LINUX SCHOOL
Magazine

n°1
3,80 euros

hors série n°1 Mars-Avril 2008

Hors série

plus de 150 URL 100% underground

Tous les sites cachés des meilleurs hackers du monde

technique. culture. activisme

Sommaire

LINUX SCHOOL HS
est édité par LPN
15 rue Chevreul
94700 MAISONS-ALFORT
Représentant légal : O. André
Principaux associés : LPN
Rédacteur en chef : simon Ley

Conception Graphique : Luber
ISSN en cours
Numéro de commission paritaire en cours
Dépôt légal à parution
Directeur de publication : Olivier André
Imprimé en France par Rota Garonne
Z.A."Mestre-Marty" 47310 Estillac

TOUT DIRE

Les livres, les journaux sur la sécurité informatique ou le hacking ne représentent qu'une infime partie de la totalité de l'information disponible sur le sujet, notamment sur Internet. Pour les hackers comme pour les chercheurs ou professionnels, il est naturel de publier directement sur le Web, par confort d'une part, par culture aussi, mais d'autre part pour obtenir une visibilité maximale. S'ensuit une accumulation incroyable d'annonces de failles, de rapports, de présentations d'outils ou de techniques, d'essais, de documents scientifiques, pédagogiques ou techniques, écrit par des gens compétents comme par des amateurs plus ou moins sérieux. Comment s'y retrouver ?

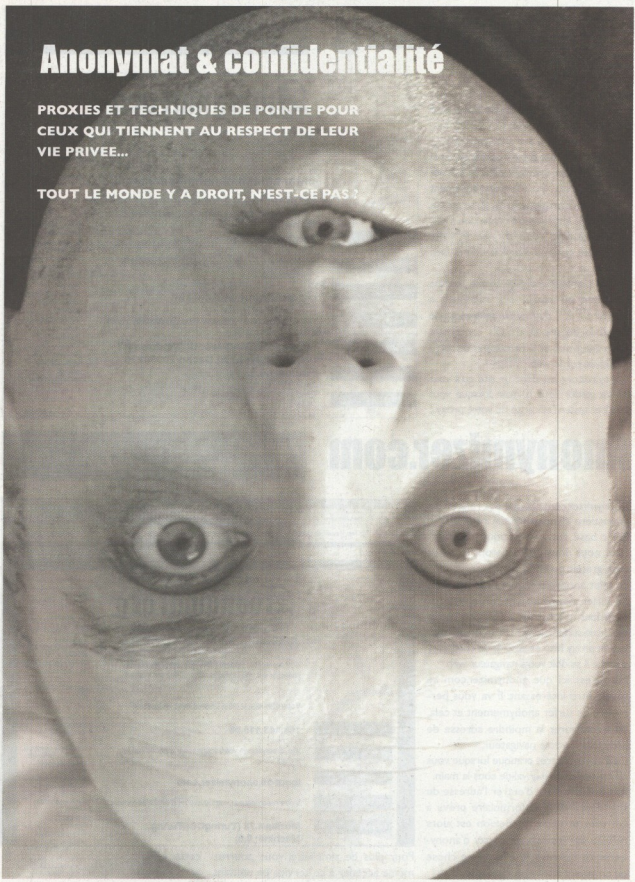
Linux school HS vous révèle… tous ces secrets.

...Sauf des bêtises

Anonymat & confidentialité

PROXIES ET TECHNIQUES DE POINTE POUR CEUX QUI TIENNENT AU RESPECT DE LEUR VIE PRIVEE...

TOUT LE MONDE Y A DROIT, N'EST-CE PAS ?



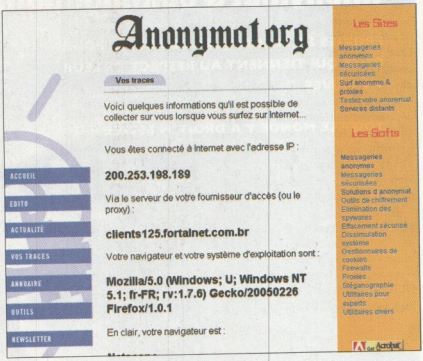
Anonymat.org

LANGUE : Français
URL : http://www.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 ! Vous pourrez alors grâce à ce site savoir si votre proxy est vraiment efficace. Le site vous renverras alors automatiquement toutes les informations qu'il a pu se procurer sur vous lors de votre connexion à leur 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 référence une multitude de site 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 !



Anonymizer.com

LANGUE : Anglais
URL : http://www.anonymizer.com

Anonymizer.com est une des références en matière d'anonymat sur internet.

Etant basé sur une optique commerciale, nous nous intéresseront ici qu'au coté gratuit du site.

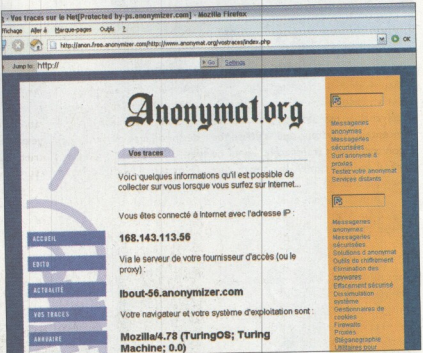
En effet anonymizer.com vous propose de surfer anonymement sur le web.

Rappelons qu'à la base, la méthode la plus simple de 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 être intéressant. Il va vous permettre de surfer anonymement et cela, sans configurer la moindre adresse de proxy dans votre navigateur.

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

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

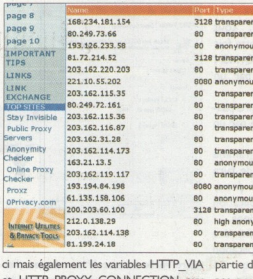


Pour plus de simplicité, vous pourrez même accéder à ce service en utilisant cette URL : http://anon.free.anonymizer.com/http://www.lesitedesire.com.

Proxy4free

LANGUE : Anglais
URL : http://www.proxy4free.com

On voit souvent sur des forums des personnes désespérées à la recherches de proxy valides et éfficaces.
Que ceux-la se réjouissent, proxy4free.com est l'une des plus grandes bases de données de proxy au monde. En effet ce site recense quotidiennement plusieurs milliers de proxy différents classés selon leur type (transparent, anonymous et high anonymity) et leur localisation.
Notons qu'on ne comprends 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 pas celle-ci mais également les variables HTTP_VIA et HTTP_PROXY_CONNECTION aux serveurs demandés par le client.
Malgré les mises à jours quotidiennes, une partie de la liste des proxy ne fonctionne pas, pour éviter de les tester un par un, aidez vous d'un testeur de proxy comme: http://www.checker.freeproxy.ru/checker/



Proxychains

OS : Linux
URL : http://proxylabs.netwu.com/proxychains

Qui a dit que les proxys ne servaient qu'aux navigateurs Web ? Le gros reproche que l'on peut faire à tous les outils d'anonymats actuel semble être leur manque de fonctionnalités et la difficulté de leur mise en place. Une solution excellente est Proxychains.
Proxychains est un programme au concepteur 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 proxys de votre choix. Les types de proxys supportés sont : http (connect), socks4 et socks5.
Etant donné qu'il intercepte toutes les fonctions de types sockets, aucune configuration des logiciels utilisés n'est nécessaire et ceux-ci sont tous compatibles. Ainsi, au lieu de taper :

```
ssh monordi.com
```

vous taperez :

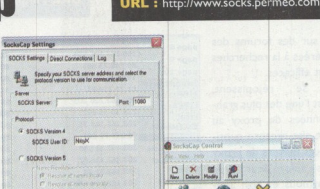
```
proxychains ssh monordi.com
```

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 proxys valides dans votre fichier de configuration et de spécifier le mode de chaînage parmi les 3 suivants : Random, Strict ou Dynamic. L'authentification sur les proxys est elle aussi gérée, et il vous suffira pour cela d'informer les champs utilisateurs et mot de pass 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 internets, 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 type Unix, à savoir Linux, BSD ou Solaris.

SocksCap

OS : Windows
URL : http://www.socks.permeo.com

Socksçap 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 sur 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 possibilité offertes par Sockscap n'ont de limite que celle de votre imagination !



Ars-cryptographica

LANGUE : français
URL:http://www.apprendre-en-ligne.net/crypto/menu/index.html

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 expliqués, 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'oublierons pas de souligner que des exercices pratiques vous permettrons 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.

Bmap

OS : Linux
URL : http://packetstormsecurity.org/linux/security/bmap-1.0.17.targz

Vous connaissez sûrement l'art de la steganographie qui consiste à dissimuler un fichier dans un autre. L'intérêt de cette méthode est 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 d'ajouter par exemple 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'ils ne leurs faut véritablement (du 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 :

```
/* Vérifions d'abord si quelqu'un a eu la même idée que nous, apparemment non, le slackspace est vide */
nitryx:~/bmap# bmap -checkslack exemple.gif
exemple.gif does not have slack

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

/* L'opération a fonctionnée */
nitryx:~/bmap# bmap -check-slack exemple.gif
exemple.gif has slack

/* On regarde maintenant le contenu du slackspace de 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:::
```

Burneye

OS : Linux
URL : http://www.packetstormsecurity.org/groups/teso/burneye-1.0.1-src.tar.bz2

