

# LINUX SCHOOL

M a g a z i n e



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

### **p.3 : 1-Anonymat & Confidentialité**

- p.4 Proxys/Anonymisers
- p.7 Confidentialité

### **p.9 : 2-Hacking**

- p.10 Connaissances de base
- p.13 Zines & groupes
- p.17 Failles et exploitation
- p.19 Réseau
- p.25 Sécurisation
- p.31 Mots de passe

### **p.34 : 3-Administration & Développement**

- p.35 Unix
- p.38 Programmation
- p.40 Firewalls

### **p.41 : 4-The Dark Side**

Virus, worms, defaces, script kiddies...

## 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 Roto Garonne  
ZA "Mestre-Marty" 47310 Estillac

© LPN 2008

## 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 ?

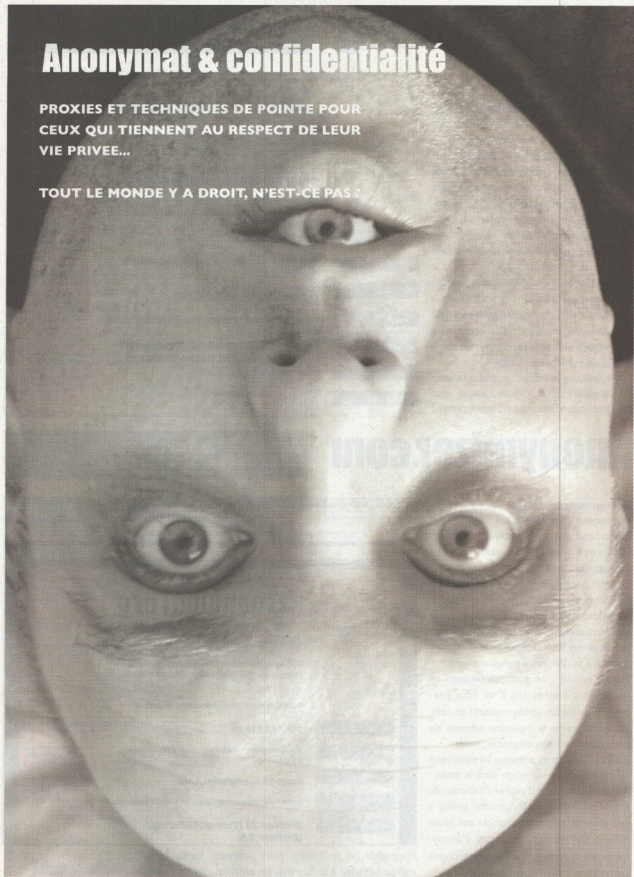
Linux school HS vous révèle... tous ces secrets.

## ...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

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](http://anonymat.org) ! Vous pourrez alors grâce à ce site savoir si votre proxy est vraiment efficace. Le site vous renverra alors automatiquement toutes les informations qu'il a pu se procurer sur vous lors de votre connexion à 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 !

**LANGUE :** Français  
**URL :** <http://www.anonymat.org>

**Anonymat.org**

**Vos traces**

Voici quelques informations qu'il est possible de collecter sur vous lorsque vous surfez sur Internet...

Vous êtes connecté à Internet avec l'adresse IP : **200.253.198.189**

Via le serveur de votre fournisseur d'accès (ou le proxy) : **clients125.fortanet.com.br**

Votre navigateur et votre système d'exploitation sont : **Mozilla/5.0 (Windows; U; Windows NT 5.1; fr-FR; rv:1.7.6) Gecko/20050226 Firefox/1.0.1**

En clair, votre navigateur est :

**Les Sites**

- Messages anonymes
- Messages anonymes sécurisés
- Surf anonyme & proxy
- Testez votre anonymat
- Services distants

**Les Scripts**

- Messages anonymes
- Messages anonymes sécurisés
- Solutions d'anonymat
- Outils de chiffrement
- Élimination des spywares
- Effacement sécurisé
- Documentation système
- Ordinateurs de cookies
- Firewall
- Proxy
- Recherche
- Utilitaires pour experts
- Utilitaires divers

ACCUEIL  
EDITO  
ACTUALITE  
VOS TRACES  
ANNUAIRE  
OUTILS  
NEWSLETTER

Messages anonymes  
Messages anonymes sécurisés  
Surf anonyme & proxy  
Testez votre anonymat  
Services distants

Messages anonymes  
Messages anonymes sécurisés  
Solutions d'anonymat  
Outils de chiffrement  
Élimination des spywares  
Effacement sécurisé  
Documentation système  
Ordinateurs de cookies  
Firewall  
Proxy  
Recherche  
Utilitaires pour experts  
Utilitaires divers

## 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 côté gratuit du site.

En effet [anonymizer.com](http://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](http://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.com](http://anonymizer.com), ce qui revient à la même chose qu'un proxy anonyme classique.

**Anonymizer.com**

**Vos traces**

Voici quelques informations qu'il est possible de collecter sur vous lorsque vous surfez sur Internet...

Vous êtes connecté à Internet avec l'adresse IP : **168.143.113.56**

Via le serveur de votre fournisseur d'accès (ou le proxy) : **ibout-56.anonymizer.com**

Votre navigateur et votre système d'exploitation sont : **Mozilla/4.78 (TuringOS; Turing Machine; 0.0)**

ACCUEIL  
EDITO  
ACTUALITE  
VOS TRACES  
ANNUAIRE

Messages anonymes  
Messages anonymes sécurisés  
Surf anonyme & proxy  
Testez votre anonymat  
Services distants

Messages anonymes  
Messages anonymes sécurisés  
Solutions d'anonymat  
Outils de chiffrement  
Élimination des spywares  
Effacement sécurisé  
Documentation système  
Ordinateurs de cookies  
Firewall  
Proxy  
Recherche  
Utilitaires pour experts

Pour plus de simplicité, vous pourrez 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 d sesp r es   la recherche de proxy valides et efficaces.

Que ceux-la se r joissent, proxy4free.com est l'une des plus grandes bases de donn es de proxy au monde. En effet ce site recense quotidiennement plusieurs milliers de proxy diff rents class s selon leur type (transparent, anonymous et high anonymity) et leur localisation.

Notons qu'on ne comprends pas toujours la diff rence entre un « anonymous proxy » et un « high anonymity proxy ». Celle-ci r siede en fait au niveau des informations renvoy es aux sites visit s   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-

Page	Name	Port	Type	Country	Last Test	Whois
page 8	168.234.181.154	3128	transparent	Guatemala	21.07.2005	Whois
page 9	80.249.73.66	80	transparent	Algeria	21.07.2005	Whois
page 10	193.126.233.58	80	anonymous	Portugal	21.07.2005	Whois
IMPORTANT TIPS	81.72.214.52	3128	transparent	Italy	21.07.2005	Whois
LINKS	203.162.220.203	8080	transparent	Vietnam	21.07.2005	Whois
LINK EXCHANGE	221.10.55.202	8080	anonymous	China	21.07.2005	Whois
TO DO LISTES	203.162.115.35	80	transparent	Vietnam	21.07.2005	Whois
Stay Invisible	203.162.115.36	80	transparent	Vietnam	21.07.2005	Whois
Public Proxy Servers	203.162.116.67	80	transparent	Vietnam	21.07.2005	Whois
Apornymity Checker	203.162.31.28	80	transparent	Vietnam	21.07.2005	Whois
Online Proxy Checker	203.162.114.173	80	transparent	Vietnam	21.07.2005	Whois
Proxy	163.21.13.5	80	anonymous	Taiwan	21.07.2005	Whois
0Privacy.com	203.162.119.117	80	transparent	Vietnam	21.07.2005	Whois
Internet Utilities & Bench Tools	193.194.84.198	8080	anonymous	Algeria	21.07.2005	Whois
	61.135.158.106	80	anonymous	China	21.07.2005	Whois
	200.203.60.100	3128	transparent	Brazil	21.07.2005	Whois
	212.0.138.29	80	high anonymity	Sudan	21.07.2005	Whois
	203.162.114.138	80	transparent	Vietnam	21.07.2005	Whois
	81.199.24.18	80	transparent	Uganda	21.07.2005	Whois

ci mais  galement les variables HTTP\_VIA et HTTP\_PROXY\_CONNECTION aux serveurs demand s par le client. Malgr  les mises   jours quotidiennes, une

partie de la liste des proxy ne fonctionne pas, pour  viter de les tester un par un, aidez vous d'un testeur de proxy comme: <http://www.checkipfreeproxy.com/checkip/>

# 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   tous les outils d'anonymats actuel semble  tre leur manque de fonctionnalit s et la difficult  de leur mise en place. Une solution excellente est Proxychains.

Proxychains est un programme au concepteur novateur qui s'utilise de fa on totalement transparente. Pour ce faire, il va intercepter les appels aux fonctions utilisant les sockets (gr ce au Preload de biblioth ques) et intercaler lors de vos connexions un ou plusieurs proxys de votre choix. Les types de proxys support s sont : http (connect), socks4 et socks5.

Etant donn  qu'il intercepte toutes les fonctions de types sockets, aucune configuration des logiciels utilis s n'est n cessaire et ceux-ci sont tous compatibles. Ainsi, au lieu de taper :

ssh monardi.com  
vous taperez :

proxychains ssh monardi.com  
et vous serez connect  au travers d'un ou plusieurs proxys   votre destination. Le gros point fort de ce programme est que sa configuration est relativement simple, puisqu'il vous suffit d'entrer une s rie de proxys valides dans votre fichier de configuration et de sp cifier le mode de chaînage parmi les 3 suivants : Random, Strict ou Dynamic. L'authentification sur les proxys est elle aussi g r e, et il vous suffira pour cela d'informer les champs utilisateurs et mot de pass lors de la r alisation de votre fichier de configuration (/etc/proxychains.conf).

