. In this case, specific article are available, please consult the heading **Alertes Virus** on the left.

Advanced Archive password recovery

Advanced Archive Password Recovery (ARCHPR) est le cracker de passes d'archives ZIP (PKZip, WinZip), ARJ/WinARJ, RAR/WinRAR et ACE/WinACE (1.x) le plus rapide au monde.

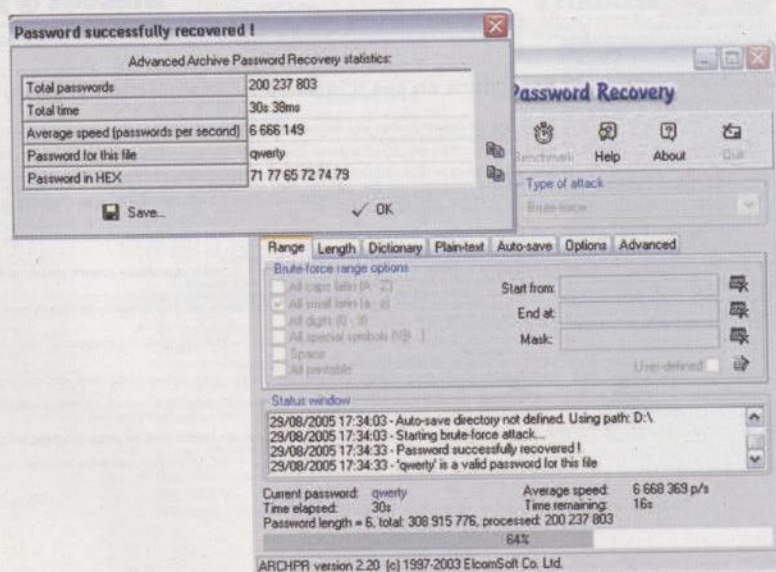
À ce jour, aucune méthode d'extraction du mot de passe directement depuis l'archive n'est possible, la méthode par brute force est donc la seule solution. L'utilisation d'un dictionnaire est également possible.

Sa rapidité est étonnante ! Ainsi, avec un processeur de 1Ghz, les tests ont révélé qu'ARCHPR pouvait tester jusqu'à 15 millions de possibilités à la seconde.

Notons également que les développeurs de ARCHPR ne se sont pas arrêtés au cracking d'archives mais ont aussi développé des crackers pour les documents offices, Outlook Express, Internet Explorer ainsi que pour de multiples messageries instantanées, Windows XP et j'en passe... Allez donc jeter un œil aux autres projets disponibles sur le site ;)

OS : Windows

URL : <http://www.elcomsoft.com>



Cmospwd

Le mot de passe du bios est souvent l'une des premières protections logicielles à laquelle un attaquant physique pourra avoir affaire. La majorité d'entre nous savons qu'il suffit simplement d'enlever la pile de la mémoire du bios pour la réinitialiser, donc supprimer toute protection au niveau du bios et ainsi faire sauter le mot de passe.

Cependant, il existe des méthodes plus subtiles qui consistent à réinitialiser ce mot de passe en interférant directement avec le bios.

Cmospwd est ici le logiciel qu'il nous faut car il permet en effet de cracker différentes marques de bios. Cmospwd permet de sauvegarder, de restaurer et d'effacer la cmos. Ainsi il est possible de récupérer, de restaurer et d'effacer le mot de passe du bios. La compatibilité du programme avec votre matériel n'est pas un problème puisque cmospwd est open source et que cela lui permet de bénéficier de nombreuses contributions afin de travailler sur de nombreux bios à partir de nombreux OS.

N'hésitez pas à lire le fichier README pour de plus amples informations sur ce soft !

OS : Dos, Windows, Linux, FreeBSD, NetBSD

URL : <http://www.cgsecurity.org>

```
firewall:~/cmospwd-4.6/src# ./cmospwd --help
CmosPwd - BIOS Cracker 4.6, February 2005, Copyright 1996-2005
GRENIER Christophe, grenier@cgsecurity.org
http://www.cgsecurity.org/

Usage: cmospwd [/k[de|fr]] [/d]
       cmospwd [/k[de|fr]] [/d] /{rlw} cmos_backup_file      restore/load/v
rite
       cmospwd /k                                           kill cmos
       cmospwd [/k[de|fr]] /m[01]*                          execute selected module

/kfr french AZERTY keyboard, /kde german QWERTY keyboard
/d to dump cmos
/m0010011 to execute module 3,6 and 7

NB: For Award BIOS, passwords are different than original, but work.
firewall:~/cmospwd-4.6/src#
```


John The Ripper

John the Ripper est le plus célèbre cracker de mots de passe. Il est développé par Solar Designer en licence GNU. Le plus rapide de sa catégorie, il permet d'auditer la sécurité de vos passwords et leur résistance à une attaque par brute force. Conçu à l'origine pour les mots de passe Unix, la dernière version (1.6) supporte de nombreux types de hachage, ce qui en fait un outil complet pour tout type de plate-forme : *NIX, DOS, Win32, BeOS et OpenVMS. S'il peut paraître un peu rebutant aux newbies par sa prise en main en ligne de commande, il suffit pourtant d'un peu d'entraînement et de lecture avec john --help pour découvrir toutes les possibilités de ce logiciel incontournable dans le monde de la sécurité informatique.