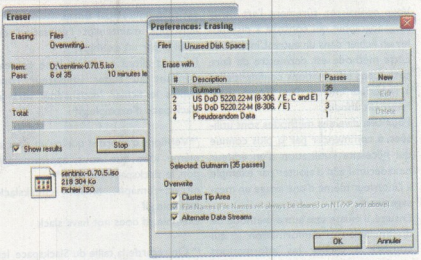
Garder ses binaires secrets n'est pas chose aisée. Cependant, afin d'assurer de la confidentialité d'un programme dont on ne souhaite dévoiler le fonctionnement, un outil formidable a été dévoilé par scut de la team Teso, il s'agit de burneye. En effet, burneye permet d'encrypter un exécutable au format ELF Linux sur machine Intel x86. Afin d'éviter les techniques dites de reversing, il offre plusieurs options telle que l'obfuscation rendant le code exécutable beaucoup plus difficile à débugger 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 on a oublié le mot de passe, attention à ne pas vous brûler les yeux ...

```
Matrix:/tmp/burneye-1.0.1/src# ./burneye
burneye - TESO 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

URL : http://www.tolvanen.com/eraser/
Taille : 2.7 MiB ● *Logiciel Libre*

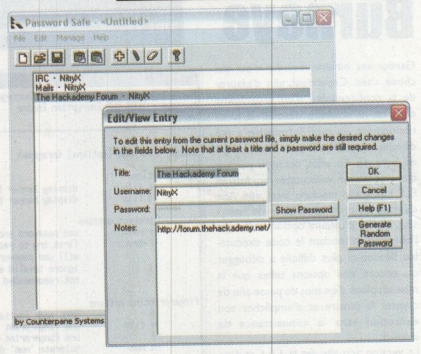
Ce programme s'est fait un nom dans le monde de la sécurité Windows. Il s'agit du meilleur outil de suppression sécurisée de fichiers.
Grâce à Eraser vous pouvez enfin supprimer efficacement vos données confidentielles. Vous savez, toutes celles que vous ne voulez absolument pas qu'un tiers puisse retrouver 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 défini 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 taches qui pourra vous permettre de supprimer automatiquement les fichiers contenus, par exemple, dans un répertoire temporaire.



Password Safe

OS : Windows 9x/2000/XP/CE
TAILLE : 172 KiB ● *Logiciel libre*
URL : http://www.schneier.com/passsafe.html

On a toujours besoin de retenir des tonnes et des tonnes de mot de passe : travail, forums, service en ligne, banques, comptes ftp, mail, etc.
Password Safe, permet en effet de palier ce problème en enregistrant de manière sûre vos 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 une de vos entrées pour que le mot de passe correspondant soit transféré directement dans le presse papier.
Passworf 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.semanticgap.com/mypwsafe/).

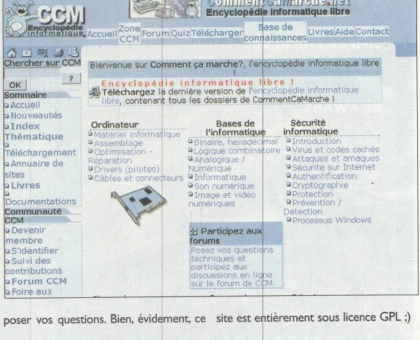



Hacking
SIMPLY THE BEST
DIGEST ON THE WEB
BE AWARE

Commentcamarche

LANGUE : Francais
URL : http://www.commentcamarche.net

Comment ça marche l'informatique ? Et, 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 sur l'informatique. Il y a de tout : architectures, systèmes d'exploitation, histoire, lois et droits, programmation WEB, bases de données, langages de progs, réseaux, sécurité. Bref, y en a pour tout le monde et surtout pour les néophytes de l'informatique.
Les documentations sont réalisées dans des formats divers : pdf, html, doc, etc. En plus, dans la partie télécharchement, vous pouvez downloader le site complet afin de le consulter offline (ce qui constitue une base d'information relativement complète sur votre disque dur). Un forum est aussi à votre disposition, où vous pourrez poser vos questions. Bien, évidement, ce site est entièrement sous licence GPL ;)



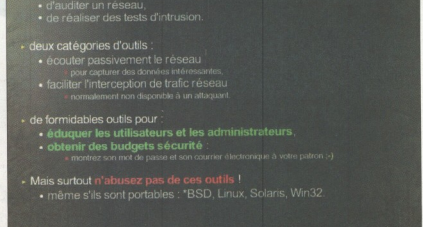
Dsniff

OS : Windows/Linux
URL : http:// naughty.monkey.org/~dugsong/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 mot de passe uniquement.
Dsniff c'est aussi une collection d'outils pour le réseau : dsniff, le filesnarf, le mailsnarf, le msgnarf, l'urlsnarf et webspy 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 concu 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.

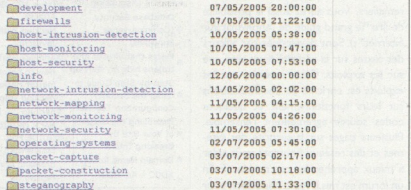


Vous l'auriez compris, la puissance de dsniff est telle que nous pouvons tout vous expliquer ici, le plus simple et toujours de tester par soi-même ;).

ftp.zedz.net

LANGUE : Anglais
URL : ftp://ftp.zedz.net

Il n'y a pas que les simples sites internet qui peuvent être très interessants sur le net. En effet, vous avez peut-être pu constater tout au longs de vos recherches que les ftp peuvent aussi être une source précieuse d'information.
ftp.zedz.net rentre parfaitement dans cette catégorie. Ce ftp regorge en outre une multitude de documents qui méritent le coup d'oeil.
Certes, certains date d'une dizaines d'années mais ils restent toujours aussi instructifs et intéressants.
Vous pourrez par éxemple 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 passes, 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 au savoir !

Google

URL : http://www.google.fr

Qui ne connaît pas le plus populaire des moteurs de recherche ? Personne, évidement. Et pourtant, êtes vous conscient des nombreuses possibilités offertes par ce site ?

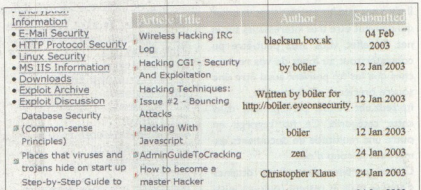
Lors d'une recherche vous pouvez spécifier des paramètres qui parfois pourront se révéler intéressants. Par exemple, essayez de taper, "allinurl: cmd.php", dans le champ de recherche ! En effet, cela vous renvoie sur un nombre impressionnant de pages possédant une adresse composée de cmd.php, qui comme 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'oeil dans les diverses options de recherche avancée ou même du coté 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

Government

LANGUE : Anglais
URL : http://Governmentsecurity.org

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 documentations sur leurs fonctionnement et quelques codes source agrémentent l'ensemble. Plusieurs pages sur la sécurité des sytèmes 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'offent à vous !

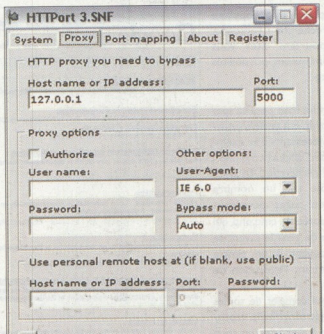


Governmentsecurity.org est un site en Anglais (Et oui, il faut donc maîtriser la langue), mais tout de même bien réalisé avec un contenu dynamique! Par exemple des icônes nous indiquent quels sont les articles les plus consultés de la semaine ainsi que les derniers publiés. Governmentsecurity.org est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

Httport

OS : Windows
URL : http://www.htthost.com

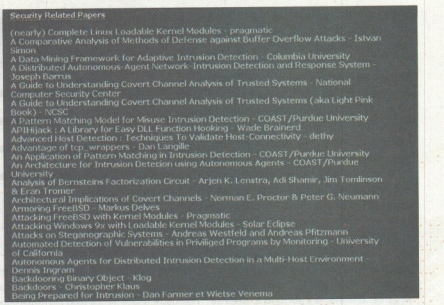
Quoi de plus énervant que d'avoir un accès à Internet mais pas la possibilité, par exemple, de discuter sur le forum de the Net secret's ? Pas de panique car nous avons la solution. HTTPort est un logiciel des plus utiles qui vous permettra de « bypasser » un proxy HTTP lorsque votre connexion à Internet est bridé. 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 Proxy relais. A ce sujets vous pouvez trouver ce type de service en cherchant sur google avec ses 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 leur 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 gourmant en mémoire et en ressources qui pourrait rendre service dans de nombreuses occasions.

Minithins

LANGUE : Anglais
URL : www.minithins.net



Minithins.net est un site au design plutôt simpliste mais qui cache en lui une véritable mine d'or. C'est en effet dans la rubrique Knowledge que l'on trouve la substantifique moelle du site. Cette rubrique référencie près de 250 liens ayant rapport soit à la programmation soit aux réseaux soit à la sécurité. Le choix des liens ont 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.

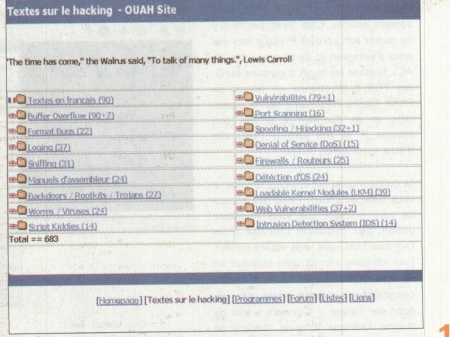
Dans cette même rubrique nous trouverons également des liens vers d'importants sites de sécurité, de team ou de repository.

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.

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

Ouah.org

LANGUE : français, anglais
URL : http://ouah.org



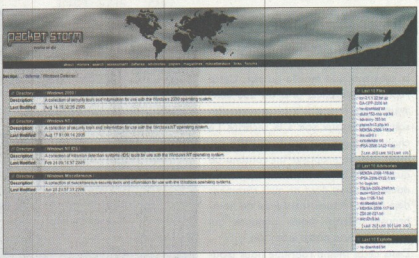
Ouah.org recense presque tous les meilleurs textes électroniques sur la sécurité informatique. C'est une mine d'information avec près de 700 textes sur le sujet, dont une centaine sont en français. Bien sûr, ceux-ci ont été soigneusement sélectionnés et classé par catégories et sont accompagnés d'une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

Les principaux thèmes abordés vont des différents types de vulnérabilités, aux techniques d'attaques, 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. A noter que ouah.org possède aussi une belle collection d'outils incontournables.

Packetstorm

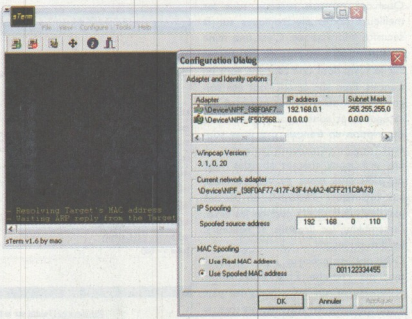
LANGUE : Anglais
URL : http://packetstormsecurity.org



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 privé, le site ne comporte aucun cookie (hormis pour le forum) et tous les logs et statistiques concernant votre visite sont renvoyées vers /dev/null.
Le contenu, quant à lui, ne devrait décevoir personne. Le site regroupe une quantité d'information faramineuse répartie dans quatre grandes catégories. « Assessment » qui regroupe entre autre la base de donnée 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 ensuite 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 bonne surprise. A la carte : programmation, virus, phreaking et même humour informatique.

Sterm

OS : Windows
URL : http://www.oxid.it/sterm.html



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 Poisonning 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 vore machine que vous souhaitez utiliser, puis choisissez l'adresse IP et l'adresse MAC que vous voulez simuler (ces adresses seront celle utilisées en sources de vos paquets lors de votre connexion au serveur cible) puis cliquer 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.

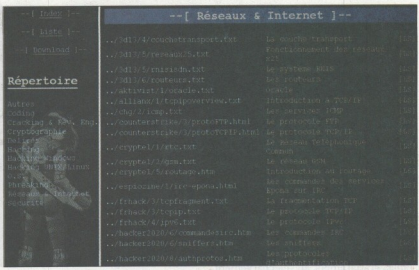
Frenchzines

LANGUE : Français
URL : http://www.frenchzines.tk