Le nombre de proxys   cha ner n'est pas limit , bien que le temps de latence augmente de fa on proportionnelle au nombre de proxys utilis s. Vous pourrez utiliser ce logiciel en toutes circonstances : navigateurs internet, mails, ssh, ftp, telnet, etc... L'utilisation de proxys reste   ce jour la meilleure forme d'anonymat et de protection de la vie priv e sur le Web et plus g n ralement sur Internet. Ce programme permet leur utilisation de fa on vraiment simplifi e, alors pourquoi s'en priver ?  
Ce programme en est actuellement   sa version 1.8.2 et s'adresse aux OS type Unix,   savoir Linux, BSD ou Solaris.



## SocksCap

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

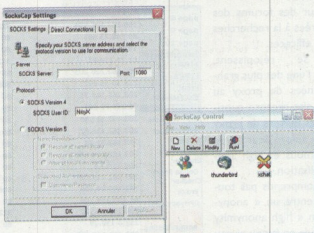
SocksCap est la solution qui va vous permettre d'être anonyme, tout comme avec proxy http mais cette fois ci sur des serveurs FTP, IRC, ICQ, MSN et bien d'autres en passant par un proxy sock.

En effet, socksCap permet de faire passer n'importe quelle application par un proxy sock.

Toute la puissance de ce programme réside 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 clients. On voit également qu'il est possible de lancer votre client mail depuis socksCap, cela permet de cacher votre réelle adresse

IP dans les mails que vous envoyez. Bref, les possibilités offertes par SocksCap n'ont de limite que celle de votre imagination !

## 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'oublions pas de souligner que des exercices pratiques vous permettront de mettre en pratique ce

I. Page d'accueil

II. Table des matières

III. Comment utiliser ce client

IV. Introduction

V. Définitions des termes clés

VI. Lexique de cryptologie

VII. Histoire de la cryptologie

VIII. Cryptographie des années 1940-1950

IX. Léon Battista Alberti

X. Jean Trithème

XI. Chiffres polyalphabétiques

1. Tableau de Trithème

2. Chiffre de Bellaso

3. Chiffre de Porta

4. Chiffre de Vigenère et variantes

A. Carré de Vigenère

B. Règles de Saint-Cyr

C. Chiffre de Vigenère

D. Décryptement du chiffre de Vigenère

E. Tableaux Kasiski (Vigenère)

F. Tableaux Kasiski (Lafont)

G. Tableaux de Kasiski

H. Tableaux de Kasiski

1. Tableaux de Kasiski

2. Tableaux de Kasiski

3. Tableaux de Kasiski

4. Tableaux de Kasiski

XII. Le tableau de Trithème

Les Allemands et de nombreux auteurs de l'époque 1800-1900 prétendent que c'est le tableau Trithème qui a inventé le carré de Vigenère. Un tel tableau (voir ci-dessous) se trouve bien dans *Arithmetica*, mais il s'agit d'un tableau de transposition et ne ressemble pas du tout au carré de Vigenère. En outre, le carré de Vigenère est complètement absent de l'ouvrage de Trithème. C'est cependant bien la première fois qu'un tel tableau apparaît.

Comment Trithème utilisait-il sa table recte ? Il chiffrait la première lettre du message clair avec la première lettre de la deuxième ligne, etc. Si le message n'y avait pas d'alphabet clair distinct, mais la première lettre du tableau servait en tant que clé. Quand il arrivait à

XVII. Cryptanalyse

A. Principes de Kasiski

B. Nombres d'alignements

C. Techniques classiques de cryptanalyse

D. Construction d'un carré

Message clair : 0 1 2 3 4 5 6 7 8 9 10  
 Message chiffré : C I K I J ; W K K M C B

Le programme javascript ci-dessous va vous permettre de voir l'entree en message non accésé (au besoin prétraiter le texte).

CHIFFRE DE TRITHÈME

Message clair : [input type="text"]  
 Message chiffré : [input type="text"]

[Chiffrer] [Déchiffrer] [Tout effacer]

que vous venez d'apprendre ; Nous recommandons donc ce site à ceux qui voudraient en savoir plus sur les multiples aspects de la cryptogra-

phie, 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.tar.gz>

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 has slack
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 -checkslack 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:$1$gDeNjPe8$gVUd.fwBNxln5pFXNhdJ0:12877:0:99999:7:::
```

# 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 déboguer ou encore des options telles que la mise en place d'un mot de passe afin de crypter le binaire et d'empêcher son exécution sans la connaissance de celui-ci.

La version actuelle est la 1.0.1 et à ce jour, il n'existe aucun moyen de reverser un binaire encrypté par cette

```
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
               ignore invalid entered password and execute junk
               not recommended (default: off)
  -i