OS : *NIX, DOS, Win32, BeOS, OpenVMS

URL : www.openwall.com/john/

```

C:\WINDOWS\system32\cmd.exe
C:\unzipped\john-16u\john-16u\run>john.exe

John the Ripper Version 1.6 Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]
-singl                    "single crack" mode
-wordfile:FILE -stdin    wordlist mode, read words from FILE or stdin
-rules                    enable rules for wordlist mode
-incremental[:MODE]      incremental mode [using section MODE]
-external[:MODE]         external mode or word filter
-stdout[:LENGTH]         no cracking, just write words to stdout
-restore[:FILE]          restore an interrupted session [from FILE]
-session:FILE            set session file name to FILE
-status[:FILE]           print status of a session [from FILE]
-makechars:FILE          make a charset, FILE will be overwritten
-show                    show cracked passwords
-test                    perform a benchmark
-users:[-]LOGIN:UID[...] load this (these) user(s) only
-groups:[-]GID[...]     load users of this (these) group(s) only
-shells:[-]SHELL[...]  load users with this (these) shell(s) only
-salts:[-]COUNT        load salts with at least COUNT passwords only
-format:NAME            force ciphertext format NAME (DES/BSDI/MDS/BF/AFS/LM)
-savenem:LEVEL          enable memory saving, at LEVEL 1..3

C:\unzipped\john-16u\john-16u\run>

```

Mdcrack

Nous voilà face au cracker de MD5 considéré comme étant le plus puissant en la matière : MDCrack. Les MD5 servent surtout à vérifier l'intégralité d'un fichier. En effet, le MD5 a la particularité de ne pouvoir se décrypter, il n'y a donc pas de calcul inverse pour retrouver la chaîne de caractères originale.

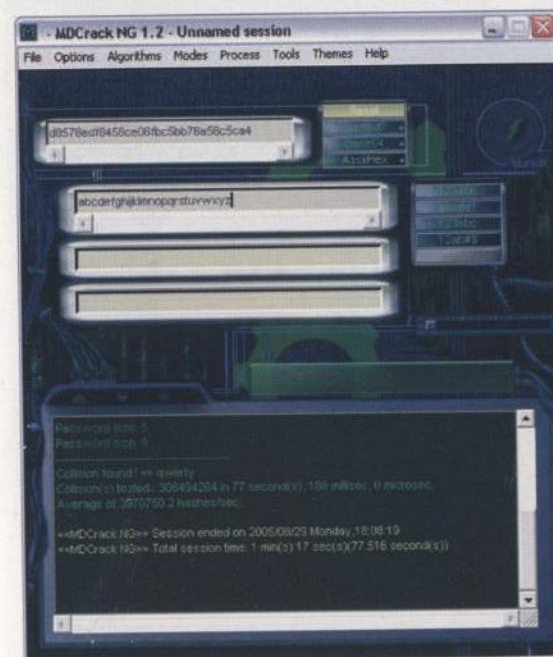
Il est également beaucoup utilisé dans les bases de données pour stocker les mots de passe. Cela s'applique par exemple aux forums qui utilisent cette méthode pour authentifier les utilisateurs. Lorsque vous voudrez vous authentifier, le forum comparera la signature MD5 du mot de passe que vous venez de lui fournir avec la signature MD5 du passe que vous avez choisi lors de la création de votre compte. Si les deux hashes correspondent, le mot de passe est valide.

Ainsi, MDCrack procède de la même manière. Il compare les signatures de toutes les combinaisons de chaînes de caractères possibles avec la signature que vous voulez cracker.

MDCrack est donc un bon soft, mais ne vous réjouissez pas trop vite, cela peut prendre du temps...

OS : Windows, Unix

URL : <http://c3rb3r.openwall.net/mdcrack/>



passcracking.com (md5 online cracking)

Vous avez un hash à cracker ? Passcracking.com pourra vous être d'une aide précieuse. En effet, passcracking.com vous propose de cracker vos hashes en un temps record ! Loin d'avoir des machines surpuissantes, le site dispose d'une énorme base de données de hashes, appelée Rainbow tables.

Comme dit sur le site, la méthode de cracking est basée sur la technologie du RainbowCrack (<http://www.antsight.com/zsl/rainbowcrack/>) en disposant de 80 tables de 610 Mo chacune, soit l'équivalent d'environ de 48 Go !

Outre son aspect pratique, ce site permet de se pencher davantage sur l'utilisation des Rainbow tables pour comprendre davantage leur fonctionnement. Je vous invite à lire la Surf Session du The Hackademy n°17 où dvrasp nous explique brièvement et clairement tout cela. Un site donc à la fois utile et éducatif ! À visiter :)

LANGUE : Anglais

URL : <http://passcracking.com/>

MD5 Online Cracking

using Rainbow Tables

[\[Add hash\]](#) [\[View results\]](#) (*empty field means - not found)