Frenchzines est un site regroupant plus de 800 e-zines francophones. Dans une athmosphère 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 se révèle avoir 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.

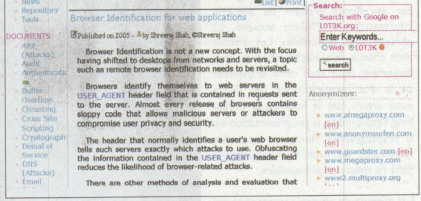


Les textes sont au format txt ou html, pour un plus grand confort de lecture et sont parfois agrémentés d'images pour offrir une meilleure compréhension. Très complet, nous qualifierons frenchzines.tk comme une des plus grandes bases de données de zines Francophone. A consulter!

L0t3k.org

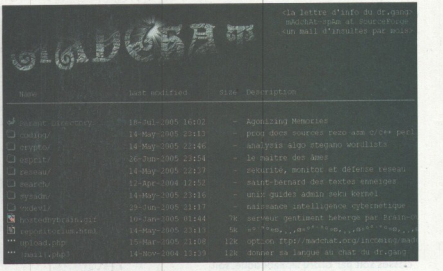
URL : http://www.l0t3k.org

Ho 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 tollz. Que rêvez de mieux ? La sécurité informatique exposée dans des couleurs roses 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 ...



Madchat

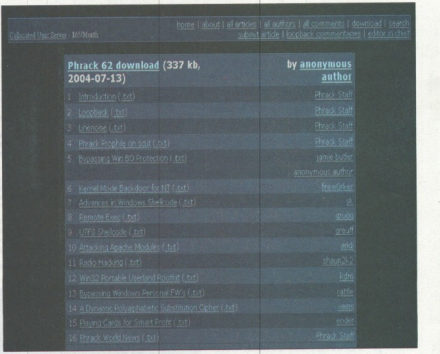
LANGUE : Français / Anglais
URL : http://www.madchat.org



Un site haut en couleurs et pourtant assez controversé. La revendication « anar » et libertaire y sont peut-être pour quelque chose. La censure n'est donc pas au 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 forcement 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. Parmis les rubriques les plus fournies, on trouve entre autre la sécurité admin et réseau pour les système Unix/Linux. Tout ce qu'il y a à savoir sur la crypto et son utilisation. Et pour es 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. A explorer dans tous les sens.

Phrack

LANGUE : Anglais
URL : http://www.phrack.org



Qui ne connaît pas le magazine de référence Phrack ? Le magazine 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. A l'heure actuelle, 62 phracks sont disponibles. Les articles sont chaque fois sélectionnés scrupuleusement, 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 mais la plupart des articles sont cependant 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 vrai de vrai hacker ! ;)

The Hackers Choice

LANGUE : Anglais
URL : http://www.thc.segfault.net/

Porteur d'un nom qui pourrais 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 désirant 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 ! Parmis eux, nous pouvons citer AMAP ou VMAP qui ont déjà eu dans le passé, droit à quelques lignes à travers diverses publications de The Net secret's.

A ne pas oublier également que le site comporte une partie /root qui serais 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'autre domaines encore. Vous aurez aussi la possibilité de visiter la partie /root/phun qui contient tout les documents … fun de la team ! :)

Frsirt

LANGUE : Francais
URL : http://www.frsirt.com

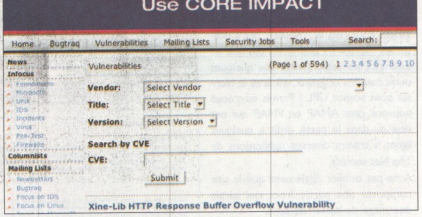
Trouver de l'information à jour sur la sécurité en français n'est pas évident. Frsirt.com (anciennement connu sous le nom de k-otik) est un site qui répond à ces critères puisqu'il est entièrement en français et totalement dédié à la sécurité informatique. Vous aurez la possibilité de consulter leur base de donnée 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, 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 récent en vous inscrivant à leur mailing liste. Ce site est donc une excellente alternative à Security Focus pour se tenir informer quotidiennement des différents exploits et advisories parus et tout ça en français. Bref, un site à bookmarker au plus vite.

Securityfocus

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

Securityfocus est tant pour le hacker que l'administrateur une source très précieuse d'informations. Malgré son coté 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 une base de données impressionnantes de vulnérabilités en lien avec la liste de diffusion BUGTRAQ. En effet cette liste de diffusion, à laquelle chacun d'entre nous devrait être abonné permet de se mettre au courant chaque jours des nouvelles vulnérabilités. L'inscription rapide est thématique, ainsi vous pourrez vous abonner, selon vos centres d'intérêt au 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 !



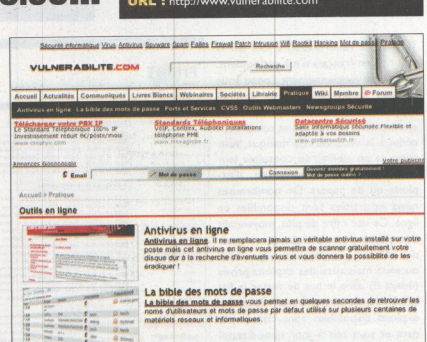
Au-delà du « coté base de vulnérabilité et liste de diffusion », Securityfocus dispose d'un nombre intéressant d'outils. Je vous invite donc à aller y jeter un coup d'œil. Vous l'aurez compris, Securityfocus est donc une référence en la matière ! A découvrir donc, ou à redécouvrir :).

Vulnerabilite.com

LANGUE : Francais
URL : http://www.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..

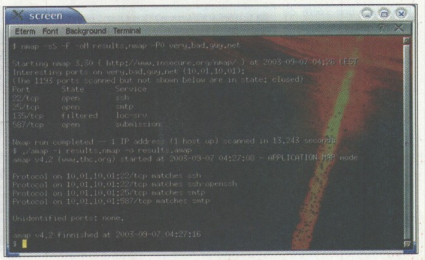
Vulnerabilite.com ne fait pas que livrer l'actualité, il fournit également des outils pour les professionnels tel qu'un annuaire des acteurs de la sécurité, une bible des mots de passe par défaut des constructeurs, une liste des services fonctionnant derrière chaque port d'un réseau, ou encore des solutions 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.



AMAP

OS : Linux
URL : http://thc.org.segfault.net/thc-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 (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'amusent rarement à modifier un numéro de port (surtout pour les services qu'ils ouvrent à Internet), mais

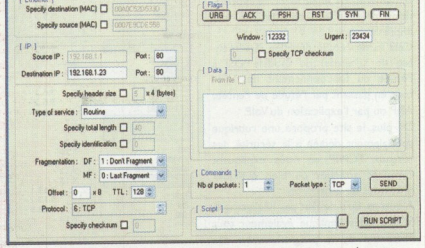


il arrive que l'on souhaite identifier le service tournant derrière un port élevé... AMAP fera cela très bien, très vite et très facilement !
Les protocoles supportés nécessitant un envoi sont : dns, ftp, http, jrmi, ldap, ms-ds, ms-remote-desktop-protocol, ms-sql, netbios-session, ntp, oracle-tns-listener, rpc, sap-r3, smtp, snmp-public, ssl et x-windows. En ajoutant les protocoles identifiables dès la connection, on obtient un total de 147 protocoles différents supportés !

Engage Packet Builder

OS : Windows
URL : http://www.engagesecurity.com

Engage Packet Builder (EPB) est un programme Windows, permettant de forger des 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.

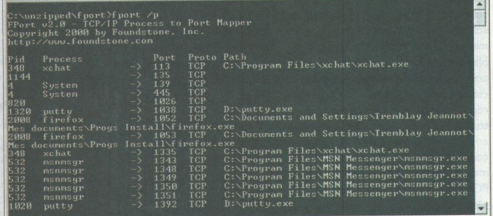


Reparlons un peu de sa gestion des scripts, EBP permet en effet la création de scripts personnalisés très puissants (scripts de connexions, de syn floods, etc.). Jetez un oeil aux exemples de scripts fournis avec le programme, ils détaillent toutes les commandes utilisables dans les scripts. Un programme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

Fport

OS : Windows NT4, 2k, XP
URL : http://www.foundstone.com/knowledge/proddesc/fport.html

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.

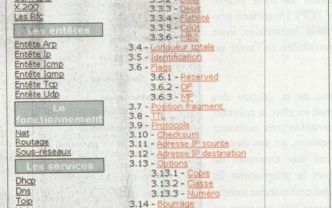


En connaissant son nom et le chemin complet de l'exécutable, il est plus facile de le repérer dans la base de registre, par exemple. On peut également déterminer facilement quels sont les services qui sont réellement activés. Utile pour les habitués de Linux, à qui la commande netstat –atp fait cruellement défaut sur Windows.

Frameip.com

LANGUE : Francais
URL : http://www.frameip.com

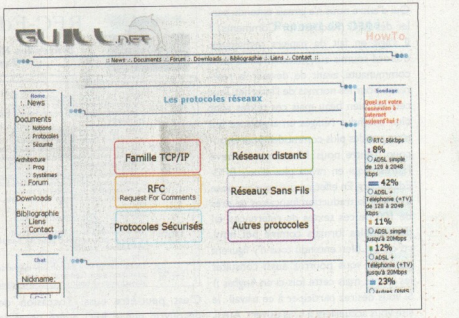
Frameip est un site dédié à la compréhension dans ses moindres recoins des protocoles de communications des réseaux. Au menu, TCP/IP, UDP, ARP, ICMP, IGMP et j'en passe…
Frameip est une véritable mine d'or en la matière! En effet, le tas d'informations présent sur ce site est très impressionnant !
Cela 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 le coté interactif du site, qui propose, en outre, un QCM afin de tester les connaissances que vous aurez acquises tout au long de votre visite sur le site ! :).



Guill.net

LANGUE : Français
URL : http://www.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 possède en plus de cela un 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 également que ce site comporte une rubrique bibliographie qui pourra guider l'achat de votre prochain livre de chevet ! ;)



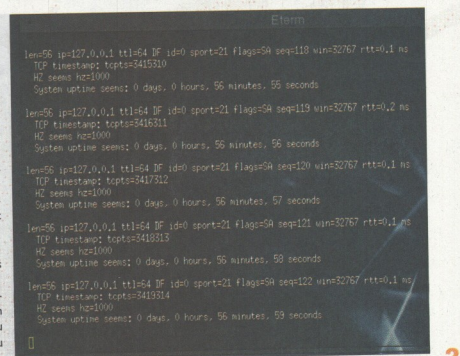
En bref, ce site est incontournable pour tous ceux qui s'intéressent de près ou de loin aux domaines informatiques que constituent les réseaux de communications.

Hping

OS : Unix
URL : http://www.hping.org

Peu d'entres 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 traffic TCP/IP.
Hping est un outil complet et peut par exemple servir à tester la sécurité de votre firewall, tester le fnctionnement de votre réseau, s'entrainer à l'OS fingerprinting, 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 est souvent intéressant de travailler avec un analyseur de trafic comme tcpdump ou ethereal. En effet lorsqu'on génére du traffic avec Hping il est impératif d'analyser les réactions du réseau ou du système cyble.



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

Rfc-editeur.org

LANGUE : Français
URL : http://rfc-editeur.org

Qui d'entre nous 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, mais cette fois-ci en Anglais ;)
Si vous désirez participer à ce travail , le site vous accueillera à bras ouvert. Aussi, vous pouvez consulter les textes en cours de traduction.

C'est peut-être aussi l'occasion de découvrir quelle RFC a été posté 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'autre projets similaires.

Nmap

OS : Unix, Windows
URL : www.insecure.org

Qui ne connais pas Nmap ? Entre nous, peu de monde. Cependant, pour les quelques uns qui découvrent ce soft 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 est 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 IP1,IP2,ME,IP3
–P0 IPCIBLE
```