fingerprinting options
  -S           SERIAL 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
```

méthode si on a oublié le mot de passe, attention à ne pas vous brûler les yeux ...

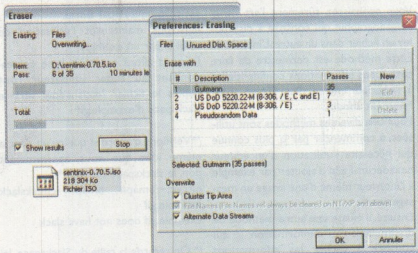
# Eraser

**URL :** <http://www.tolvonen.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 utilisés par Eraser a été élaboré à partir de l'article de Peter Gutmann ("Secure Deletion of Data from Magnetic and Solid-State Memory"). Celui-ci définit précisément comment faire disparaître toute trace magnétique d'un disque dur.

En outre, Eraser ne se contente pas d'ajouter une entrée « Erase » lors du



clic droit d'un fichier. Il comporte également un gestionnaire de tâches qui pourra vous permettre de supprimer

automatiquement les fichiers contenus, par exemple, dans un répertoire temporaire.

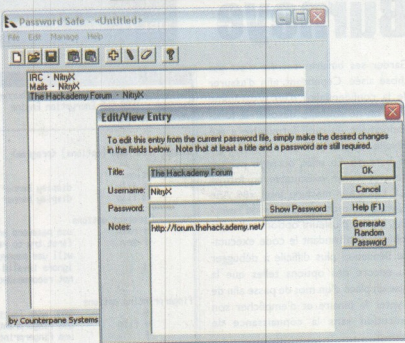
# Password Safe

**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.

Password Safe a fait l'objet de vérifications poussées afin, par exemple, de veiller à ce qu'il ne reste aucune trace d'information sensible en mémoire, après utilisation. Un développeur indépendant propose



une version Linux, similaire et compatible, qui n'a toutefois pas fait l'objet d'autant

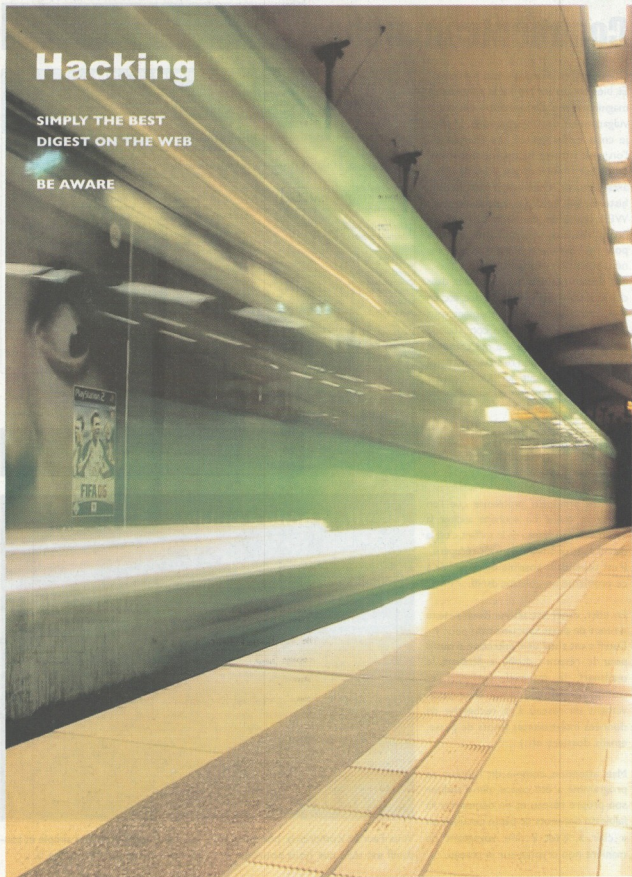
de vérifications : MyPasswordSafe (<http://www.semanticgap.com/mypsw/>).



# Hacking

SIMPLY THE BEST  
DIGEST ON THE WEB

BE AWARE



## Commentcamarche

LANGUE : Français

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 téléchargement, vous pouvez télécharger 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, évidemment, ce site est entièrement sous licence GPL !)

## 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 msgsnarf, 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 conçu afin d'auditer son propre réseau et de démontrer la faiblesse des mots de passe circulant en « clair », c'est à dire voyageant de manière non cryptée sur le réseau.

OS : Windows/Linux

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

### dsniff, la boîte à outils

- une collection d'outils permettant :
  - d'auditer un réseau,
  - de réaliser des tests d'intrusion.
- deux catégories d'outils :
  - écouter passivement le réseau
    - pour capturer des données intéressantes,
  - faciliter l'interception de trafic réseau
    - normalement non disponible à un attaquant.
- de formidables outils pour :
  - **éduquer les utilisateurs et les administrateurs,**
  - **obtenir des budgets sécurité**
    - montrez son mot de passe et son courrier électronique à votre patron ;)
- Mais surtout **n'abusez pas de ces outils !**
  - même s'ils sont portables : \*BSD, Linux, Solaris, Win32.

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

## Vers un rép. de plus haut niveau

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

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, évidemment. Et pourtant, êtes vous conscient des nombreuses possibilités offertes par ce site ?

Lors d'une recherche vous pouvez spécifier des paramètres qui parfois pourront se révéler intéressants. Par exemple, essayez de taper, "allinurl:cmd.php", dans le champ de recherche ! En effet, cela vous renvoie sur un nombre impressionnant de pages possédant une adresse composée de cmd.php, qui comme beaucoup de gens le savent se résume assez souvent à un simple script php, permettant l'exécution de commandes.

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

The screenshot shows the Google search engine interface. At the top, there's the Google logo and navigation links for Web, Images, Groups, Answers, and Actualités. Below that is the search bar with the text "Rechercher" and "Rechercher avancé". There are also links for "Rechercher dans" and "Pages : France".

The main content area is titled "Web" and lists several information resources:

- Information en direct**: L'actualité mise à jour en continu 500 sources mondiales d'Info presse
- Bibliothèque publique d'information**: Bibliothèque publique d'information (Bpi), la bibliothèque du Centre Pompidou (Beaubourg) à Paris - encyclopédique et multimedia
- Institut de l'information scientifique et technique**: Porté par le CNRS, l'INIST gère un fonds documentaire international, produit et diffuse les bases.
- Premier Ministre**: Accueil Thématique - Toute l'information gouvernementale en continu - Les chartiers - Le Gouvernement - Participez aux forums ...
- Europe.gov.fr**: Le service d'information du gouvernement de la République française propose articles, dossiers ...
- Government of Canada Site / Site du gouvernement du Canada**: The Canada Site, le Site du Canada, is a single point of access to all programs, services, departments, ministries and organizations of the Government of ...
- Internet en France**: L'action de l'état français en matière de société de l'information.

Essayez aussi [www.google.fr/linux](http://www.google.fr/linux) pour fameux Gmail qui offre un espace de stockage d'un giga : [mail.google.com](mailto: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 fonctionnements et quelques codes source agrémentent l'ensemble. Plusieurs pages sur la sécurité des systèmes et des réseaux pourront vous aider à mieux appréhender ces notions. Enfin un forum est mis à votre disposition pour éclaircir les articles, les approfondir, voire aborder d'autres sujets. Notons aussi qu'une section download avec quelques softs intéressants s'offre à vous !

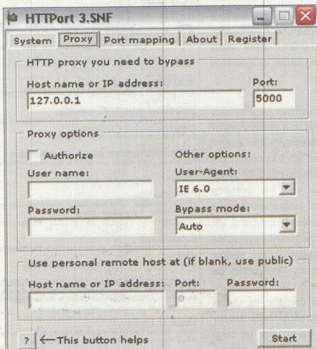
Information	Article Title	Author	Submitted
• <a href="#">E-Mail Security</a>	Wireless Hacking IRC Log	blacksun.box.ak	04 Feb 2003
• <a href="#">HTTP Protocol Security</a>	Hacking CGI - Security And Exploitation	by böiler	12 Jan 2003
• <a href="#">Linux Security</a>	Hacking Techniques: Issue #2 - Bouncing Attacks	Written by böiler for <a href="http://böiler.eyeonsecurity">http://böiler.eyeonsecurity</a> .	12 Jan 2003
• <a href="#">MS IIS Information</a>	Hacking With Javascript	böiler	12 Jan 2003
• <a href="#">Downloads</a>	AdminGuideToCracking	zen	24 Jan 2003
• <a href="#">Exploit Archive</a>	How to become a master Hacker	Christopher Klaus	24 Jan 2003
• <a href="#">Exploit Discussion</a>	Hacking step by step.	phantom	24 Jan 2003
Database Security	hacking the bios	anand bhaskar	24 Jan 2003
• (Common-sense Principles)	BACK DRIFICE 2000	nexus	24 Jan 2003
• Places that viruses and trojans hide on start up	GUIDE FOR BEGINNERS	unknown	24 Jan 2003
• Step-by-Step Guide to Using the Security Configuration Tool Set	Breaking Windows 98 Passwords		
• Improving the Security of Your Site by Breaking Into It			
• Domain Name Robbery			
• XDCC - An .EDU			

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 !

## Httpport

OS : Windows  
URL : <http://www.httthost.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 « passer » 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, ressources qui pourrait rendre service très peu gourmand en mémoire et en 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 référence 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

## Security Related Papers

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

manque de mise à jour depuis près d'un an, un très bon site.

A noter que minithins.net est en langue

française. 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 certaine sont en français. Bien sûr, ceux-ci ont été soigneusement sélectionnés et classés 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 précieuse 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,

**Textes sur le hacking - OUAH Site**

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

<ul style="list-style-type: none"> <li><a href="#">Textes en français (90)</a></li> <li><a href="#">Buffer Overflow (90-7)</a></li> <li><a href="#">Format Bugs (22)</a></li> <li><a href="#">Logging (17)</a></li> <li><a href="#">Sniffing (31)</a></li> <li><a href="#">Manuels d'assembleur (24)</a></li> <li><a href="#">Backdoors / Rootkits / Trojans (27)</a></li> <li><a href="#">Worms / Viruses (24)</a></li> <li><a href="#">Script Kiddies (14)</a></li> </ul> <p>Total == 683</p>	<ul style="list-style-type: none"> <li><a href="#">Vulnérabilités (79+1)</a></li> <li><a href="#">Port Scanning (16)</a></li> <li><a href="#">Sniffing / Hijacking (32+1)</a></li> <li><a href="#">Denial of Service (DoS) (15)</a></li> <li><a href="#">Firewalls / Routeurs (26)</a></li> <li><a href="#">Détection d'IDS (24)</a></li> <li><a href="#">Loadable Kernel Modules (LKM) (20)</a></li> <li><a href="#">Web Vulnerabilities (37+2)</a></li> <li><a href="#">Intrusion Detection System (IDS) (14)</a></li> </ul>
---	--

[\[Home\]](#) [\[Textes sur le hacking\]](#) [\[Evènements\]](#) [\[Forum\]](#) [\[Listes\]](#) [\[Liens\]](#)

actuelle, d'informations pointues pour les plus chevronnés. A noter que

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

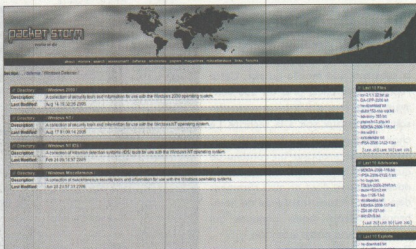
## Packetstorm

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 farfameuse 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.

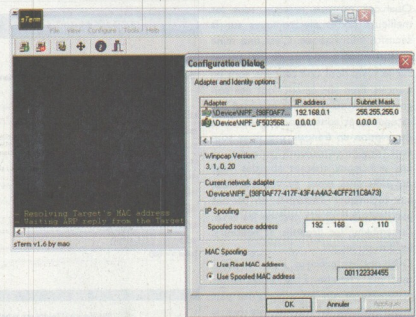
Et enfin, la partie « miscellaneous » qui vous réserve également de bonne surprise. A la carte : programmation, virus, phreaking et même humour informatique.

## 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 votre 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



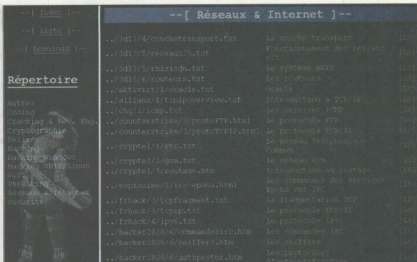
avec parcimonie : après tout, si des règles de filtrage existent sur un firewall qui vous embête, pensez que c'est avant tout pour votre sécurité.

# Frenchzines

**LANGUE :** Français  
**URL :** <http://www.frenchzines.tk>

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

Au-delà de son apparence, le site 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>

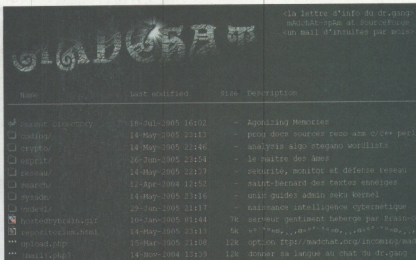
Ho mon dieu ! Quel ne fut pas ma stupéfaction en découvrant ce site ! Un site de Hackeuses qui n'ont pas froid aux yeux ! Vous avez bien lu ! L0t3k est un site (apparemment) créé par de jeunes demoiselles adeptes de l'Unix, du Backdooring et du Buffer Overflow (Sans arrières pensées). Au programme : 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 toolz. 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

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 forcément une priorité (navigation dans les rubriques en mode texte), le contenu lui est bien présent. Madchat c'est l'une des meilleures sources de tutoriaux disponibles gratuitement en téléchargement. Les contributions en français et en anglais peuvent offrir une base non négligeable d'informations aux débutants comme aux confirmés. Parmi les rubriques les plus fournies, on trouve

**LANGUE :** Français / Anglais  
**URL :** <http://www.madchat.org>



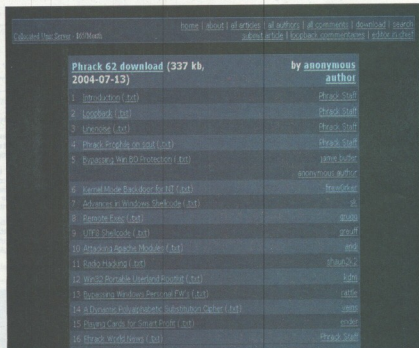
entre autre la sécurité admin et réseau sécurisée orientée réseau. De plus, si vous vous en sentez le courage et le niveau, les contributions sont bien sûr possibles. A explorer dans tous les sens.

## Phrack

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,

**LANGUE :** Anglais  
**URL :** <http://www.phrack.org>



titre ou commentaire. Pour résumer, la documentation nécessaire pour devenir un 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 pourrait être qualifié de déviant aux yeux de certains, thc.org (site de la team The Hackers Choice) n'en est pas moins un très bon site de hackers 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 ! Parmi eux, nous pouvons citer AMAP ou YMAP qui ont déjà eu dans le passé, droit à quelques lignes à travers diverses publications de The Net secrets.

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

En parcourant cette rubrique, vous pourriez par exemple en savoir davantage sur le fameux projet Echelon de la NSA, sur la cryptographie, sur les LKM

**The Hacker's Choice**

**THC Releases**

Welcome to the THC release section. Below you will find the collection of THC software applications. It includes sophisticated network analysis and penetration and weak cryptographic utilities that manage, disrupt or collapse or downgrade a credit card numbers and a lot of other interesting stuff for the security expert's pleasure.

- THC-Hydra (4 Nov)**  
Version: 3.0 - [Download](#) - [Source](#) - [Size: 34276](#)
- THC-4Vdo (6 Oct)**  
The 4Vdo is the best password login hacker for Samba, FTP, POP3, IMAP, Telnet, HTTP, Auth LDAP, NNTP, SSH/RC, VNC, RQ, Socks), PCAN's Cines and more. Includes SSL support and a part of Netwin. Has the proxy's workflow to download W3.2, Fida and AMAP binaries. Changes in 5.3: Finally there is a web both a1 and module, and NTLM support for proxy, snmp and stmp-auth!
- THC IPv6 Attack Toolkit**  
Version: 3.0 - [Download](#) - [Source](#) - [Size: 10414](#)
- THC-Scan**  
Version: 3.0 - [Download](#) - [Source](#) - [Size: 13366](#)

For the 10th anniversary of THC, here is a special update to THC-Scan: Recompiled in rust with modern compilers without problems. A new version of world's best free multiplatformer, THC-Sc on v2.0! It works under OS/390, Win9x/NT/XP and all OS/390 emulators (WIN, en all other processors. CPUID, dualstack support, completely rewritten some, correct, with scanning, large pool of analyzing tools. Included a C++ shell tool source code.

**Downloaded Software**

- THC-4Vdo v3.01 (4178)
- THC-4Vdo v3.0 (4178)
- THC-Scan v2.0 (4400)
- THC-Scan v3.0 (4400)
- THC-Sc on v2.0 (4400)
- THC-Sc on v2.0 (4400)
- THC-Sc on v2.0 (4400)
- THC-Sc on v2.0 (4400)
- THC-Sc on v2.0 (4400)
- THC-Sc on v2.0 (4400)

**Search Software**

Search Software

Yes  No

Yes  No

Yes  No

Yes  No

et sur bien d'autres domaines encore. la partie /root/phun qui contient tout. Vous aurez aussi la possibilité de visiter les documents ... fun de la team ! ;)

# Frsirt

LANGUE : Français  
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 récentes en vous inscrivant à leur mailing liste. Ce site est donc une excellente alternative à Security Focus pour se tenir informé

**Frsirt**

Actualités de Sécurité

**Vous recrutez ?** Recevez des candidats

**Liste des vulnérabilités les plus importantes**

- 06.07.2006 - Adobe Reader/Flash Player Code Execution and Denial of Service Vulnerability
- 06.07.2006 - IBM Rational Policy Services Adapter Client Access Data Buffer Overflow Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability
- 06.07.2006 - Microsoft Office Word Remote Code Execution Vulnerability

**Recrutement de développeurs**

- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability
- 06.07.2006 - NetScout Systems Web Proxy Code Execution and Denial of Service Vulnerability

**Frsirt VMS™**  
Vulnerability Monitoring Service

quotidiennement des différents en français. Bref, un site à bookmarker exploits et advisories parus et tout ça 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 côté un peu plus commercial depuis son rachat par Symantec (pour 75 millions de dollars), le site n'en reste pas moins intéressant.

Securityfocus mets à disposition 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 à différentes listes : Linux Security News, Focus on BSD, Firewalls, Microsoft Security News, Secure Programming et j'en passe. Au total une trentaine de sujets différents

vous sont proposés, il y a donc de quoi satisfaire tout le monde ! Au-delà du « côté base de vulnérabilité et liste de diffusion », Securityfocus dispose d'un nombre intéressant d'outils. Je vous

invite 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 :** Français  
**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 [securelabs.com](http://www.securelabs.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 télé-

chargeable 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'amusez rarement à modifier un numéro de port (surtout pour les services qu'ils ouvrent à Internet), mais