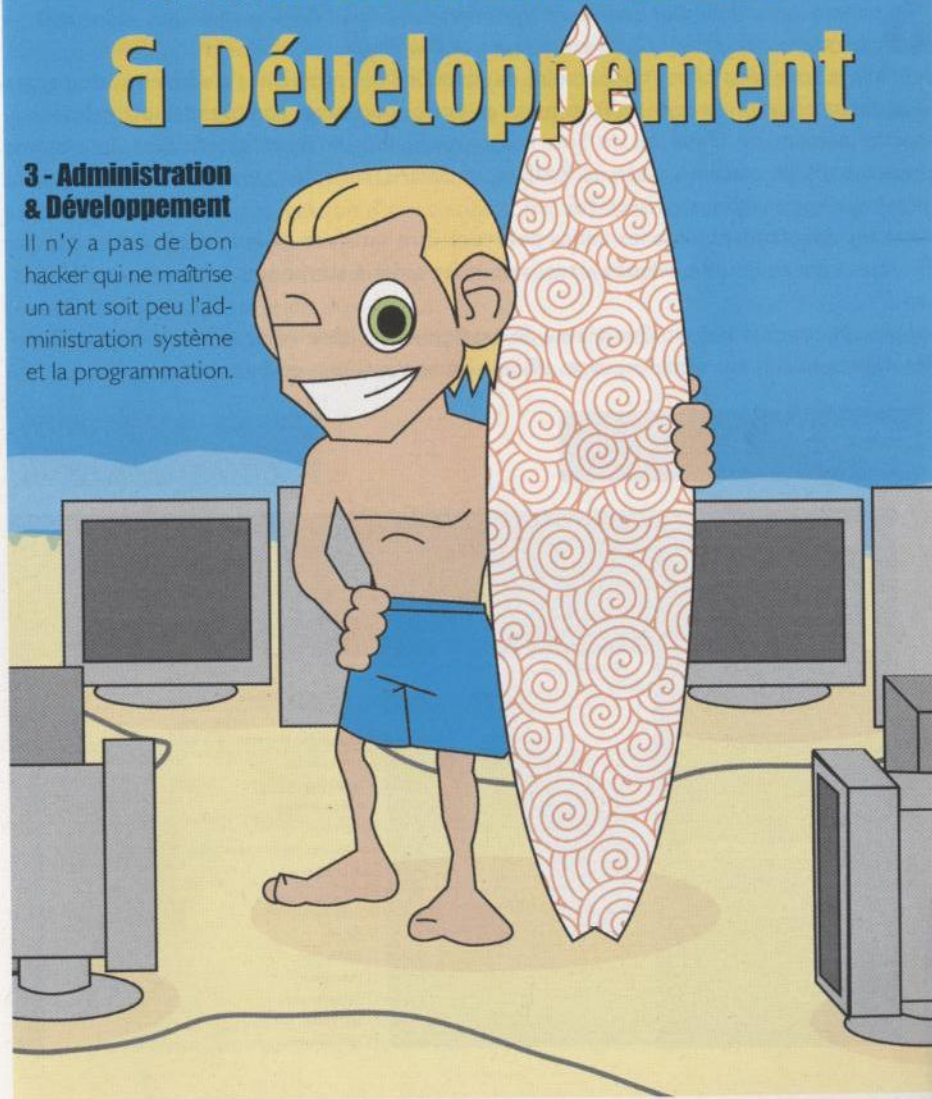
[NEWS]

- Any company or individual who would like to purchase this project (website, domain, tables, 30 000 results archive etc.) drop a line to info [at] passcracking.com.
- Table benchmark tests:
 - 10 hashes on P4, 2GHz, 512 RAM - all hashes are found ~73 minutes (1,2 hours) [\[results\]](#)
 - 10 hashes on P4, 2GHz, 512 RAM - no hashes are found ~446 minutes (7,4 hours) [\[results\]](#)
- Added two frequently asked questions with answers - about distributed variant of the project and about public availability of the Rainbow tables. See below.
- Going at full speed (~115 hashes / 24 hours).
- This project has been [hashidotted](#) - so the waiting line to crack hashes has increased rapidly.

Administrateur & Développement

3 - Administration & Développement

Il n'y a pas de bon hacker qui ne maîtrise un tant soit peu l'administration système et la programmation.



Admin-sys

« Site d'aide à l'administration, pour les administrateurs et toutes les personnes qui souhaitent en savoir plus sur leurs systèmes UNIX, LINUX », tels sont les mots qui ouvrent le site et qui résument bien sa raison d'être.

Admin-sys.com vous offre l'opportunité de résoudre vos problèmes d'administration grâce à sa documentation complète. Vous pourrez donc apprendre, comprendre et maîtriser le fonctionnement de Linux ou de Solaris. Par exemple : les bases essentielles du système Unix, mettre en place un système RAID sous Solaris, faire des sauvegardes sous hpux, et même quelques notions de sécurité.

Ainsi, les débutants comme les initiés pourront être satisfaits de leur visite sur ce site car ils trouveront toujours quelques astuces pour les aider à surmonter leurs petites défailances...

Admin-sys.com est le fruit d'un travail de passionné qui désire offrir au monde les ressources nécessaires à une administration efficace de son système et de son réseau.

LANGUE : Français

URL : <http://www.admin-sys.com>

FreeEOS

FreeEOS est une solution basée sous Gnu/Linux qui va vous permettre d'héberger facilement et rapidement les services internet dont vous aurez besoin. L'installation est des plus enfantines. Une fois installé, FreeEOS vous permettra de partager votre connexion internet entre plusieurs machines, de les protéger grâce à son firewall automatisé, d'héberger vos sites, emails et messageries instantanées ou de gérer un domaine, que ce soit pour des stations sous GNU/Linux, MacOS ou Windows.

Vous pourrez également profiter de nombreuses applications dynamiques (comme des forums, galeries de photos, gestion d'association, CMS et bien d'autres), partager des imprimantes et bien plus encore...

Toute l'administration peut s'effectuer simplement via une interface web accessible directement depuis votre poste de travail.

Bref, FreeEOS est la solution à tous les administrateurs débutant comme confirmés n'ayant pas le temps (ou la motivation ;) de s'adonner à la configuration manuelle de leur serveur !

URL : <http://free-eos.org/>

OS et logiciels libres

Gcu Squad

AVIS AUX AMATEURS D'UNIX EN TOUT GENRE !

Nous n'aurions pu envisager une partie Unix sans parler du célèbre gcu-squad !