Ainsi, la cible (ici IPCIBLE) aura l'impression de s'être fait scanné à la fois par IP1,2,3 et nous.

```
firewall:~/p0f# ./p0f -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)
192.168.0.1:1403 - 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
  -> 212.27.33.225:80 (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
```

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 !

POf

OS : *BSD, Linux, Windows
URL : http://lcamtuf.coredump.cx/p0f.shtml

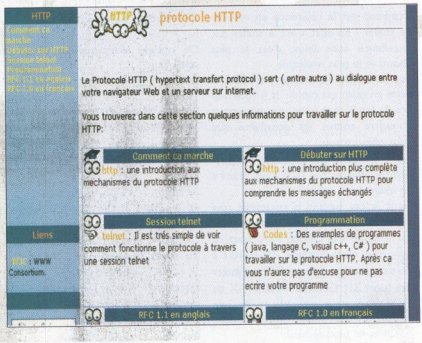
D'abord, POf est l'outil de fingerprinting passif le plus évolué à ce jour.
Le fingerprinting passif consiste à détecter le système d'exploitaiton de machines dialoguant sur le réseau en ne faisant qu'écouter le trafic. Ainsi, aucun paquet n'est envoyé vers les machines, ce qui rends cette méthode de 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://lcamtuf.coredump.cx/p0f-help/.

```
firewall:~/p0f# ./p0f -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)
192.168.0.1:1403 - 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
  -> 212.27.33.225:80 (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 !

LANGUE : Français
URL : http://www.iprelax.fr

Ce site est sérieux même s'il porte un nom plutôt amusant. Salemioche.com donne un 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. 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 codes nous montrent comment manier certains protocoles à travers plusieurs languages (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 francais directement disponible sur le site. Bonne visite!

Scapy

OS : Linux ● Logiciel Libre
URL : http://www.secdev.org/projects/scapy/

Il y a quelques jours sur le salon officiel de l'Net secret's une personne est venue en demandant quel était le meilleur langage de programmation pour débuter. Je lui ai proposé le Python qui est simple et complet pour débuter. 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 foie, j'ai trouvé Scapy qui est un programme très intéressant en Python, et 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, arpsk, arping, tcpdump, ethereal 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.

```
Fichier  Edition  Affichage  Terminal  Onglets  Aide
>>> a=sniff(filter="tcp and ( port 25 or port 110 )",
 prn=lambda x: x.sprintf("%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 faile
```

Tcpdump

OS : Linux
URL : http://www.tcpdump.org

Tcpdump est la référence en matière de sniffer ! En effet, c'est le sniffer par excellence sous linux, c'est le plus abouti et le plus malléable.

Son utilisation est des plus simples, la prise en main est rapide et il vous suffira de lire le man (man tcpdump) pour connaître toutes les possibilité que vous offre ce soft.

Admirons alors quelques unes des possibilités offertes par TCPDump grâce à un exemple.

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 obtiens alors quelque chose du style:

[..]
00:34:03.145837
192.168.0.1.2698 >
ftpperso.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..
[..]
```

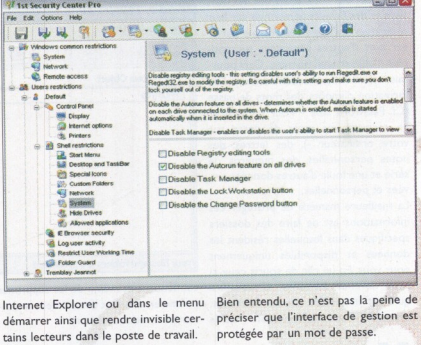
On voit clairement que la commande FTP 'CWD nitryx' (la commande FTP 'CWD' correspond au 'cd' sur une machine unix.) a été lancée par 192.168.0.1 sur le serveur.

Bien entendu, cela ne reste qu'un exemple. Il y a en effet des utilisation bien plus intéressantes que celle-ci à faire de tcpdump. Par exemple, auditer votre réseau pour découvrir ce qui transite ou non en « clair » sur votre réseau (donc non-crytpé), 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.

1st security

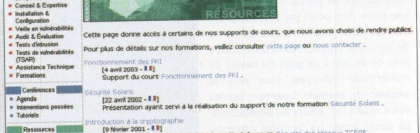
OS : Windows
URL : http:// www.1securitycenter.com



L'application de règles différentes pour chaque utilisateurs 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 invisible 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.

Hsc

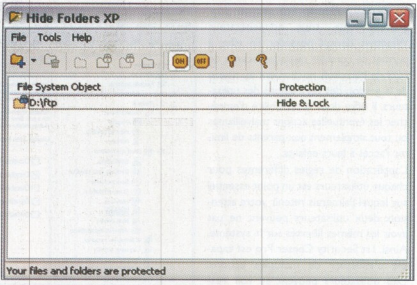


Le site de cette célèbre société de conseil en sécurité informatique est très intéressant par le nombre de documents techniques de références qui y sont publiés. Par les temps qui courent, il est très rare qu'une société commerciale fournisse les codes sources de ses travaux et interventions publiques. 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 clair 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 philosophique du site bien sûr ! ;)

Hide Folder

OS : Windows
URL : http://www.fspro.net

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 pourrais inclure l'information financiere, l'information d'impôts, des mots de passe (Cf. Password Safe - Pour enregistrer en securité 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 specifiques dans lesquelles 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



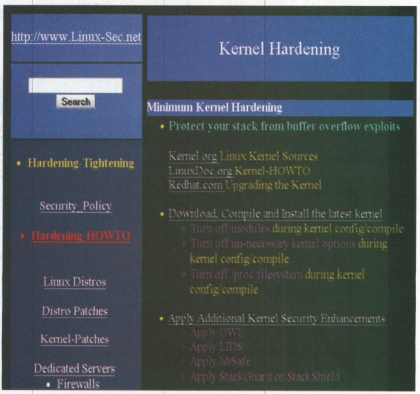
contiennent et même de les supprimer (même en enlevant directement le dossier de niveau supérieur).