```

xterm
-----
Etern Font Background Terminal
1 nmap -iR -f -Pn -mssql2008 --amap/
Starting nmap 3.20 ( http://www.insecure.org/nmap/ ) at 2005-09-07 04:12:01 EDT
Internet (ip) ports on www.segfault.seg.net (10.01.10.01)
(The 1153 ports scanned but not shown below are in state: closed)
Host: 10.01.10.01
22/tcp open  ssh
25/tcp open  smtp
135/tcp closed locustman
567/tcp open  subversion

Host scan completed -- 1 IP address (1 host up) scanned in 13.243 seconds
1 nmap -iR -f -Pn -mssql2008 --amap
nmap 3.2.2 (www.thc.org) started at 2005-09-07 04:27:10 -- HPLIATION HPLI mode

Probed on 10.01.10.01220/tcp watches ssh
Probed on 10.01.10.01220/tcp watches subversion
Probed on 10.01.10.01225/tcp watches smtp
Probed on 10.01.10.01250/tcp watches smtp

Identified ports: none.

nmap 3.2.2 finished at 2005-09-07 04:27:16
  
```

il arrive que l'on souhaite identifier le service tournant derrière un port évilé... AMAP fera cela très bien, très vite et très facilement !

Les protocoles supportés nécessitant un envoi sont : dns, ftp, http, jrm1, ldap, ms-ds,

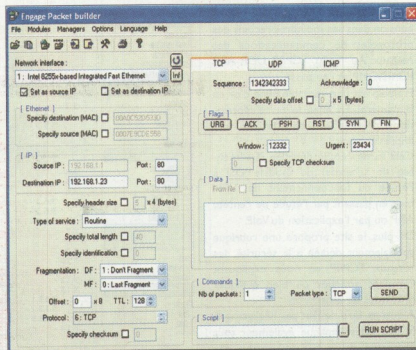
ms-remote-desktop-protocol, ms-sql, netbios-session, ntp, oracle-tns-listener, rpc, sap-r3, smtp, snmp-public, ssl et x-windows. En ajoutant les protocoles identifiables dès la connection, on obtient un total de 147 protocoles différents supportés !

# 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, EPB 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 paquets 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.

```

C:\WINDOWS\system32\cmd.exe

C:\unzipped\Fport>Fport /p
Fport v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid Process          Port Proto Path
348 xchat              -> 113  TCP  C:\Program Files\xchat\xchat.exe
1144          -> 135  TCP
4 System            -> 139  TGP
4 System            -> 445  TCP
820          -> 1026 TCP
1320 putty             -> 1038 TCP  D:\putty.exe
2000 Firefox           -> 1052 TCP  C:\Documents and Settings\Trenblay Jeannot\
Mes documents\Progs Install\Firefox.exe
2008 Firefox         -> 1053 TCP  C:\Documents and Settings\Trenblay Jeannot\
Mes documents\Progs Install\Firefox.exe
340 xchat              -> 1335 TCP  C:\Program Files\xchat\xchat.exe
532 msnmnggr         -> 1343 TCP  C:\Program Files\MSN Messenger\msnmnggr.exe
532 msnmnggr         -> 1348 TCP  C:\Program Files\MSN Messenger\msnmnggr.exe
532 msnmnggr         -> 1349 TCP  C:\Program Files\MSN Messenger\msnmnggr.exe
532 msnmnggr         -> 1350 TCP  C:\Program Files\MSN Messenger\msnmnggr.exe
532 msnmnggr         -> 1351 TCP  C:\Program Files\MSN Messenger\msnmnggr.exe
1020 putty             -> 1392 TCP  D:\putty.exe
    
```

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 : Français

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 côté interac-

Général		Entête IP par_SebF
Accueil		
Recherche		
Les News	1 - Définition du protocole	
Participation	2 - Structure de l'entête	
Les partenaires	3 - Définition des différents champs	
Les modèles	3.1 - Vég.	
TcpIp	3.2 - Ihl	
Osi	3.3 - Service	
Osi-TcpIp	3.3.1 - Prorité	
X-200	3.3.2 - Offset	
Les Rtc	3.3.3 - Offset	
	3.3.4 - Protocol	
	3.3.5 - Code	
	3.3.6 - Mbz	
Les entêtes	3.4 - Longueur totale	
Entête Arp	3.5 - Identification	
Entête Ip	3.6 - Flags	
Entête Icmp	3.6.1 - Reserved	
Entête Icmp	3.6.2 - DF	
Entête Tcp	3.6.3 - NP	
Entête Udp	3.7 - Position fragment	
Le fonctionnement	3.8 - TTL	
Nat	3.9 - Protocole	
Routeur	3.10 - Checksum	
Sous-réseaux	3.11 - Adresse IP source	
	3.12 - Adresse IP destination	
Les services	3.13 - Options	
Dhcp	3.13.1 - Code	
Dns	3.13.2 - Classe	
Tcp	3.13.3 - Numéro	
Voin	3.14 - Routage	

tif 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 !).

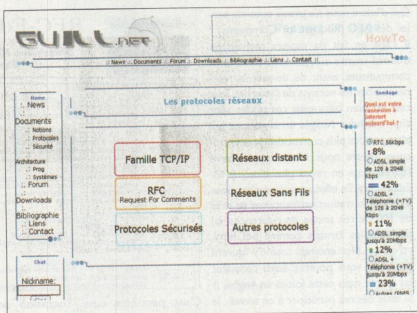
# Guill.net

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>

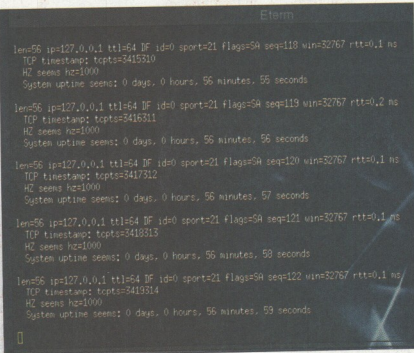
Peu d'entre nous n'ont jamais entendu parler de Hping et c'est bien normal. En effet, sa puissance fait toute sa popularité dans le monde de la sécurité des réseaux.

Hping est un outil de création et d'analyse de trafic TCP/IP.

Hping est un outil complet et peut par exemple servir à tester la sécurité de votre firewall, tester le fonctionnement de votre réseau, s'entraîner 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 etheareal. En effet lorsqu'on génère du trafic avec Hping il est impératif d'analyser les réactions du réseau ou du système cible.



Les fonctionnalités offertes 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.

RFC-Editeur.org		toutes les RFC traduites en Français	
	Un peu d'éthique... INFO - To be "Sc" the Internet Ce document attend un lecteur, contacter l'auteur si ce document vous intéresse.	Y. Bouhal	73 Ko 54 Ko
RFC 1775	IBTF - Le TAG de l'IETF Un guide à l'usage des nouveaux participants aux travaux de l'IETF. Ce RFC est rendu obsoleète par le RFC3160 - FTLT (aussi en vfr).	Immanuel Jossé	15 Ko 28 Ko
RFC 1718	PPP-TRANS - Transmission PPP Fliable Ce document définit une méthode pour la négociation et l'usage du mode numéroté, pour fournir un lien série fiable.	Yves Lescoff	22 Ko 40 Ko 31 Ko
RFC 1663	PPP-HDLC - PPP dans un trameage similaire à HDLC Ce document décrit l'utilisation du trameage comme HDLC pour les paquets encapsulés par PPP.	Yves Lescoff	55 Ko 106 Ko 77 Ko
RFC 1602 STD 51	PPP - Point-to-Point Protocol Le Protocole PPP fournit une méthode standard pour transporter des datagrammes multiprotocoles au-dessus	Valéry G. Fremeaux	193 Ko 212 Ko 182 Ko

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

## Nmap

**OS :** Unix, Windows  
**URL :** [www.insecure.org](http://www.insecure.org)

Qui ne connaît 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.

Ceci peut être pratique si on se base sur le fait qu'un admin ne pourra analy-