En effet, ce site est une des références dans le monde Unix. C'est dans une atmosphère sombre et originale que vous pourrez vous mettre au courant des dernières news et apprendre à administrer votre poste de travail comme votre serveur. Tout cela en mode console bien sûr ;)

La diversité des sujets est grande. Vous pourrez par exemple y apprendre à sécuriser votre Unix, recompiler votre kernel OpenBSD, crypter votre swap, monter un firewall sous linux ou BSD, accélérer le système de fichiers de NetBSD (qui a tendance à être un peu lent à la base) et j'en passe...

N'hésitez pas à faire un tour sur leur canal IRC ([#gcu](http://irc.freenode.com)), ça peut toujours aider ! Bref, gcu-squad a de quoi vous scotcher à votre écran pendant de longues et belles heures !

LANGUE : Français

URL : <http://www.gcu-squad.org>

Kernelnewbies

Kernelnewbies est, comme son nom l'indique, un site dédié aux débutants voulant s'initier à cette chose extraordinaire qu'est le kernel linux. On peut y trouver de nombreux tutoriaux explicatifs et un glossaire très complet permettant d'obtenir une définition exhaustive des principaux éléments relatifs au kernel.

De plus, une FAQ est mise à la disposition des usagers pour répondre de façon claire aux questions que peuvent se poser beaucoup de gens sur le fonctionnement du noyau de leur Linux adoré. Un channel IRC est aussi disponible sur le serveur irc.kernelnewbies.org, salon #kernelnewbies, où tout un tas de passionnés se feront une joie de répondre à vos questions. Je pense qu'il s'agit du point de départ indispensable pour toute personne désireuse d'explorer le fonctionnement du kernel linux. Ce site est vraiment celui d'une communauté de gens qui s'entraident.

Une seule chose à dire : adeptes des organes du pingouin, n'hésitez plus ;) ce site est pour vous.

LANGUE : Anglais

URL : <http://www.kernelnewbies.org>

Labo Linux

LE LABO LINUX EST L'UN DES LABOS DE L'ÉCOLE D'INFORMATIQUE SUPINFO.

Une fois arrivé sur la page d'accueil, on a déjà une vue d'ensemble du site. L'interface permet de se repérer facilement. Un système d'icônes différencie les types d'articles, de news ou de tips. On peut également trier les documents du site par type, date ou popularité. Les dernières news, les derniers articles comme les plus populaires ou même le dernier kernel disponible sont visibles en un coup d'œil ! Ceci donne un ensemble convivial, simple et pratique. Par ailleurs, il faut noter que les concepteurs ont fait des efforts pour toucher un large éventail d'utilisateurs. L'ensemble est classé selon les compétences de chacun pour permettre une compréhension aisée des articles. Ainsi les débutants pourront comprendre facilement les informations présentes sur le site.

Nous soulignerons enfin que tous le labo linux est régulièrement en mouvement et la rubrique news est actualisée quotidiennement.

LANGUE : Français

URL : <http://www.labo-linux.org>

Linux Entre Amis (Léa)

Comme il se définit lui-même « le site d'aide Linux francophone », Linux Entre Amis (Léa) est une référence pour tous les utilisateurs francophones de Linux qui souhaitent obtenir une aide en ligne sur un problème précis. Ce site est l'un de mes préférés en la matière. Il possède une base de données d'articles qui s'enrichit continuellement pour vous offrir la solution à votre problème. Parmi les nombreuses rubriques qui composent ce site, vous pourrez trouver de nombreux conseils et astuces dans les domaines aussi variés que les réseaux, X-Window, l'administration de votre poste, le noyau et j'en passe. Vous pourrez également apprendre à vous servir de vieux minitel comme terminal ! Bref, de quoi vous scotcher à votre écran et votre console un bon bout de temps. Mais Léa, c'est aussi la possibilité de télécharger au format PDF l'ensemble des informations disponibles sur le site pour une consultation hors-ligne. C'est un geste très appréciable de la part des concepteurs du site. À consulter sans modération !

LANGUE : Français

URL : <http://www.lea-linux.org>



Léa-Linux.org

PDF de tous les articles de la section

© 2002, Frédéric Bonnaud
dernière modification le 16/12/2002.

Pages connexes

Léa-Linux.org >>

- » Découvrir Linux
- » Fiches pratiques
- » Forum
- » Trucs & astuces
- » Contacts
- » Carte du site
- » Liste d'aide
- » Confidentialité
- » Plus de rubriques...

Rubriques >>

- » Installation
- » X Window
- » Matériel
- » Logiciels
- » Le réseau
- » Administrer
- » Noyau et modules
- » Développer
- » Léavancé

Léa pour les pros ! >>

Cette section contient les chapitres relatifs à une utilisation professionnelle de Linux.

Plans des articles >>

Sous-sections :

- Administration Système
- Administration réseau
- Applications

Koders.com

AVIS AUX ACCROS DE LA PROGRAMMATION ! NOUS AVONS DÉNICHÉ POUR VOUS UNE VÉRITABLE MINE D'OR !

Koders.com est le plus grand moteur de recherche de codes source au monde. Il répertorie environ 200 millions de lignes de code en 30 langages différents !

Son utilisation est des plus simples. Vous entrez un ou plusieurs mots clé, vous choisissez le langage et la licence sous laquelle vous voulez faire apparaître les codes. Vous validez, et hop ! Des dizaines, voire des centaines de fichiers sources différents apparaissent sous vos yeux. À vous de faire votre choix !