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

Linux-sec.net

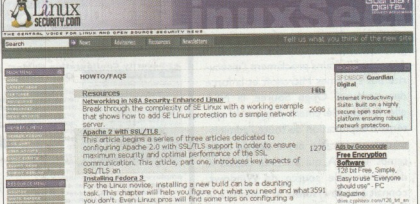
LANGUE : Anglais
URL : http://www.linux-sec.net

Personnellement, j'adore ce site ! Plutôt axé sur le contenu que la présentation, celui-ci 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 révèlera 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 sujet. Au hasard de nombreuses rubriques, vous pourrez trouver par exemple (attention, prenez votre souffle ;>) : toutes les distributions, les patchs 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.
Ce site a de quoi satisfaire les plus exigeants et permet de trouver rapidement les meilleurs sites sur tous ces sujets.



Linuxsecurity

LANGUE : Anglais
URL : http://www.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 certaine 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 meilleurs bases de données dans ce domaine pour les machines fonctionnant sous linux.

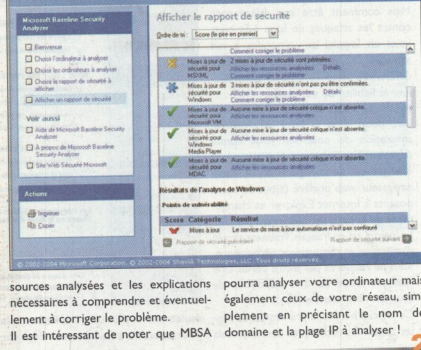
Sur celui-ci vous pourrez trouver les meilleurs tutoriaux et How-To à télécharger (en anglais) pour optimiser au mieux les performances de votre système.

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.

MBSA

OS : Windows 2K, XP, 2003
URL : http://microsoft.com/technet/security/tools/mbsahome.mspx



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 jours 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 inexistants, 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.

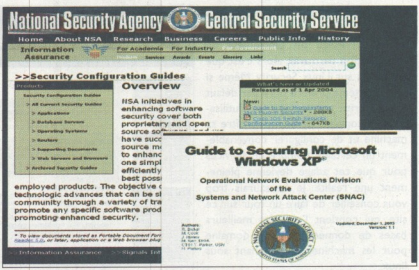
Le rapport présenté à la fin de l'analyse est intéressant et même pédagogique. En effet, il donne non seulement le résultat, positif ou négatif, des nombreux tests, mais aussi le détail des ressources analysées et les explications nécessaires à comprendre et éventuellement à corriger le problème.

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 !

Nsa.gov

LANGUE : Anglais
URL : http://www.nsa.gov/snac/

La plus grande agence gouvernementale américaine livre ses connaissances en matière de sécurité informatique au grand publique 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

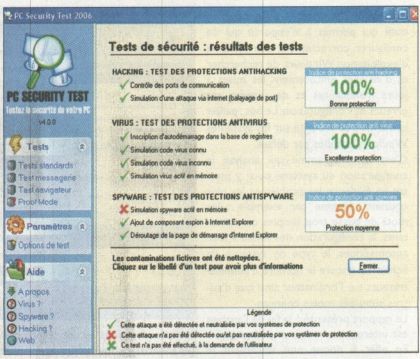


trouverez le guide du légendaire Microsoft IIS, d'IE 5.5 et même de Netscape.
Bien entendu, d'autre termes sont abordé. En tout cas, pas moins d'une quarantaine de guides de sécurité et de fichiers de configuration sont disponibles. Cependant, aucun logiciel libre n'est à l'affiche…

PC Security Test 2005

OS : Windows
URL : http://www.pc-st.com

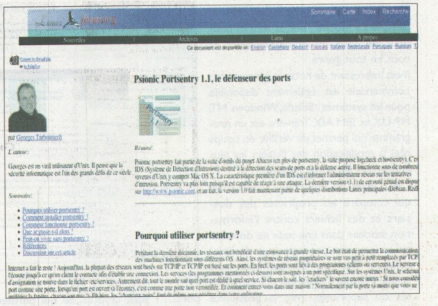
Vous voilà devant votre nouveau système fraîchement refait et configuré. Il est à jour et vous avez dépensé des centaines d'euros pour le protéger. Mais comment être sur d'être paré contre les attaques de base ? Et bien, voici un logiciel qui répondra à vos attentes. PC Sécurity Test va simuler différentes 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 connu (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 risquerez 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 ;)

Portsentry

OS : Linux
URL : http://sourceforge.net/projects/sentrytools/



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, loggé dans /var/log/messages. Pour les plus paranos d'entre nous, il est également possible d'exécuter une commande lorsqu'un scan est détecté. Exemple: ifconfig -i eth0 down. ;) PortSentry marque alors un point essentiel par rapport aux programmes passifs qui se contentent seulement de détecter les scans en cours.

Rootkithunter

OS : Unix
URL : http://www.rootkit.nl

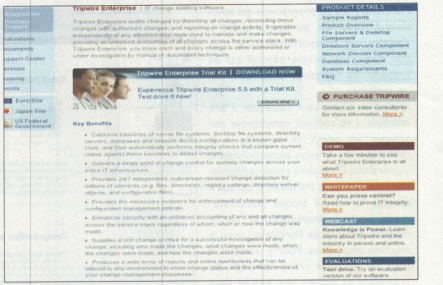
```
/usr/bin/du                                              [ OK ]
/usr/bin/file                                            [ OK ]
/usr/bin/find                                            [ OK ]
/usr/bin/head                                            [ OK ]
/usr/bin/kill                                            [ OK ]
/usr/bin/login                                           [ OK ]
/usr/bin/lsattr                                          [ OK ]
/bin/netstat                                             [ BAD ]
/bin/ps                                                  [ OK ]
/bin/sh                                                  [ OK ]
/bin/su                                                  [ OK ]
/usr/bin/chattr                                          [ 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 ]
```

RootKit Hunter est un logiciel libre qui permet de détecter la présence de certains rootkits sur les systèmes UNIX. Pour y arriver, ce script bash effectue une longue série de tests. D'abord, il y a un test d'intégrité (md5) des fichiers importants – notament des binaires utilisés par le script même – en fonction d'une base de données de divers systèmes et leur différentes version (surtout pertinent sur les système 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.

Tripwire

OS : Linux
USL : http://sourceforge.net/projects/tripwire/

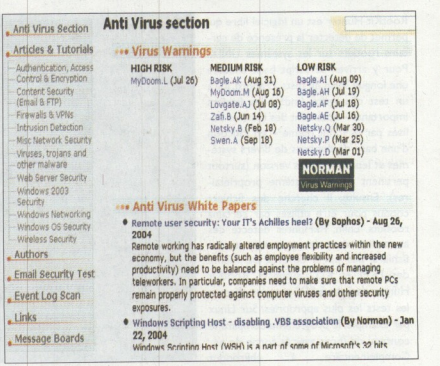
Ce logiciel open source est en priorité destiné au monde *nix et fera le bonheur de tous les administrateurs et root en tout genre.
Il est intéressant de noter qu'une version commerciale est également disponible pour les systèmes : Solaris, Windows NT, HP-UX et IBM AIX. Tripwire est un programme qui 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..



Windowsecurity.com

LANGUE : Anglais
URL : http://www.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 pour 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'intrusion 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.

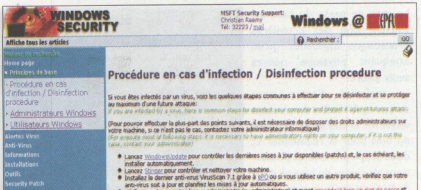


Windowsecurity est un site au contenu très varié qui ne demande qu'à être visité par tous ceux qui désirent améliorer leur sécurité.

Winsec.epfl.ch

LANGUE : Français
URL : http://winsec.epfl.ch

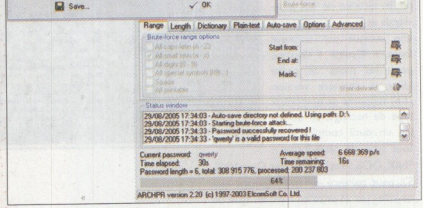
Ce site, Suisse et francophone, vous propose de vous donner les bases et les moyens pour sécuriser votre machine fonctionnant sur un système Windows 32 bits. Vaste programme ! Sur le site vous trouverez 5 rubriques principales. La première, qui vous donnera, en tant qu'administrateur ou utilisateur, 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 offensif sur les systèmes Windows, ainsi que des conseils pour vous prémunir contre ces derniers. Le site possède aussi des pages : outils, patchs et spam, qui vous permettrons 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.



Advanced Archive password recovery

OS : Windows
URL : http://www.elcomsoft.com

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.
A 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 on 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 ;).