```
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
-> 64.102.9.104:80 (distance 0, link: ethernet/modem)
192.168.0.1:1401 - Windows 2000 SP4, XP SP1
-> 64.102.9.104:80 (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
```

ser une quantité impressionnante de log et contacter un à un le fai de chaque IP. Nmap, un outil à utiliser sans modération !

# P0f

D'abord, P0f est l'outil de fingerprinting passif le plus évolué à ce jour.

Le fingerprinting passif consiste à détecter le système d'exploitation de machines dialoguant sur le réseau en ne faisant qu'écouter le trafic. Ainsi, aucun paquet n'est envoyé vers les machines, ce qui 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 P0f plus fiable encore, l'auteur nous invite à augmenter la base de fingerprint en visitant la page de son site située à l'URL <http://camtuf.coredump.cx/p0f-help/>.

OS : \*BSD, Linux, Windows

URL : <http://camtuf.coredump.cx/p0f.shtml>

```
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 langages (principalement : C, C#, Java, VB). Enfin une synthèse est présentée pour clore l'analyse.

Comment ça marche


100% sur HTTP

Service telnet

Programmation

RFC 1.1 en anglais







RFC 1.0 en français



protocole HTTP

Le Protocole HTTP (hypertext transfert protocol) sert (entre autre) au dialogue entre votre navigateur Web et un serveur sur internet.

Vous trouverez dans cette section quelques informations pour travailler sur le protocole HTTP.

<p><b>Comment ça marche</b></p> <p>100%  <b>http</b> : une introduction aux mécanismes du protocole HTTP</p>	<p><b>Débuter sur HTTP</b></p> <p>100%  <b>http</b> : une introduction plus complète aux mécanismes du protocole HTTP pour comprendre les messages échangés</p>
<p><b>Session telnet</b></p> <p>100%  <b>telnet</b> : il est très simple de voir comment fonctionne le protocole à travers une session telnet</p>	<p><b>Programmation</b></p> <p>100%  <b>Codes</b> : Des exemples de programmes (java, langage C, visual c++, C#) pour travailler sur le protocole HTTP. Après ça vous n'aurez pas d'excuse pour ne pas écrire votre programme</p>
<p><b>Liens</b></p> <p>100%  <b>www Consortium.</b></p>	<p><b>RFC 1.1 en anglais</b></p> <p>100%  <b>RFC 1.0 en français</b></p>

Bien entendu, si vous voulez aller plus loin sur l'étude d'un protocole, rien de

tel que la RFC en français directement disponible sur le site. Bonne visite!

## 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 débiter. Je lui ai proposé le Python qui est simple et complet pour débiter. 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

```

Fichier  Édition  Affichage  Terminal  Onglets  Aide
>>> a=sniff(filter='tcp and ( port 25 or port 110 )',
prn=lambda x: x.strftime('*%IP.src%>TCP.sport% -> %IP.dst%:%TCP.dport
% %s,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@p
p2-1.free.fr>
192.168.8.10:47226 -> 213.228.0.14:110  A :
192.168.8.10:47226 -> 213.228.0.14:110  PA : USER toto
213.228.0.14:110 -> 192.168.8.10:47226  A :
213.228.0.14:110 -> 192.168.8.10:47226  PA : +OK
192.168.8.10:47226 -> 213.228.0.14:110  A :
192.168.8.10:47226 -> 213.228.0.14:110  PA : PASS tata
213.228.0.14:110 -> 192.168.8.10:47226  PA : -ERR authorization failed
    
```

de manière interactive ou scriptée, ture et les nombreuses démos du site). assez simplement (voir la séance de sniff Packages disponibles pour RedHat et Debian.

## 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 possibilités que vous offre ce soft. Admirez 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.ê....0....
0x0010  d41b 28fc 0a8a
0015 dc77 67ee 7b1d 4ffe
..(.....wg.{}.0.
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 utilisations 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-crypté), vérifier l'efficacité de votre forgeur de paquets et j'en passe...

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

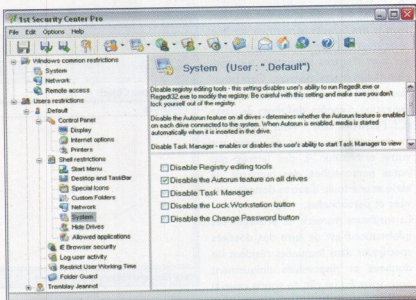


# 1st security

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

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

L'application de règles différentes pour chaque 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), sstunnel (établissement d'un tunnel ppp par dessus une connexion ssl) et bien d'autres choses utiles en libre téléchargement. Comme quoi toutes les boîtes de sécurité ne

font pas que se gaver de la recherche en sécurité réalisée gratuitement par des hackers. Tout cela est présenté de manière claire et un index permet d'accéder rapidement aux documents

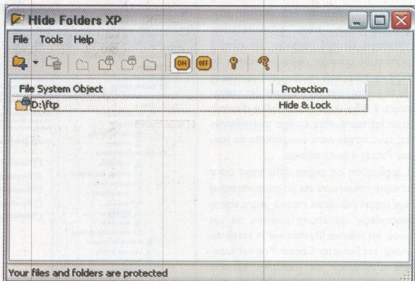
concernant un thème particulier. Un bel exemple qui, nous l'espérons, sera pillé par les autres entreprises de sécurité... du point de vue de la philosophie du site bien sûr ! ;)

## 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 pourrait inclure l'information financière, l'information d'impôts, des mots de passe (Cf. Password Safe - Pour enregistrer en sécurité vos mots de passe sur votre ordinateur -), des lettres, des notes personnelles, des numéros de série et une foule d'autres données privées et personnelles.

La meilleure manière de protéger ces informations est de faire des dossiers spécifiques dans 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 révèle 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 patches kernel, les dernières vulnérabilités, les stats des attaques, les outils de sécurité (firewall, IDS, monitoring, tracking...). Et ce n'est qu'une partie seulement ;) ! De nombreux conseils et astuces sont aussi disséminés sur le site et au fil des pages on peut apprendre à mieux connaître son OS préféré. Ce site a de quoi satisfaire les plus exigeants et permet de trouver rapidement les meilleurs sites sur tous ces sujets.

<http://www.Linux-Sec.net>

### Kernel Hardening

#### Minimum Kernel Hardening

- Protect your stack from buffer overflow exploits

Kernel.org Linux Kernel Sources  
LinuxDoc.org Kernel-HOWTO  
Redhat.com Upgrading the Kernel

- Download, Compile and Install the latest kernel
  - Turn off modules during kernel config compile
  - Turn off unnecessary kernel options during kernel config compile
  - Turn off proc files stem during kernel config compile
- Apply Additional Kernel Security Enhancements
  - Apply OWL
  - Apply LIDS
  - Apply libSafe
  - Apply StackGuard or StackShield

- [Hardening Tightening](#)
- [Hardening HOWTO](#)
- [Security Policy](#)
- [Linux Distros](#)
- [Distro Patches](#)
- [Kernel-Patches](#)
- [Dedicated Servers](#)
- [Firewalls](#)

# 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 certain nombre de services pour que cet adage devienne pleinement une réalité. Je ne saurais trop vous conseiller de faire un tour sur ce site, qui contient l'une des meilleures bases de données dans ce domaine pour les machines fonctionnant sous Linux.

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.

The screenshot shows the Linux Security website interface. At the top, there's a search bar and navigation tabs for Home, Archives, Features, and Newsletter. Below that, a list of articles is displayed under the 'HOWTO/FAQS' section. The articles listed are:

- Networks in NSA Security: Enhanced Linux** (166 views) - Break through the complexity of SE Linux with a working example that shows how to add SE Linux protection to a simple network server.
- Apache 2 with SSL/TLS** (2096 views) - This article begins a series of three articles dedicated to configuring Apache 2.0 with SSL/TLS support in order to ensure maximum security and optimal performance of the SSL communication. This article, part one, introduces key aspects of SSL/TLS an
- Installing Fedora 2** (1270 views) - For the Linux novice, installing a new build can be a daunting task. This chapter will help you figure out what you need and what 2004 you don't. Even Linux pros will find some tips on configuring a build that can help enhance security.
- Securing Linux Production Systems** (3607 views) - This article is a practical step-by-step guide for securing Linux production systems. It shows how to meet basic security requirements for Linux systems that need to pass security audits. This guide also discusses some Linux security steps that come

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.msp>

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 inexistant, la configuration des mises à jour automatiques, le type de système de fichier ou encore le nombre d'administrateurs sur l'ordinateur ainsi que d'autres subtilités moins connues. Le rapport présenté à la fin de l'analyse est intéressant et même pédagogique. En effet, il donne non seulement le résultat, positif ou négatif, des nombreux tests, mais aussi le détail des res-

The screenshot shows the Microsoft Baseline Security Analyzer (MBSA) interface. The window title is "Microsoft Baseline Security Analyzer". The main area displays a security report with a score of 100 (100%). The report lists several items that are up to date, such as Windows, Microsoft VM, and Media Player. The interface is in French.