Quel intérêt d'avoir un tel site sous la main ? C'est simple, vous pourrez par exemple mieux comprendre l'utilisation d'une fonction mal documentée, ou voir comment s'utilise une bibliothèque dans différents langages. Il y a quelques jours, il m'a par exemple été d'une aide précieuse lorsque j'ai voulu comprendre de quelle manière je pouvais coder mon petit bot IRC.

Amateurs de programmation, koders.com est donc un site qui rentrera dans vos favoris et dont vous ne pourrez plus vous passer.

LANGUE : Français

URL : <http://www.koders.com>

The screenshot shows the search results for 'socket.c' on Koders.com. The search bar at the top contains 'socket' and 'Filter: C' and 'GPL'. The results show a file named 'socket.c' with the following details:

- Project Info: Camserv(cserv), Server: SourceForge, Type: cvs
- download License: GPL
- Copyright: (C) 1999-2002 Jon Travis (jtravis@p00p.org)
- LOC: 177

The file content is displayed in a code editor window, showing the beginning of the 'canserv' application source code, including comments and license information.

Phpsecure

PHP Secure est un site très riche, au design sympathique, qui ravira à merveille toutes les personnes sensibles à la programmation PHP et à la sécurité de leurs codes. Très complet et assez astucieux, il vous rendra de précieux services.

Le site comporte plusieurs points intéressants que nous allons mettre en avant.

D'abord la partie news qui permet de se tenir informé des dernières nouveautés et vulnérabilités PHP.

Ensuite, le site propose une dizaine d'articles relatifs à la sécurité PHP. Il est vrai qu'une dizaine d'articles, ça peut paraître un peu léger pour un tel site mais le contenu est de qualité !

De plus, vous aurez la possibilité de télécharger des scripts, des patches ou des outils afin de rendre votre code plus sécurisé.

Nous terminerons sur un des points majeurs de ce site. En effet, si vous le souhaitez, vous aurez la possibilité de proposer une news ou même un patch pour le site.

Et oui, c'est grâce à ses contributeurs que le site est, aujourd'hui, devenu une référence.

LANGUE : Français, Anglais, Russe

URL : <http://www.phpsecure.info>

The screenshot shows the phpsecure() website interface. The main content area displays a list of security vulnerabilities under the heading 'Last trous'. The list includes:

- phpAdsNew SQL Injection and Command Execution Vulnerabilities (8hits) - 200
- CPAINT Ajax Toolkit Remote Command Execution Vulnerabilities (5hits) - 200
- phpPgAds SQL Injection and Command Execution Vulnerabilities (2hits) - 200
- Vuln: PHTB Topic Board Multiple Remote File Include Vulnerabilities (3hits) - 200
- Vuln: Mediabox404 Login_Admin_Mediabox404.PHP SQL Injection Vulnerability (3hits) - 200
- Vuln: PHPFreeNews Multiple Cross-Site Scripting Vulnerabilities (4hits) - 200
- eGroupWare XML-RPC for PHP Nested Tags Remote Code Execution (5hits) - 200
- ECW-Shop SQL Injection and Cross Site Scripting Vulnerabilities (5hits) - 200
- phpWebSite "module" Parameter Remote SQL Injection Vulnerability (4hits) - 200
- phpWebSite Input Validation Hole in "Module" Parameter Permits SQL Injection (4hits) - 200
- MiniBB Include File Bug in "includeFooter" Lets Remote Users - 200

The left sidebar contains navigation links for 'News du site', 'News du web', 'Archives des news', 'PHP', 'Advisories', 'Backends', 'RSS', 'Forum', 'Liens', 'Whois', 'Articles', 'Patches', and 'Scripts'.

Developpez.com

La programmation est de nos jours l'une des bases indispensables de l'apprentissage de l'informatique. Nombreux d'entre vous sont ceux qui demandent, sur IRC ou sur les forums, de l'aide sur telle ou telle fonction ou le plus souvent même pour savoir par quel langage de programmation débiter.

La majorité des réponses, c'est ici que vous pourrez les trouver ! Developpez.com est l'un des sites de référence francophone pour les amateurs de programmation en tout genre.

Le site passe en revue près d'une vingtaine de langages, à commencer par le C, le C++ en passant par le PHP ou même le Java.

Pour chaque langage vous est proposée de l'aide grâce à des tutos clairs et précis ainsi qu'à un forum très actif où l'ambiance est conviviale. De plus, pour ceux qui préfèrent les livres à l'écran, le site indique pour chaque langage quelques ouvrages qui vous aideront dans votre apprentissage.

Bref, un concentré de points positifs qui feront la joie de certains !

LANGUE : Français

URL : <http://www.developpez.com>

Developpez.com
Club des Développeurs

Rechercher: Go

sur developpez.com sur les forums

Forums | Tutoriels | F.A.Q's | Participez | Hébergement | Contacts

Club Blogs Dév. Web PHP XML XMLRAD Autres Systèmes Windows Linux
Accueil Java DotNET Visual Basic C & C++ Delphi Pascal Access SQL & SGBD Oracle UML

FORUMS C/C++ LES FAQS TUTORIELS LIVRES C/C++ COMPILATEURS SOURCES BCB

Les meilleurs cours, tutoriels, livres électroniques et Docs sur
C, C++, C++Builder, Borland C++ Compiler, Borland C++, Visual C++, Gcc
à consulter ou à télécharger sur le Web