Cmospwd

OS : Dos, Windows, Linux, FreeBSD, NetBSD
URL : http://www.cgsecurity.org

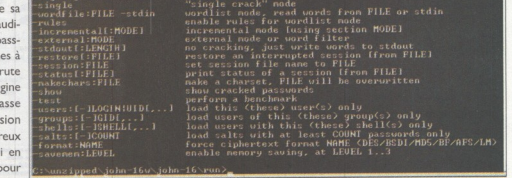
Le mot de passe du bios est souvent une des premières protections logicielles qu'un attaquant physique pourra avoir affaire.
La majorité d'entre nous savons qu'il suffit simplement d'enlever la pile de la mémoire du bios pour la réinitialiser et donc supprimer toutes protections au niveau du bios et donc de 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.

```
firewall:~/cmospwd-4.6/src# ./cmospwd --help

CmosPwd - BIOS Cracker 4.6, February 2005, Copyright 1996-2005
CERNIER Christophe, cgenier@cgsecurity.org
http://www.cgsecurity.org/

Usage: cmospwd [/k[de|fr]] [/d]
       cmospwd [/k[de|fr]] [/d] /[r|w] cmos_backup_file          restore/loa
rite
       cmospwd /k                                                kill cmos
       cmospwd [/k[de|fr]] /m[01]*          execute selected module

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

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

Cmospwd est ici le logiciel qu'il nous faut car il permet en effet de cracker différentes marques de bios. Cmospwd permet de sauvegarder, restaurer et effacer la cmos. Ainsi il est possible de récupérer, restaurer et effacer le mot de passe du bios. La compatibilité du programme avec votre matériel n'est pas un problème, cmospwd est open source, et cela lui permet de bénéficier de nombreuses contributions afin de travailler sur de nombreux bios à partir de nombreux OS.
Cmospwd est donc une alternative intéressante à la, n'hésitez pas à lire le fichier README pour de plus amples informations sur ce soft !

John The Ripper

OS : *NIX, DOS, Win32, BeOS, OpenVMS
URL : www.openwall.com/john/

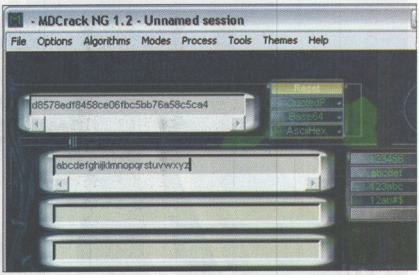


John the Ripper est le plus célèbre cracker de mots de passe. Il est développé par Solar Designer en licence GNU. Le plus rapide de sa catégorie, il permet d'auditer la sécurité de vos passwords et leurs résistances à une attaque par « brute force ». Conçu à l'origine pour les mots de passe Unix, la dernière version (1.6) supporte de nombreux type 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.

Mdcrack

OS : Windows, Unix
URL : http://c3rb3r.openwall.net/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 caractère originale. Il est également beaucoup utilisé dans les bases de données pour stocker les mots de passes. 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 choisis lors de la création de votre compte. Si les deux hashs correspondent, le mot de passe est valide.

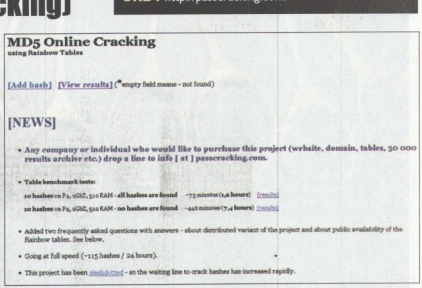


Ainsi MDCrack procède de la même manière. Il compare les signatures de toutes les combinaisons de chaînes de caractères possible avec la signature que vous voulez cracker.
MDCrack est donc un bon soft, mais ne vous réjouissez pas trop vite, cela peut prendre du temps …

passcracking.com (md5 online cracking)

LANGUE : Anglais
URL : http://passcracking.com/

Vous avez un hash à cracker ? Passcracking.com pourra vous être d'une aide précieuse. En effet, passcracking.com vous propose de cracker vos hash en un temps record !
Loin d'avoir des machines surpuissantes, le site dispose d'un énorme base de donnée de hash, appelées 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'environs de 48 Go !!
Outre le coté pratique de ce site, il permet de se pencher davantage sur l'utilisation des Rainbow tables pour ainsi comprendre davantage son fonctionnement. Je vous invite à lire la surf session du The Net secret's Journal n°17 ou dvrasp nous explique brièvement et clairement tout cela.
Un site donc à la fois utile et éducatif ! A visiter :).



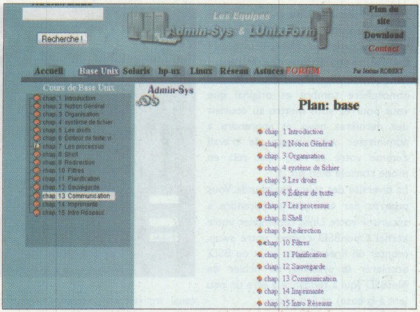
Administration & développement

L'ADMINISTRATION ET LE HACKING SONT LES DEUX FACES DU MEME TOKEN

! REMEMBER !

Admin-sys

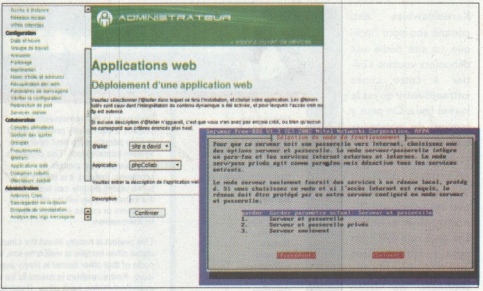
LANGUE : Français
URL : http://www.admin-sys.com



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

FreeEOS

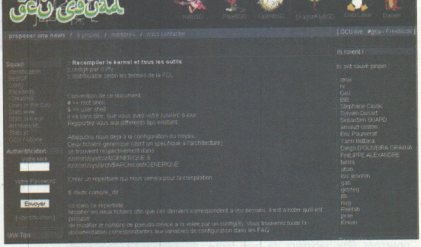
URL : http://free-eos.org/
OS et logiciels libres



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 messagerie instantanée ou 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 !

Gcu Squad

LANGUE : Français
URL : http://www.gcu-squad.org



Avis aux amateurs d'Unix en tous genres ! 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 original 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 sur ;).

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 fichier 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 (irc.freenode.com #gcu), ça peut toujours aider !

Bref, gcu-squad a de quoi vous scotcher à votre écran pendant de longues et belles heures !

Kernelnewbies

LANGUE : Anglais
URL : http://www.kernelnewbies.org

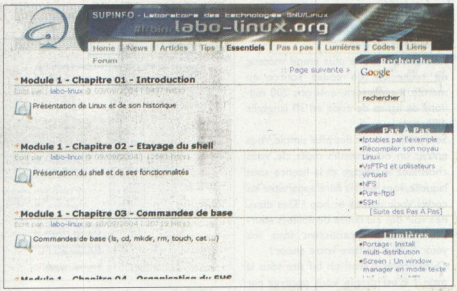
Kernelnewbies est, comme son nom l'indique, un site dédié aux débutants voulant s'initier à cette chose extraordinaire qu'est le kernel linux. On peut y trouver de nombreux tutoriaux explicatifs, un glossaire très complet permettant d'obtenir une définition exhaustive des principaux éléments relatifs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

Labo Linux

LANGUE : Français
URL : http://www.labo-linux.org

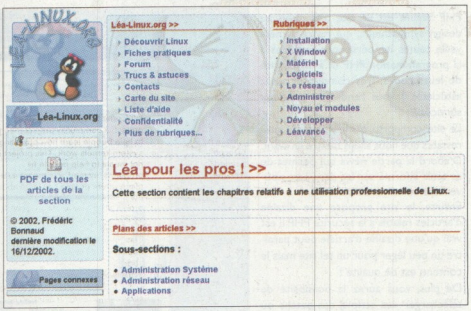
Le labo linux est l'un des labos de l'école d'informatique supinfo. Une fois arrivé sur la page d'accueil, on a déjà une vue d'ensemble du site. L'interface permet de se repérer facilement. Un système d'icônes différencie les types d'articles, de news ou de tips. On peut également trier les documents 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'oeil ! Ceci donne un ensemble convivial, simple et pratique. Par ailleurs, il faut noter que les concepteurs on 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.



Linux Entre Amis (Léa)

LANGUE : Français
URL : http://www.lea-linux.org

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 pars des concepteurs du site. A consulter sans modération !



Koders.com

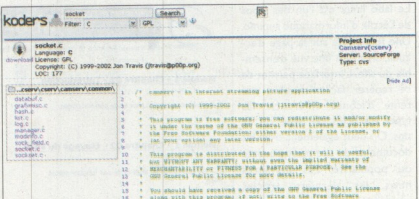
LANGUE : Francais
URL : http://www.koders.com

Avis aux accrocs 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 environs 200 millions de lignes de code en 30 langages différents !

Son utilisation est des plus simple. 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 voir des centaines de fichiers sources différents apparaissent sous vos yeux. A 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.

Phpsecure

LANGUE : Français, Anglais, Russe
URL : http://www.phpsecure.info

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 sur les 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'article 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 patchs ou des outils afin de rendre votre code plus sécurisé.

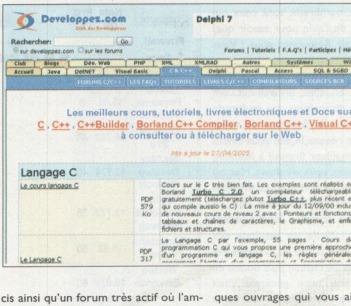
Nous terminerons sur un des points majeurs de ce site. En effet, si vous le souhaitez, vous aurez la possibilité de proposer une news ou même un patch pour le site. Et oui, c'est grâce à ses contributeurs que le site est, aujourd'hui, devenu une référence.

Developpez.com

LANGUE : Français
URL : http://www.developpez.com

La programmation est de nos jours une des bases indispensables 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 débuter.

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

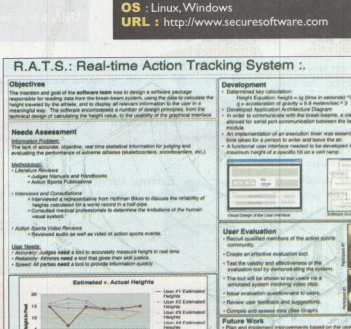