**Afficher le rapport de sécurité**

Guide de la : Score (le plus en premier)

État	Score	Description	Action
✘	Mises à jour de sécurité pour MDAC	Comment corriger le problème	Annule les ressources analysées
✘	Mises à jour de sécurité pour Windows	Comment corriger le problème	Annule les ressources analysées
✔	Mises à jour de sécurité pour Microsoft VM	Aucune mise à jour de sécurité critique n'est attendue.	Annule les ressources analysées
✔	Mises à jour de sécurité pour Windows Media Player	Aucune mise à jour de sécurité critique n'est attendue.	Annule les ressources analysées
✔	Mises à jour de sécurité pour MDAC	Aucune mise à jour de sécurité critique n'est attendue.	Annule les ressources analysées

**Résultats de l'analyse de Windows**

Poids de vulnérabilité

Score Catégorie Résultat

100 100 Le service de mise à jour automatique n'est pas configuré

Rapport de sécurité précédent Rapport de sécurité suivant

sources 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

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

trouvez le guide du légendaire Microsoft IIS, d'IE 5.5 et même de Netscape. Bien entendu, d'autres termes sont abordés. En tout cas, pas moins d'une quarantaine

de guides de sécurité et de fichiers de configuration sont disponibles. Cependant, aucun logiciel libre n'est à l'affiche...

## 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 sûr d'être paré contre les attaques de base ? Et bien, voici un logiciel qui répondra à vos attentes. PC Sécurité Test va simuler différentes attaques simples pour évaluer la fiabilité de vos outils.

Au menu : contrôle et scan des ports, inscription dans la base de registre, simulation de code de virus 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 risquez pas d'être perdu. Une rubrique d'aide est à la disposition de ceux qui voudraient en savoir plus.

Ce logiciel n'a pas la prétention de tester toutes les techniques connues, mais

seulement les plus utilisées. Redoutable pour convaincre quelqu'un en deux clic

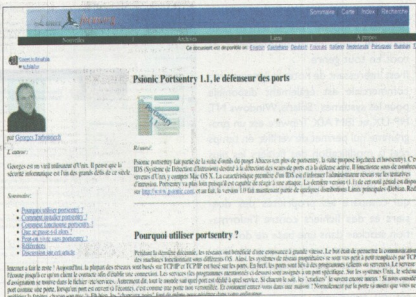
qu'il devrait changer de protection... ou de système d'exploitation ;)

# 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 com-



mande lorsqu'un scan est détecté. essentiel par rapport aux programmes passifs qui se contentent seulement de détecter les scans en cours.

# Rootkithunter

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

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 – notamment 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](http://www.chkrootkit.org)), cet outil peut s'avérer très utile si vous craignez que votre

```

/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 'AjoKit'... [ OK ]
Rootkit 'aPa Kit'... [ OK ]

```

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

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, rap-

**Tripwire Enterprise** | IT change auditing software

Tripwire Enterprise audits changes to directory file systems, monitoring these changes with thorough checks and reporting on change activity. It operates independently of any administrative tools used to manage and make changes, providing an unbiased accounting of all changes across the serviceable. With Tripwire Enterprise, you know each and every change is either authorized or under investigation by means of automated techniques.

**EXPLORE TRIPWIRE ENTERPRISE TRIAL KIT | DOWNLOAD NOW**

Experience Tripwire Enterprise 5.0 with a Trial Kit. Test drive it now!



**Key Benefits**

- Captures thousands of server file systems, desktop file systems, directory servers, databases and network device configuration files in a known good state, and then automatically performs integrity checks that compare current states against these baselines to detect changes.
- Delivers a single point of change control for auditing changes across your entire IT infrastructure.
- Provides 24/7 independent, subscription-revoked change detection for servers of all sorts (e.g. files, directories, registry settings, directory server objects, and configuration files).
- Provides the necessary evidence for enforcement of change and configuration management policies.
- Enforces security with an unbiased accounting of any and all changes across the entire track regardless of when, where, or how the change was made.
- Supplies a rich change archive for a thorough investigation of any change, including who made the changes, what changes were made, when the changes were made, and how the changes were made.
- Produces a wide array of reports and online dashboards that can be tailored to any environment to show change status and the effectiveness of your change management processes.

**PRODUCT DETAILS**

Sample Reports  
Product Overview  
File Servers & Desktop Component  
Directory Servers Component  
Network Devices Component  
Database Component  
System Resources Component  
FAQ

**PURCHASE TRIPWIRE**

Contact our sales consultants for more information. [More >](#)

**DEMO**

Take a five minute to see what Tripwire Enterprise is all about. [More >](#)

**WHITEPAPER**

Can you prevent control? Read this to prove IT integrity. [More >](#)

**WEBCAST**

Knowledge is Power. Learn more about Tripwire and the industry it serves and orders. [More >](#)

**EVALUATIONS**

Test drive. Try an evaluation version of our software.

ports...) 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 pen-

dant 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.

**Anti Virus section**

- Articles & Tutorials
  - Authentication, Access Control & Encryption
  - Content Security (Email & FTP)
  - Firewalls & VPNs
  - Intrusion Detection
  - Misc Network Security
  - Viruses, trojans and other malware
  - Web Server Security
  - Windows 2003 Security
  - Windows Networking
  - Windows OS Security
  - Wireless Security
- Authors
- Email Security Test
- Event Log Scan
- Links
- Message Boards

### Anti Virus section

**\*\*\* Virus Warnings**

<p><b>HIGH RISK</b></p> <p>MyDoom.L (Jul 26)</p>	<p><b>MEDIUM RISK</b></p> <p>Bagle.AK (Aug 31)</p> <p>MyDoom.M (Aug 16)</p> <p>Lovgate.AJ (Jul 08)</p> <p>Zafi.B (Jun 14)</p> <p>Netsky.B (Feb 18)</p> <p>Swen.A (Sep 18)</p>	<p><b>LOW RISK</b></p> <p>Bagle.AI (Aug 09)</p> <p>Bagle.AH (Jul 19)</p> <p>Bagle.AF (Jul 18)</p> <p>Bagle.AE (Jul 16)</p> <p>Netsky.P (Mar 30)</p> <p>Netsky.Q (Mar 25)</p> <p>Netsky.D (Mar 01)</p>
--	---	---

**NORMAN**  
Virus Warnings

**\*\*\* Anti Virus White Papers**

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

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, patches et spam, qui vous permettront de télécharger et d'installer les outils les

**WINDOWS SECURITY**  
MSFT Security Support: Christian Rasmus, Tel: 3272 / 3242

Windows @ EPFL

Procédure en cas d'infection / Disinfection procedure

Si vous êtes infecté par un virus, voici les quelques étapes communes à effectuer pour se désinfecter et se protéger au maximum d'une future attaque.

Si you are infected by a virus, here is common steps for disinfect your computer and protect it against a future future attack.

Si vous pouvez effectuer la plus-part des points suivants, il est nécessaire de disposer des droits administrateur sur votre machine, si ce n'est pas le cas, contactez votre administrateur informatique.

If you can't do the following steps, it is necessary to have administrator rights on your computer, if it is not the case, contact your administrator.

- Lancez Windows Update pour contrôler les dernières mises à jour disponibles (patches) et, le cas échéant, les installer automatiquement.
- Lancez l'outil pour contrôler et nettoyer votre machine.
- Installez le dernier anti-virus Windows 7 à jour à 100% ou si vous utilisez un autre produit, vérifiez que votre anti-virus est à jour et automatisé.
- Vérifiez que les comptes locaux administrateur (ou administrateur) ont quand possible bien un mot de passe et que ce dernier ne soit ni vide, ni trop simple (1234, admin, etc.). Car beaucoup de virus rentrent dans votre machine comme ça.
- Lancez Windows Update to control the last updates available (patches) and, if necessary, to install them automatically.
- Launch the tool to control and clean your machine.
- Install the last antivirus (Windows 7 is 100% or if you use another product, check your anti-virus is up to date and automatic update available).
- Check the local administrator account (or administrator) and if you do not have a blank password or the same as: 1234, admin, etc... Because some virus use this way to enter your computer.

Pour certains virus, des actions supplémentaires sont peut-être nécessaires. Un article spécifique est dans ce cas disponible, il suffit de consulter la rubrique [patches](#) à gauche.

For some virus, additional actions are perhaps necessary. In this case, specific article are available, please consult the heading patches link on the left.

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 crackeur 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 ont révélé qu'ARCHPR pouvait tester jusqu'à 15 millions de possibilités à la seconde.

Notons également que les développeurs de ARCHPR ne se sont pas arrêtés au cracking d'archives mais ont aussi développé des crackeurs 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 ;).

Password successfully recovered!

Advanced Archive Password Recovery statistics:

Total passwords	200 237 803
Total time	30s 30ms
Average speed (passwords per second)	6 666 148
Password for this file	qwerty
Password in HEX	71 77 65 72 74 79

Save... OK

Range Length Dictionary Plain-text Auto-save Options Advanced

Brute-force range options

- All characters (A-Z)
- All lowercase (a-z)
- All digits (0-9)
- All special symbols (P.S. 1)
- Space
- All printable

Status window

```

23/08/2005 17:34:03 - Auto-save dictionary not defined. Using path: D:\
23/08/2005 17:34:03 - Starting brute-force attack...
23/08/2005 17:34:33 - Password successfully recovered!
23/08/2005 17:34:33 - 'qwerty' is a valid password for this file
    
```

Current password: qwerty Average speed: 6 666 369 p/s  
Time elapsed: 30s Time remaining: 15s  
Password length = 6, total: 308 915 776, processed: 200 237 803  
64%

ARCHPR version 2.20 (c) 1997-2003 ElcomSoft Co. Ltd.