Mis à jour le 27/04/2005

Langage C			
Le cours langage C	PDF 579 Ko	Cours sur le C très bien fait. Les exemples sont réalisés en Borland Turbo C 2.0 , un compilateur téléchargeable gratuitement (téléchargez plutôt Turbo C++ , plus récent et qui compile aussi le C). La mise à jour du 12/09/00 inclus de nouveaux cours de niveau 2 avec : Pointeurs et fonctions, tableaux et chaînes de caractères, le Graphisme, et enfin fichiers et structures.	Eric Berthomier
Le Langage C	PDF 317	Le Langage C par l'exemple, 55 pages. Cours de programmation C qui vous propose une première approche d'un programme en langage C, les règles générales concernant l'écriture d'un programme et l'organisation du	Jean-Michel Bouchard

RATS

Quel programmeur n'a jamais rêvé d'un outil qui audite son code à la recherche de failles de sécurité ou de buffer overflow ? Eh bien avec RATS, c'est aujourd'hui une réalité ! Ce logiciel est développé et maintenu par les ingénieurs de sécurité de Secure Software. RATS est un outil qui permet de scanner son code C, C++, Perl, PHP ou Python à la recherche des erreurs de programmation qui pourraient poser des problèmes de sécurité. Il permet par exemple d'identifier rapidement les appels de fonctions potentiellement dangereux et exécute également une analyse de base pour essayer d'éliminer les conditions qui ne sont pas forcément des problèmes à l'origine mais peuvent le devenir dans une utilisation détournée du programme audité. De plus, le logiciel donne, si possible, les modifications à apporter pour régler le problème.

Bien évidemment, même s'il permet de voir rapidement les problèmes rencontrés le plus fréquemment dans les codes sources, vous ne devriez pas exclure de faire ce travail vous-même. Et n'oubliez pas de le tester comme pourrait le faire un hacker. Couplé à votre bon sens, RATS deviendra alors un outils indispensable.

OS : Linux, Windows

URL : <http://www.securesoftware.com>

```
nitryx@hzy:~$ rats --help
RATS v2.0 - Rough Auditing Tool for Security
Copyright 2001, 2002 Secure Software Inc
http://www.securesoftware.com

usage: rats [-adhilrwxR] [--help] [--database|--db] name1 name2
-a <fun>      report any occurrence of function 'fun' in t
-d <filename> specify an alternate vulnerability database
--db          --db
--database    --database
-h            display usage information (what you're read
--help       --help
-i           report functions that accept external input
--input      --input
-l <language> force the specified language to be used
--language <language>
-r           include references that are not function ca
--references --references
-w <1,2,3>   set warning level (default 2)
--warning <1,2,3>
-x           do not load default databases
-R          don't recurse subdirectories scanning for m
--no-recursion
```

Firewall-net

Sur Internet, nombreux sont ceux qui recherchent de l'aide pour savoir quel firewall choisir. Réjouissez-vous ! Vous allez avoir entre les mains une véritable mine d'or ! En effet, firewall-net.com met à votre disposition une multitude de comparatifs. En fonction de votre configuration réseau, le site vous aidera à choisir le meilleur firewall à installer. Que vous soyez sous Windows, Mac ou Linux, vous serez servi ! Les firewalls sont testés scrupuleusement afin de vous offrir des comptes rendus précis. Le site affiche les résultats aux tests de sécurité, liste les avantages et inconvénients de chacun puis donne en conclusion une note générale. Bien entendu, après l'installation de votre nouveau firewall, vous pourrez utiliser l'outil "Scan Test" du site pour évaluer la sécurité de votre machine.

À noter : si votre esprit de curiosité est en éveil, vous remarquerez que ce site est également enrichi de quelques articles intéressants, notamment une introduction au fonctionnement des antivirus. Bonne visite !

LANGUE : Français, Anglais

URL : <http://www.firewall-net.com>

Comparer	Note /20	Prix €	Système								Ping	Net bus	TCP	UDP	Leak test
Firewall			95	98	ME	2000	NT	XP	Mac	Linux					
<input type="checkbox"/> Tous															
<input type="checkbox"/> Look'n'Stop	17.46	39	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓
<input type="checkbox"/> Kerio Personal Firewall	15.04	0	✗	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓
<input type="checkbox"/> Outpost Pro	14.732	40	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	1/2	✓	
<input type="checkbox"/> McAfee Desktop Firewall	13.776	40	✓	✓	✓	✓	✗	✓	✗	✗	✓	1/2	✓	✓	
<input type="checkbox"/> Xelios Personal Firewall	12.772	35	✓	✓	✓	✓	-	✓	✗	✗	✓	✓	✗	-	
<input type="checkbox"/> Zonealarm Pro	10.92	60	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	
<input type="checkbox"/> Norton Personal Firewall	10.072	60	✗	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	

Smoothwall

Smoothwall est une mini distribution linux destinée à transformer votre vieux Pentium en véritable firewall/routeur. Ce dernier va vous permettre de protéger votre réseau des milliers d'intrus qui rôdent sur la toile.

L'installation ne prend que quelques minutes ! La configuration de votre nouveau firewall se révèle très simple grâce à son un panneau d'administration convivial (cf. capture). Ajoutons également que vous aurez la possibilité de créer plusieurs zones, par exemple une pour la DMZ et une pour le réseau local. Alors, héberger un serveur web consultable depuis Internet devient une tâche enfantine.

Par ailleurs, Smoothwall est bien plus qu'un simple firewall. Il intègre également un serveur DHCP et un serveur proxy. Il comporte un IDS (snort). De plus, l'analyse des logs est facilitée grâce à une interface graphique.

Enfin, smoothwall vous prévient lorsqu'une mise à jour de sécurité est disponible.