Pour chaque langage vous est proposé de l'aide grâce à des tutos clairs et précis ainsi qu'un forum très actif où l'ambiance y est conviviale. De plus pour ceux qui préfèrent les livres à l'écran, le site donne pour chaque langage quelques ouvrages qui vous aiderons dans votre apprentissage.
Bref, un concentré de points positifs qui feront la joie de certains !

RATS

OS : Linux, Windows
URL : http://www.securesoftware.com

Quel programmeur n'a jamais rêvé d'un outil qui audite son code à la recherche de failles de sécurité ou de buffer overflow ? Et 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 ainsi d'identifier rapidement les appels potentiellement dangereux des fonctions par exemple. Il exécute également une analyse de base pour essayer d'éliminer les conditions qui ne sont pas forcement 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 si il permet de voir rapidement les problèmes rencontrés les 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 pourrais le faire un hacker.
Couplé à votre bon sens, RATS deviendra alors un outils indispensable.



Firewall-net

LANGUE : Français, Anglais
URL : http://www.firewall-net.com

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 servis ! Les firewalls sont testés scrupuleusement afin de vous offrir des comptes rendus précis. Le site vous affiche les résultats aux tests de sécurité, il liste les avantages et inconvenients 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.

Comparer | Note /20 | Prix € | Système

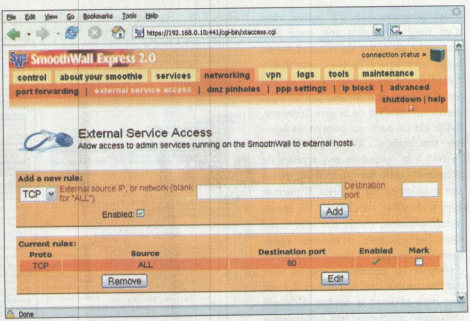
Firewall Tous	95	98	ME	2000	NT	XP	Mac	Linux	Ping	Net bus	TCP	UDP	Leak test
Look'n'Stop 17.46 39	✓	✓	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓
Kerio Personal Firewall 15.04 0	x	✓	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓
Outpost Pro 14.732 40	✓	✓	✓	✓	✓	✓	x	x	✓	✓	✓	1/2	✓
McAfee Desktop Firewall 13.776 40	✓	✓	✓	✓	x	✓	x	x	✓	1/2	✓	✓	✓
Xelios Personal Firewall 12.772 35	✓	✓	✓	✓	-	✓	x	x	✓	✓	-	-	✓
Zonealarm Pro 10.92 60	✓	✓	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓
Norton Personal [illegible] 10.072 60	x	✓	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓

A noter: si votre esprit de curiosité est en éveil, vous remarquerez que ce site est également enrichis de quelques articles intéressant notamment une introduction au fonctionnement des anti-virus. Bonne visite !

Smoothwall

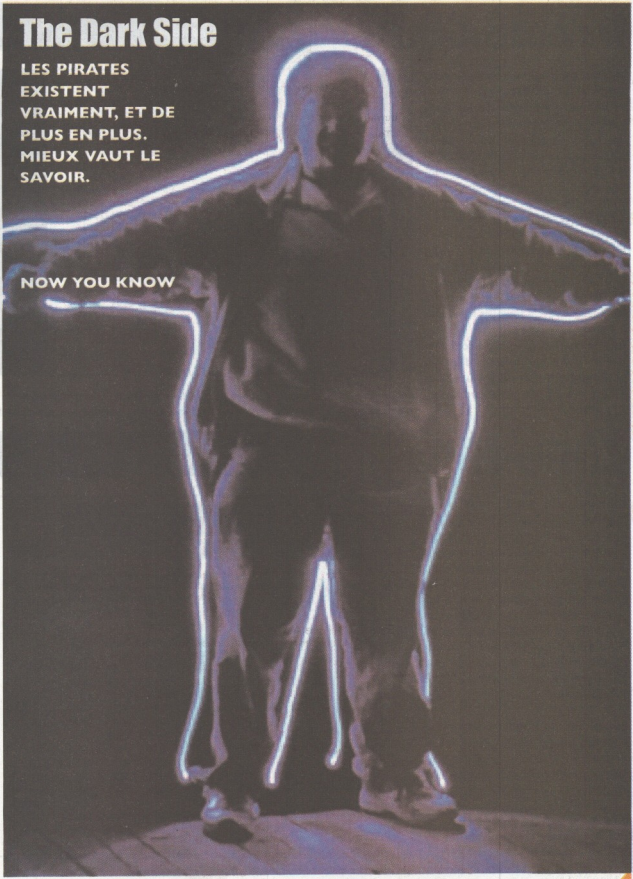
URL : http://www.smoothwall.org

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 prends 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 server 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 !


The Dark Side
LES PIRATES EXISTENT VRAIMENT, ET DE PLUS EN PLUS. MIEUX VAUT LE SAVOIR.
NOW YOU KNOW

62nds.co.nz

LANGUE : Anglais
URL : http:// 62nds.co.nz

Ne vous êtes vous jamais demandés quels étaient les secrets des plus grand virus ? Pour la majeure partis d'entre vous, vous nous répondrez que si. Cependant les seuls bout de code que la plupart d'entre nous auraient pu étudier ont la souvent été « arrangés » afin de les rendre inofensifs. 62nds.co.nz nous propose ici les codes sources bruts et complets de ces virus qui ont fait couler pas mal d'encre à travers la presse. Citons par exemple le fameux virus Annakournikova, Melissa ou même I love you. Bien sûr, lorsque l'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.

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
bkh.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
LIFZ_STAGES.TXT	08-Sep-2004 02:49
Marked.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
v90at.com.pdf	08-Sep-2004 02:50
VBSWG-AQ.decoded.txt	08-Sep-2004 02:50

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 !

Zone-H

LANGUE : Anglais, Français, Russe, Italien
URL : www.zone-h.org

Ce site traitant de sécurité informatique est des plus complets. Un nombre impressionnant de toolz (+ 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.

Ce site est mis à jour de façon régulière et offre des informations claire et concises. Vous aurez la possibilité d'interagir sur ce site par le biais de leur chat irc ou de leur forum, où les discussions vont bon train sur des sujets tels que les rumeurs sur les 0dayz (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 intéressant à visiter pour le hacker comme pour le responsable sécurité.

zone-h — Unrestricted Information

zone-h | get from JMX your zone-h t-shirt

LANGUAGE

RECHERCHE

MENU PRINCIPAL
Accueil
Infos from zone-h
Infos from the world
Astuces
Téléchargement
Zone-H works
Digital attacks
Site pirates/Archives des crimes
Site pirates/Archives des crimes +
Référencer un piratage
Stay tuned
Inscription mailing-list

STATISTIQUE DES HACKERS

No	Hacker	Piratage d'IP individuel	Piratage en masses	Total des sites pirates	Piratage de page persos	Classement
1.	iskorpitx	9511	66767	76278	9426	66852
2.	Fatal Error	8135	11626	19761	15143	4618
3.	Red Eye	4789	28504	33293	33002	291
4.	1hidek	4384	29454	33838	33757	81
5.	TechTeam	4333	32033	36366	36353	13
6.	SPrK IDS	4266	11988	16254	15286	968
7.	r00t_System	4046	19221	23267	21039	2228
8.	hacklad crew	3853	6473	10326	5267	5059
9.	Infektion group	3731	30326	34057	32480	1577
10.	Sirmens	3631	32025	35656	35606	50
11.	BloodBR	3262	16429	19691	19684	7
12.	1DN	3127	3324	6451	5128	1323
13.	PtDefisi	2909	3347	6256	568	5688
14.	nbbodycoder	2690	1257	3947	939	3008
15.	c0d3rz	2646	1655	4301	3248	1053
16.	HACKERBR	2495	12711	15206	14515	691
17.	rEt^DeViL	2405	2149	4554	2099	2455

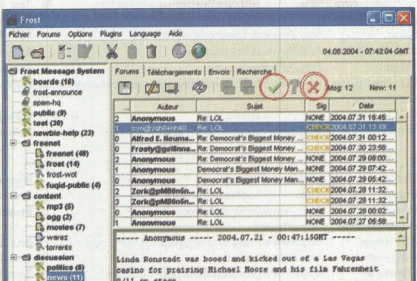
LANGUE : Anglais
URL : http://milw0rm.com

milw0rm.com est une base de données intéressantes d'exploits et shellcodes en tout genre. Le sites est mis à jour régulièrement afin de fournir des exploits pour les dernières versions d'applications vulnérables.
Ainsi le site fourni des exploits local, remotes pour des plate-forme aussi diverses que linux, windows, novell, hp-ux, bsd et j'en passe.
Le site fourni également des exploits pour des application 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 fonctionnent et le pourquoi de la faille.
Ceci se révèle être 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 pratique pour trouver ce que l'on rechercher très rapidement.
Milw0rm.com est donc un site qui pourra permettre à chacun d'évaluer efficacement la sécurité de son système ou de ses applications.

Freenet

OS : Linux,Windows
URL : http://freenet.sourceforge.net/

Freenet est un réseau informatique anonyme et décentralisé, bâti au dessus d'Internet et conçu pour exercer une liberté d'expression totale et résistant à la censure. Sa nature permet donc à chacun de lire et de publier du contenu. Il offre la plupart des services actuels d'Internet (email, téléchargement, web, etc.). Le contenu de Freenet est extrêmement varié on y trouve vraiment n'importe quoi et surtout n'importe quoi. Étant le seul réseau vraiment anonyme à large échelle, on y trouvera donc des sites de hacking très underground ne respectant pas la loi en vigueur...
Néanmoins la liberté à un prix ! Les deux principaux défauts de Freenet sont son insupportable lenteur (chaque utilisateur héberge une partie du réseau) mais aussi le contenu parfois extrêmement trash que l'on peut y trouver. Néanmoins si l'utilisation reste réfléchie il n'y aura aucun problème : on ne trouve que ce que l'on cherche.



Le logiciel d'échange de fichiers Frost

À découvrir dans

Prise d'information

1. Détection d'OS

p0f	http://lcamtuf.coredump.cx/p0f.shtml	Détection passive
Queso	http://packetstormsecurity.org.pk/UNIX/scanners/	Détection active (TCP/IP)
Xprobe2	http://xprobe.sourceforge.net/	Détection intelligente