## 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.

Cmospwd est ici le logiciel qui 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

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

Usage: cmospwd [/k[de|fr]] [/d]
cmospwd [/k[de|fr]] [/d] [/r[w] cmos_backup_file restore/loop
File
cmospwd /k kill cmos
cmospwd [/k[de|fr]] /w[01]* execute selected module
/k/fr french AZERTY keyboard, /k/de german QWERTY keyboard
/s to dump cmos
/wG010011 to execute module 3,6 and 7

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

recupérer, 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/](http://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 :

```
C:\WINDOWS\system32\cmd.exe
C>unzipped\john-16w\john-16-run>john.exe
John the Ripper Version 1.6 Copyright (c) 1996-98 by Solar Designer

Usage: john [OPTIONS] [PASSWORD-FILES]
-single "single crack" mode
-wordlist FILE read words from FILE or stdin
-rules enable rules for wordlist mode
-incremental[:MODE] incremental mode [using section MODE]
-external[:MODE] external mode or word filter
-stdout[:LEMIN] no cracking; just write words to stdout
-restore[:FILE] restore an interrupted session [from FILE]
-session[:FILE] set session file name to FILE
-status[:FILE] print status of a session [from FILE]
-makechars[:FILE] make a charset; FILE will be overwritten
-chose show cracked passwords
-test perform a benchmark
-users[:[-LOGIN|UID]...] load this (these) user(s) only
-groups[:[-IGIDI]...] load users with this (these) group(s) only
-shell[:[-SHELL]...] load users with this (these) shell(s) only
-loads[:[-COUNT] format: NAME (DES/BD1/PDS/BF/AFS/LM) force ciphertext format NAME
-save mem[:LEVEL] enable memory saving, at LEVEL 1..3

C>unzipped\john-16w\john-16-run>
```

\*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.



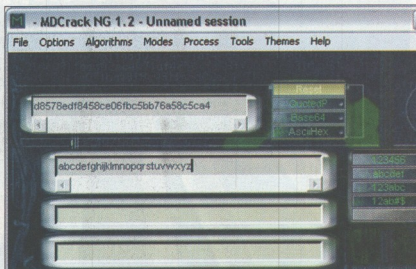
# Mdcrack

Nous voilà face au cracker de MD5 considéré comme étant le plus puissant en la matière: MDCrack.

Les MD5 servent surtout à vérifier l'intégrité 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 hashes correspondent, le mot de passe est valide.

OS : Windows, Unix

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



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)

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'environ 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 :).

LANGUE : Anglais

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

### MD5 Online Cracking

using Rainbow Tables

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

#### [NEWS]

- Any company or individual who would like to purchase this project (website, domain, tables, 30 000 results archive etc.) drop a line to info [ at ] passcracking.com.

- Table benchmark tests:

- 20 hashes on P4, 60GB, 512 RAM - all hashes are found - 773 minutes (12.8 hours) [\[results\]](#)
- 20 hashes on P4, 60GB, 512 RAM - no hashes are found - 443 minutes (7.4 hours) [\[results\]](#)

- Added two frequently asked questions with answers - about distributed variant of the project and about public availability of the Rainbow tables. See below.

- Going at full speed (~115 hashes / 24 hours).

- This project has been [restarted](#) - so the waiting line to crack hashes has increased rapidly.

## Administration & développement



L'ADMINIS-  
TRATION ET LE  
HACKING SONT  
LES DEUX FACES  
DU MEME TOKEN

! REMEMBER !

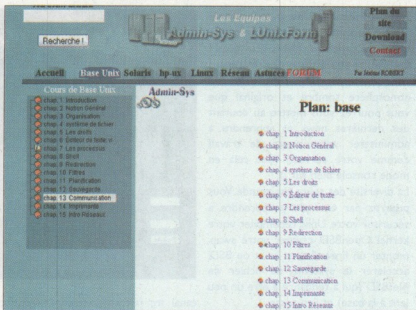
# Admin-sys

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

Admin-sys.com vous offre l'opportunité de résoudre vos problèmes d'administration grâce à sa documentation complète. Vous pourrez donc apprendre, comprendre et maîtriser le fonctionnement de Linux ou de Solaris. Par exemple : les bases essentielles du système Unix, mettre en place un système RAID sous Solaris, faire des sauvegardes sous hpux, et même quelques notions de sécurité. Ainsi, les débutants comme les initiés pourront être satisfaits de leur visite sur ce site car ils trouveront toujours quelques astuces pour les aider à surmonter leurs petites défaillances...

Admin-sys.com est le fruit d'un travail

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



de passionné qui désire offrir au monde l'administration efficace de son système et de les ressources nécessaire à une administration efficace de son système et de son réseau.

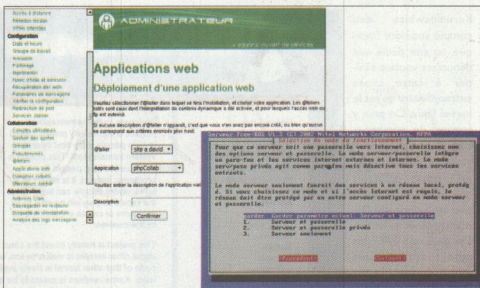
# FreeEOS

FreeEOS est une solution basée sous Gnu/Linux qui va vous permettre d'héberger facilement et rapidement les services internet dont vous aurez besoin.

L'installation est des plus enfantines. Une fois installé, FreeEOS vous permettra de partager votre connexion Internet entre plusieurs machines, de les protéger grâce à son firewall automatisé, d'héberger vos sites, emails et messagerie instantanée ou gérer un domaine, ce que 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

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



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

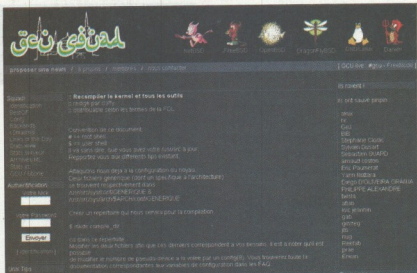
Bref, FreeEOS est la solution à tous les administrateurs débutant comme confirmés n'ayant pas le temps (ou la motivation >:) de s'adonner à la configuration manuelle de leur serveur !

## Gcu Squad

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 permet-

tre 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 franco-phone », Linux Entre Amis (Léa) est une référence pour tous les utilisateurs francophones de Linux qui souhaitent obtenir une aide en ligne sur un problème précis. Ce site est l'un de mes préférés en la matière. Il possède une base de données d'articles qui s'enrichit continuellement pour vous offrir la solution à votre problème. Parmi les nombreuses rubriques qui composent ce site, vous pourrez trouver de nombreux conseils et astuces dans les domaines aussi variés que les réseaux, X-Window, l'administration de votre poste, le noyau et j'en passe. Vous pourrez également apprendre à vous servir de vieux minitel comme terminal ! Bref de quoi vous scotcher à votre écran

et votre console un bon bout de temps. Mais Léa c'est aussi la possibilité de télécharger au format PDF l'ensemble des informations disponibles sur

le site pour une consultation hors-ligne. C'est un geste très appréciable de la part des concepteurs du site. A consulter sans modération !

## Koders.com

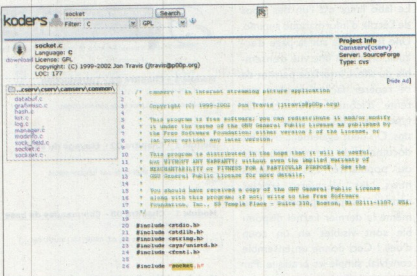
LANGUE : Français  
URL : <http://www.koders.com>

Avis aux accros de la programmation ! Nous avons déniché pour vous une véritable mine d'or !

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

Son utilisation est des plus 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 pourrais coder mon petit bot IRC.

Amateurs de programmation, koders.com est donc un site qui rentre 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 patches ou des outils afin de rendre votre code plus sécurisé.

Nous terminerons sur un des points majeurs de ce site. En effet, si vous le souhaitez, vous aurez la possibilité de



proposer une news ou même un patch pour le site. Et oui, c'est grâce à ses

contributeurs que le site est aujourd'hui, devenu une référence.

# Developpez.com

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

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

The screenshot shows the Developpez.com website interface. At the top, there's a search bar and navigation links like 'Rechercher', 'Sur les forums', 'Forum', 'Voteries', 'FAQ's', 'Partenaires', 'Hébergement', and 'Contacts'. Below this is a menu with categories like 'C++', 'Java', 'PHP', 'Perl', 'Python', 'Delphi', 'Pascal', 'Access', 'SQL', 'MS SQL', 'Oracle', and 'XML'. The main content area features a banner for 'Les meilleurs cours, tutoriels, livres électroniques et Docs sur C, C++, C++Builder, Borland C++ Compiler, Borland C++, Visual C++, Gcc à consulter ou à télécharger sur le Web'. Below the banner, there's a section titled 'Langage C' with a table of articles:

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

cis 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 quel-

ques ouvrages qui vous aiderons dans votre apprentissage. Bref, un concentré de points positifs qui feront la joie de certains !

# RATS

Quel programmeur n'a jamais rêvé d'un outil qui audite son code à la recherche de failles de sécurité ou de buffer overflow ? 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 forcément des problèmes à l'origine mais peuvent le devenir dans une utilisation détournée du programme audité. De plus, le logiciel donne, si possible, les modifications à apporter pour régler le problème. Bien évidemment, même si il permet de

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

## R.A.T.S.: Real-time Action Tracking System :

The screenshot displays the R.A.T.S. software interface with several sections:

- Objectives:** The reason and goal of the software team was to design a software package responsible for reading data from the break-line system, using the data to calculate the height traveled by the athlete, and to display all relevant information to the user in a meaningful way.
- Needs Assessment:** Information Problem: The lack of accurate, objective, real-time statistical information for judging and evaluating the performance of extreme athletes (paratroopers, skydivers, etc.).
- Methodology:** Literature Reviews, Interviews and Consultations, Action Sports Video Reviews.
- User Needs:** Accuracy: Judges need a tool to accurately measure height in real time. Possibility: Athletes need a tool that gives them real-time feedback. Speed: All parties need a tool to provide information quickly.
- Development:** Generalized test calculation, Detailed Application Architecture Diagram, An experimental analysis of an evaluation timer was essential for recording the time taken for a person to enter and leave the air.
- User Evaluation:** Recruit qualified members of the action sports community, Create an effective evaluation tool, Test the usability and effectiveness of the evaluation tool by distributing the system.
- Future Work:** Plan and implement improvements based on the user evaluations, Focus on displaying other types of statistical information: reaction, speed, etc.