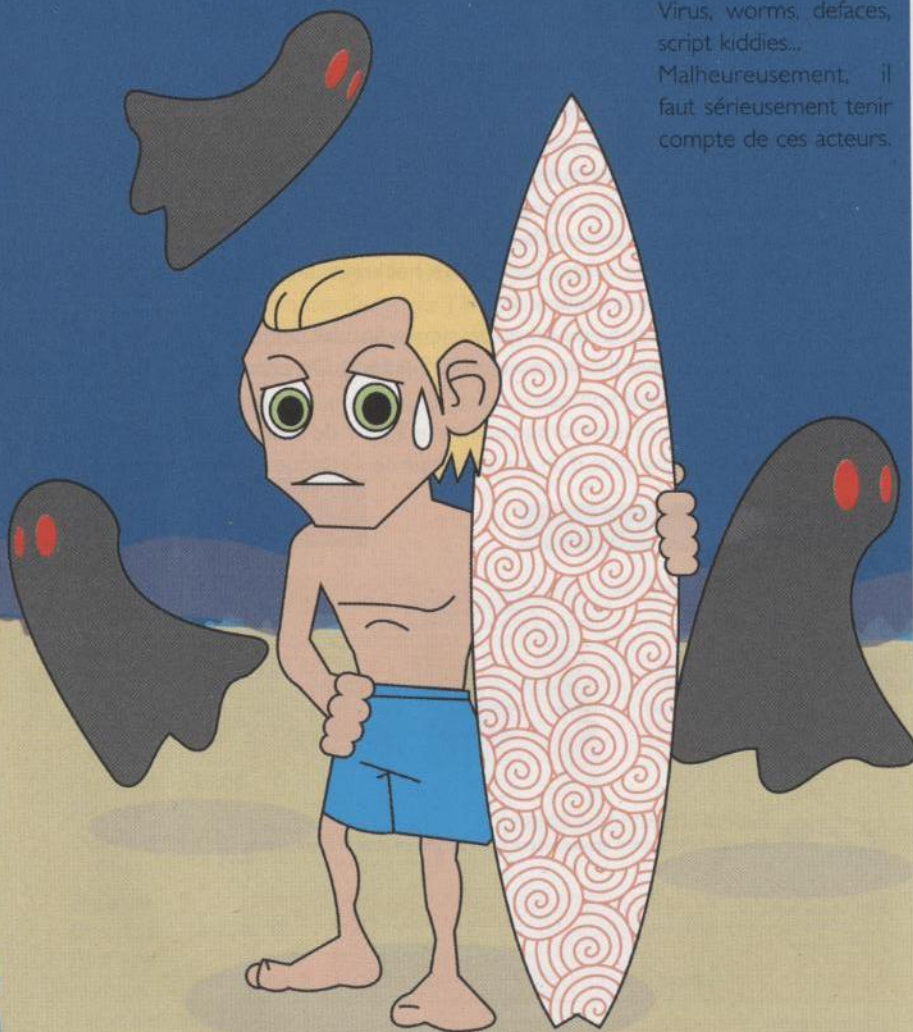
Voilà de quoi en dissuader plus d'un qui tenterait de s'attaquer à votre réseau !

URL : <http://www.smoothwall.org>

4 - The Dark Side

Virus, worms, defaces,
script kiddies...

Malheureusement, il
faut sérieusement tenir
compte de ces acteurs.



The Dark Side

62nds.co.nz

NE VOUS ÊTES VOUS JAMAIS DEMANDÉ QUELS ÉTAIENT LES SECRETS DES PLUS GRANDS VIRUS ?

La majeure partie d'entre vous nous répondra que si. Cependant, les seuls bouts de code que la plupart d'entre nous auraient pu étudier ont souvent été « arrangés » afin d'être inoffensifs. 62nds.co.nz nous propose ici les codes sources bruts et complets de ces virus qui ont fait couler pas mal d'encre dans la presse.

Citons par exemple le fameux virus Annakournikova, Melissa ou même I love you.

Bien sûr, lorsqu'on manipule ce genre de choses, il vaut mieux être prudent. Mais cela se révèle toujours formateur à un moment ou un autre.

En effet, on peut par exemple comprendre davantage les faiblesses d'un système tel que Windows face à un simple script VBS ou face à un petit code d'assembleur.

Enfin, outre les codes sources présents sur ce site, vous pourrez télécharger quelques outils plus ou moins intéressants.

Un site donc à manipuler avec précaution !

LANGUE : Anglais

URL : <http://62nds.co.nz>

Name	Last modified
Parent Directory	12-Apr-2005 19:50
beagle	12-Apr-2005 19:50
mydoom	22-Aug-2005 21:59
AnnaKournikova.txt	08-Sep-2004 02:48
cih.txt	08-Sep-2004 02:48
Code-Red-Worm.txt	08-Sep-2004 02:48
exploithtml.txt	31-Jul-2005 18:44
homepage.txt	08-Sep-2004 02:48
icecubes.asm.txt	08-Sep-2004 02:48
iloveyou.txt	08-Sep-2004 02:49
kak.txt	11-Sep-2004 18:18
kernel.dll.txt	11-Nov-2004 23:46
LIFE_STAGES.TXT	08-Sep-2004 02:49
MarkerC.txt	08-Sep-2004 02:49
mawanella.decoded.txt	08-Sep-2004 02:49
mawanella.vbs.txt	08-Sep-2004 02:49
melissa.txt	08-Sep-2004 02:49
ol_pdfworm.txt	08-Sep-2004 02:49
run_decoded.txt	08-Sep-2004 02:49
run_original.txt	08-Sep-2004 02:49
tune.txt	08-Sep-2004 02:49
v90atcom.pdf	08-Sep-2004 02:50
VBSWG-AQ.decoded.txt	08-Sep-2004 02:50
VBSWG-AQ.vbs.txt	08-Sep-2004 02:50

Zone-H

Ce site traitant de sécurité informatique est des plus complets. Il comprend en effet un nombre impressionnant de toolz (plus de 3500) classés par catégories, un chat IRC, des news et des astuces. En plus de cela, Zone-H offre un petit musée des sites piratés contenant des informations sur le type de système attaqué ainsi qu'un miroir du site défacé. Bien qu'il soit en Anglais par défaut, ce site est aussi disponible en Français. Il fournit en plus quelques statistiques liées à la sécurité informatique.