2. Scanners de ports

NmapFE	http://www.advogato.org/proj/NmapFE/	GUI complète pour nmap
Unicorn Scan	http://www.unicornscan.org/	Scanner de port distribué et plus

3. Divers

DNS enum	http://www.hackingdefined.com/tools/reconnaissance/dnsenum.zip	Énumeration d'info (zones, reveses lookups, etc.)
NBTScan	http://www.inetcat.org/software/nbtscan.html	Scan NETBIOS
LinNeighborhood	http://www.bnro.de/~schmidjo/	Navigateur SMB avec GUI pour nux
Cheops	http://www.marko.net/cheops/	Explorateurs réseau + outils
AutoScan	http://autoscan.free.fr/	Explorateur réseau + scanner de port
SNMP enum	http://packetstormsecurity.org.pk/UNIX/scanners	Explorateur SNMP
Mibble	http://mibble.org	Parser/Manipuler des MIB (SNMP)
Sam Spade	http://www.samspade.org/	Pris d'info multi-fonctions pour Windows
Luma	http://luma.sourceforge.net/ Navigateur	LDAP et outils

Exploits, vulnérabilités, Pen-testing

1. Scanners de vulnérabilités

Sql Power Injector	http://www.sqlpowerinjector.com/index.htm	Test d'injections SQL
Nessus	http://www.nessus.org/Nessus	Scanner de vulnérabilités
Nikto	http://www.cirt.net/code/nikto.shtml	Scanner de vulnérabilités web
Shadow Security Scanner	http://www.safety-lab.com	Scanner de vulnérabilités
Retina	http://www.eeye.com/	Scanner commercial (gestion de risques, etc)
Microsoft Baseline Security Analyser	http://www.microsoft.com/technet/security/tools/mbsahome.mspx	Outil local de Microsoft
CISCO Torch	http://www.arhont.com/	Scanner et prise d'info CISCO
Yersina	http://www.yersinia.net/	Scanner de vulnérabilités (protocoles)

2. Mots de passe

Hydra	http://www.thc.org/	Bruteforceur FTP, POP, IMAP, Telnet, HTTP, LDAP, etc. etc.
Brutus	http://www.hoobie.net/brutus/	Brutforceur multi-fonctions pour Windows
Mezcal	http://www.0x90.org/releases/mezcal/	Brutforceur HTTPS
thc-pptp-bruter	http://thc.org Brutforceur PPTP	
ADMsnmp	http://www.freshports.org/security/ADMsnmp	Brutforceur SNMP
Guess-who	http://www.team-teso.net/	Bruteforceur SSH
Obiwan III	http://www.phenoelit.de/obiwan/oIII.pl.txt	Bruteforceur HTTP
VNCCrack	http://www.randombit.net/projects/vnccrack/	Bruteforceur VNC (offline : après sniffing)
RainbowCrack	http://www.antsight.com/zsl/rainbowcrack/	Rainbow tables
Fcrackzip	http://www.goof.com/pcg/marc/fcrackzip.html	Cracker de ZIP
Nasty	http://www.vanheusden.com/	Cracker de pass GPG/PGP
OpenWall	ftp://ftp.openwall.com/pub/wordlists/	Petite collection de wordlists (généralistes et différentes langues)
PacketStorm	http://packetstormsecurity.org/Crackers/wordlists/	Énorme collection de wordlists

le web profond

3. Frameworks

Metasploit	http://www.metasploit.com	Plateforme de développement/test d'exploits
SecurityForest	http://www.securityforest.com/wiki	Idem (en développement)
Canvas	http://www.immunitysec.com	Idem (commercial)
CORE IMPACT	http://www.coresecurity.com/products/coreimpact/	Idem (commercial)

4. Fuzzers

Spike	http://www.immunitysec.com/resources-freesoftware.shtml	Framework générique
Bed	http://www.snake-basket.de/bed/	Fuzzer de protocoles
Peach	http://peachfuzz.sourceforge.net	Framework Python cross-plateform
SNMP Fuzzer	http://www.arhont.com/	Fuzzer SNMP

5. Sniffers/MITM

Etherape	http://etherape.sourceforge.net/	Moniteur de réseau avec GUI
Ethereal	http://www.ethereal.com	Sniffer + analyse de protocoles
Ngrep	http://ngrep.sf.net	Sniffer + recherche à la grep
NetSed	http://packetstormsecurity.org/UNIX/misc/	Injection/modification de paquets
SSLDump	http://www.rtfm.com/ssldump/	Analyse de SSLv3/TLS
Sniffit	http://www.tengu.be	Sniffer
Webmitm	http://www.monkey.org/~dugsong/	MITM http (inclu dans dsniff)

6. Spoofing/Forging

Ettercap	http://ettercap.sourceforge.net/	Sniffer/Spoofer multi-fonctions (ARP, mitm, etc)
DHCPX	http://fresh.t-systems-sfr.com/unix/src/privat2/	Flooder DHCP
Fragroute	http://www.monkey.org/~dugsong/fragroute/	Évasion d'IDS
TCPReplay	http://tcpreplay.synfin.net/	Rejeu de trafic
Etherwake	http://packages.debian.org/stable/net/etherwake	Réveil à distance (ethernet)

Sans-fil

1. WiFi

Air Crack	http://packages.debian.org/unstable/net/aircrack	Cassage WEP/WPA
Kismet	http://www.kismetwireless.net	Détection, sniffer, IDS pour 802.11
NetStumbler	http://www.netstumbler.com	Détection de réseaux sans-fil

2. Bluetooth

Trifinite	http://trifinite.org/	Excellent site sur la sécurité BT avec énormément d'outils
BlueDiving	http://bluediving.sourceforge.net/	Audit Bluetooth

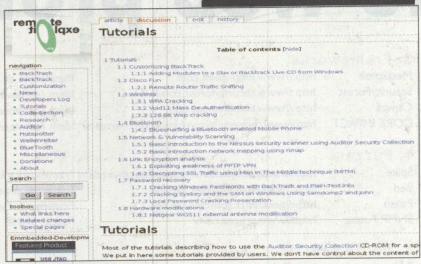
Challenges

Pull The Plug	http://www.pulltheplug.org/	Plusieurs machines dédiées
Hackers Lab	http://www.hackerslab.org/	Challenge Coréen avec 17 niveaux de difficulté croissante
Securitech	http://www.challenge-securitech.com/	Concours annuel (solutions en ligne)
3564020356	http://3564020356.org/	Challenge de reversing
Security-Challenge	http://www.security-challenge.com	100 failles web à trouver
Python Challenge	http://www.pythonchallenge.com/	Challenge de programmation
HackerGames	http://hackergames.net/	Annuaire très complet

Tutoriels vidéo : le pionnier

URLS :
http://www.hackdefined.com,
http://www.remote-exploit.org

Nous lisons tous des documents sur des sujets divers liés au hacking que nous ne comprenons parfois que partiellement (parce que, par exemple, ils ne sont pas écrits dans notre langue maternelle). Ces textes, les fameux tutoriaux – ou tutoriels, selon les disciples – permettent d'amorcer un apprentissage : on y voit comment réaliser un action, et le travail à faire reste de se renseigner sur les différentes partie qui constituent ou permettent la réalisation de cette action. Mais ces tutoriaux sont parfois long à écrire, et difficiles parfois d'expliquer avec des mots : l'idée d'une version vidéo est née, parce qu'un bon exemple vaut mieux qu'un long discours.

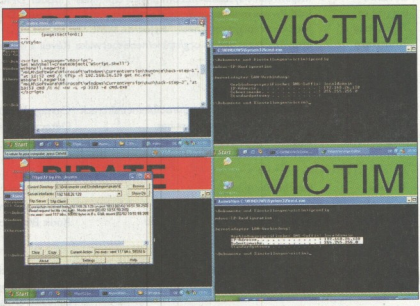


Le plus connu de ces tutoriels vidéos est certainement celui qui porte le doux titre de « Cracking Wep in ten minutes ». Disponible sur www.hackdefined.com, cette video fait office de précurseur dans le domaine : on y voit comment, en seulement quelques minutes, des outils disponibles sur feu la distrib whoopix (devenue depuis BackTrack, téléchargeable chez www.remote-exploit.org) peuvent cracker une clef de protection wifi (à noter qu'il s'agit alors de clef de 64 bits).

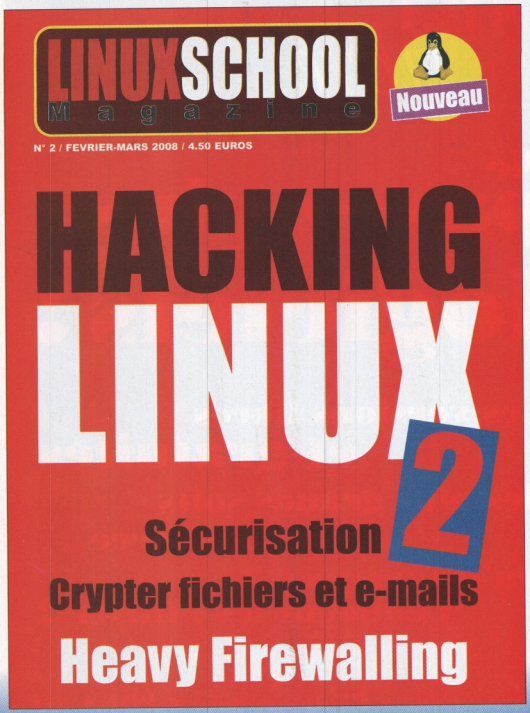
La relève

URLS : http://irongeek.com,
http://under.newbie.free.fr

Près de 40 vidéos composent la bibliothèque d'IronGeek. Certaines d'entre-elles sont issues d'autres sites, et d'autre ne sont pas vraiment des vidéos pédagogiques ; malgré cela, toutes sont intéressantes. Deux vidéo ont retenu mon attention : « Basic NMAP usage » et « Basic Tools for Wardriving ».
La première vidéo vous montrera l'utilisation de NMAP, le plus connu et probablement le plus puissant des scanneurs de ports.



La seconde vous présentera l'utilisation de logiciels pour le wardriving, une épreuve très sportive consistant à conduire un véhicule avec un ordinateur portable sur le siège passager, avec la carte wifi et un sniffer allumé pour détecter les réseaux Wifi alentours.
Vous trouverez également 17 vidéos sur le site UnderNewbie. Certaines sont appréciables en ce qu'elle démontrent l'importance de la sécurité informatique. Par exemple, la vidéo numéro 16, qui démontre comment un pirate peut voir quels sont les sites visités par sa cible. Exemple concret du tutoriel : le script VB apparaît clairement durant la vidéo, il ne reste qu'a se renseigner sur les différentes fonctions que l'on y trouve.



En vente en kiosque