Zone-H est mis à jour de façon régulière et offre des informations claires et concises. Vous aurez la possibilité d'interagir sur ce site par le biais de son chat IRC ou de son forum où les discussions vont bon train sur des sujets aussi divers que les rumeurs sur les Odayz (fake or not ?), les nouvelles vulnérabilités ou plus généralement le hacking. Pour vous retrouver dans ce site, un module de recherche est à votre disposition. Un site des plus intéressants à visiter, pour le hacker comme pour le responsable sécurité.

LANGUE : Anglais, Français, Russe, Italien

URL : www.zone-h.org



zone-h
get from Jinx your zone-h t-shirt

LANGUAGE	STATISTIQUE DES HACKERS					
RECHERCHE	No Hacker	Piratage d'IP individuel	Piratage en masses	Total des sites pirates	Piratage de page persos	Classement
MENU PRINCIPAL	1. iskorpita	9511	66767	76278	9426	66852
Accueil	2. Fatal Error	8135	11626	19761	15143	4618
Infos from zone-h	3. Red Eye	4789	28504	33293	33002	291
Infos from the world	4. In4der	4384	29454	33838	33757	81
Astuces	5. TechTeam	4333	32033	36366	36353	13
Téléchargement	6. SPYKIDS	4266	11988	16254	15286	968
Zone-H works	7. root_system	4046	19221	23267	21039	2228
Digital attacks	8. hackbsd crew	3853	6473	10326	5267	5059
Site pirates/Archives des crimes	9. Infection group	3731	30326	34057	32480	1577
Site pirates/Archives des crimes *	10. Simiens	3631	32025	35656	35606	50
* Referencer un piratage	11. BloodBR	3262	16429	19691	19684	7
Stay tuned	12. IDN	3127	3324	6451	5128	1323
Inscription mailing-list	13. PcDefail	2909	3347	6256	568	5688
	14. nobodycoder	2690	1257	3947	939	3008
	15. c0d3r2	2646	1655	4301	3248	1053
	16. HACKJRSSR	2495	12711	15206	14515	691
	17. nEt*DEVIL	2405	2149	4554	2099	2455

MilwOrm.com

MilwOrm.com est une base de données intéressante d'exploits et de shellcodes en tout genre, mise à jour régulièrement afin de fournir des exploits pour les dernières versions d'applications vulnérables.

Ainsi le site fournit-il des exploits locaux, remotes pour des plates-formes aussi diverses que linux, Windows, novell, hp-ux, bsd et j'en passe. Il fournit également des exploits pour des applications telles que les services web comme les forums, php, etc.

De plus, les exploits sont parfois accompagnés d'explications sur leur fonctionnement afin de comprendre exactement comment ils marchent et le pourquoi de la faille.

Ceci se révèle utile afin de comprendre pourquoi certaines applications sont vulnérables et comment les corriger.

Un outil de recherche ainsi qu'un plugin firefox pour ceux qui le désirent se révèlent très pratiques pour trouver ce que l'on recherche très rapidement.

MilwOrm.com pourra donc permettre à chacun d'évaluer efficacement la sécurité de son système ou de ses applications, bien que son orientation générale soit plutôt blackhat.

LANGUE : Anglais

URL : <http://milw0rm.com>



home | exploits | platforms | shellcode | search | cracker

milw0rm.com

[remote]

DATE	DESCRIPTION	HITS	AV	
2005-09-01	SimpleHTTP <= 0.4.0 Multiple Remote Exploits	674	D	Ken...
2005-08-31	VBulletin <= 3.0.0 Accessible Database Backup Searcher (update 2)	1899	D	str0...
2005-08-31	DomoWare Mini Remote Control 4.0 < 4.0 (Client Agent) Remote Exploit	724	D	ljnd...
2005-08-30	Savant 3.1 Remote Buffer Overflow Exploit	905	D	bas...
2005-08-30	HP OpenView Network Node Manager <= 7.50 Remote Exploit	698	D	Lyn...
2005-08-29	Battlefield (BF-CG/BF-VCC/BF-ZCC) Login Bypass/Pass Stealer/DoS Exploit	902	D	Luig...
2005-08-25	Microsoft IIS 5.0 (500-100.asp) Server Name Spoof Exploit	3034	D	Lyn...
2005-08-25	MS Windows Plug-and-Play Service Remote Universal Exploit (Spanish fix)	1386	M,D	RoM...
2005-08-25	MS Windows Plug-and-Play Service Remote Universal Exploit (French fix)	678	M,D	Fabr...
2005-08-22	Elm < 2.5.8 (Expires Header) Remote Buffer Overflow Exploit	1357	D	c0nt...
2005-08-22	MySQLiBoard (MyBB) <= 1.00 RC4 SQL Injection Exploit	1044	D	Alph...
2005-08-19	Servlet <= 10 LPD Arbitrary File Delete Exploit (metasploit)	954	M,D	Opt...
2005-08-19	MS Internet Explorer COM Object's File Download Exploit (MS05-038)	3608	D	Zwel...