At the bottom, there is a line graph titled 'Estimated vs. Actual Heights' showing data for five different users (User #1 to User #5) across five trials (1991 to 1995). The graph plots height in meters on the y-axis (0 to 300) against trial number on the x-axis. A legend indicates that solid lines represent 'Estimated Height' and dashed lines represent 'Actual Height'.

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 inconvénients de chacun puis donne en conclusion une note générale. Bien entendu, après l'installation de votre nouveau firewall, vous pourrez utiliser l'outil 'Scan Test' du site pour évaluer la sécurité de votre machine.

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

A noter: si votre esprit de curiosité est intéressant notamment une introduction au fonctionnement des anti-virus. est également enrichis de quelques articles Bonne visite !

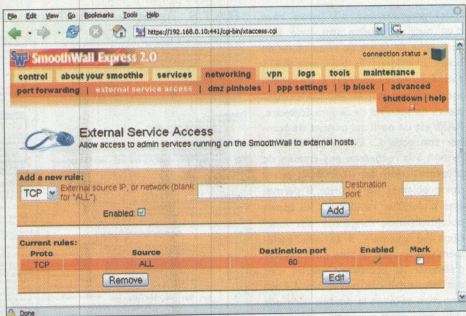
## Smoothwall

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 serveur web consultable depuis internet devient une tâche enfantine.

Par ailleurs, Smoothwall est bien plus qu'un simple firewall. Il intègre égale-



ment 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.

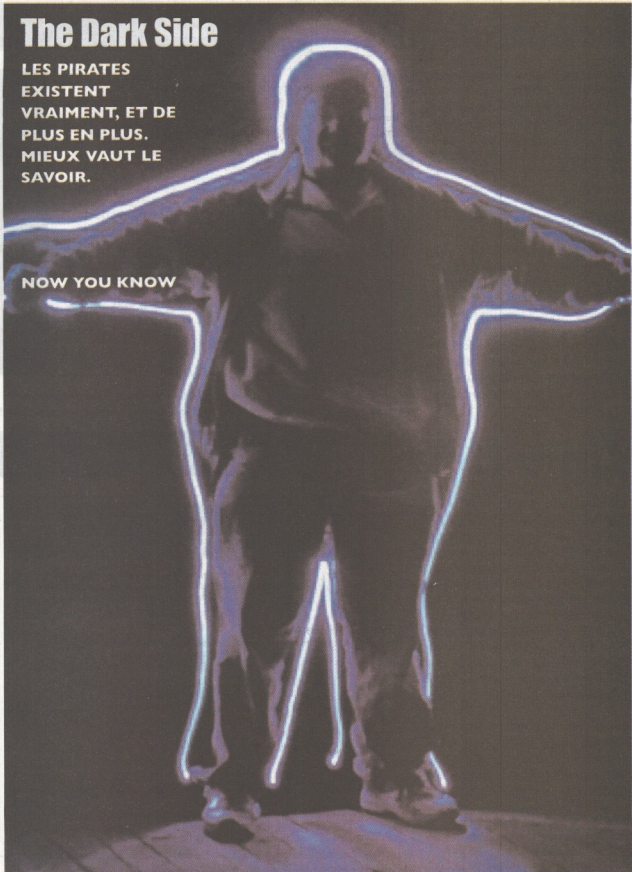
Voilà de quoi en dissuader plus d'un qui tenterait de s'attaquer à votre réseau !



# The Dark Side

LES PIRATES  
EXISTENT  
VRAIMENT, ET DE  
PLUS EN PLUS.  
MIEUX VAUT LE  
SAVOIR.

NOW YOU KNOW

A person is shown from the waist up, wearing a dark hoodie and dark pants. The person's entire silhouette is outlined with a bright, glowing blue neon light. The person is standing on a wooden floor, and the background is dark. The text "NOW YOU KNOW" is printed in white on the left side of the person's torso.

## 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 répondez 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 inoffensifs. 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 formatteur 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
oish.txt	08-Sep-2004 02:48
Code-Red-Worm.txt	08-Sep-2004 02:48
exploitthtml.txt	31-Jul-2005 18:44
homepage.txt	08-Sep-2004 02:48
1cecubes.asm.txt	08-Sep-2004 02:48
iloveyou.txt	08-Sep-2004 02:49
kak.txt	11-Sep-2004 18:18
kernel.dll.txt	11-Nov-2004 23:46
LIFE STAGES.TXT	08-Sep-2004 02:49
MarkerC.txt	08-Sep-2004 02:49
mawanela.decoded.txt	08-Sep-2004 02:49
mawanela.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
y90atcom.pdf	08-Sep-2004 02:50
VBSWS-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 claires 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 Odayz (fake or not ?), les nouvelles vulnérabilités ou plus généralement le hacking. Pour vous retrouver dans ce site, un module

LANGUAGE	STATISTIQUE DES HACKERS					
	No Hacker	Piratage d'IP individuel	Piratage en masses	Total des sites pirates	Piratage de page persos	Classement
RECHERCHE	1. iskorpitz	9511	66767	76278	9426	66852
	2. Fatal Error	8135	11626	19761	15143	4618
	3. RedEye	4789	28504	33293	33002	291
MENU	4. Jidex	4384	29454	33938	33757	81
PRINCIPAL	5. TechTeam	4333	32033	36366	36353	13
Accueil	6. SPKIDS	4266	11988	16254	15286	968
Infos from zone-h	7. root_System	4046	19221	23267	21039	2228
Infos from the world	8. haddisidrew	3853	6473	10326	5267	5059
Astuces	9. Infemio group	3731	30326	34057	32480	1577
Telechargement	10. Salmiers	3631	32025	35656	35606	50
Zone-H works	11. BloodR	3262	16429	19691	19694	7
Digital attacks	12. IDN	3127	3324	6451	5128	1323
Site pirates/Archives des crimes	13. PiDelsi	2909	3347	6256	568	5688
Site pirates/Archives des crimes *	14. nobodycoder	2690	1257	3947	939	3008
*	15. d3d3z	2646	1655	4301	3248	1053
Referencer un piratage	16. H4CK3R5B4	2495	12711	15206	14515	691
Stay tuned	17. nE7*DevIL	2405	2149	4554	2099	2455
Inscription mailing-list						

de recherche est à votre disposition. Un site des plus intéressants à visiter pour le hacker comme pour le responsable sécurité.

milw0rm.com est une base de données intéressantes d'exploits et shellcodes en tout genre. Le site est mis à jour régulièrement afin de fournir des exploits pour les dernières versions d'applications vulnérables.

Ainsi le site fournit des exploits local, remotes pour des plateformes aussi diverses que linux, windows, novell, hp-ux, bsd et j'en passe.

Le site fournit également des exploits pour des applications telles que les services web comme les forums, php, etc...

De plus, les exploits sont parfois accompagnés d'explications sur leur fonctionnement afin de comprendre exactement comment ils 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 plu-

gin firefox pour ceux qui le désirent) se révèle très pratique pour trouver ce que l'on recherche 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

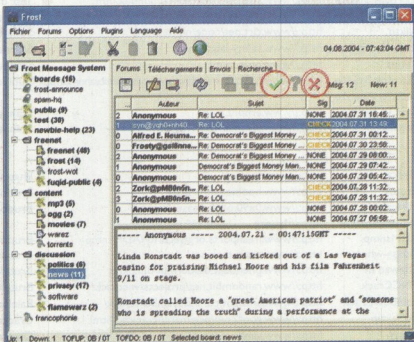
Freenet est un réseau informatique anonyme et décentralisé, bâti au dessus d'Internet et conçu pour exercer une liberté d'expression totale et résistant à la censure. Sa nature permet donc à chacun de lire et de publier du contenu. Il offre la plupart des services actuels d'Internet (email, téléchargement, 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 non 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.

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



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



Le logiciel d'échange de fichiers Frost

# À découvrir dans

## Prise d'information

### 1. Détection d'OS

p0f	<a href="http://lcamtuf.coredump.cx/p0f.shtml">http://lcamtuf.coredump.cx/p0f.shtml</a>
Queso	<a href="http://packetstormsecurity.org/pk/UNIX/scanners/">http://packetstormsecurity.org/pk/UNIX/scanners/</a>
Xprobe2	<a href="http://xprobe.sourceforge.net/">http://xprobe.sourceforge.net/</a>

Détection passive  
 Détection active (TCP/IP)  
 Détection intelligente

### 2. Scanners de ports

NmapFE	<a href="http://www.advogato.org/proj/NmapFE/">http://www.advogato.org/proj/NmapFE/</a>
Unicorn Scan	<a href="http://www.unicornscaan.org/">http://www.unicornscaan.org/</a>

GUI complète pour nmap  
 Scanner de port distribué et plus

### 3. Divers

DNS enum	<a href="http://www.hackingdefined.com/tools/reconnaissance/dnsenum.zip">http://www.hackingdefined.com/tools/reconnaissance/dnsenum.zip</a>
NBTScan	<a href="http://www.inetcat.org/software/nbtscan.html">http://www.inetcat.org/software/nbtscan.html</a>
LinNeighborhood	<a href="http://www.bnro.de/~schmidjo/">http://www.bnro.de/~schmidjo/</a>
Cheops	<a href="http://www.marko.net/cheops/">http://www.marko.net/cheops/</a>
AutoScan	<a href="http://autoscan.free.fr/">http://autoscan.free.fr/</a>
SNMP enum	<a href="http://packetstormsecurity.org/pk/UNIX/scanners">http://packetstormsecurity.org/pk/UNIX/scanners</a>
Mibble	<a href="http://mibble.org">http://mibble.org</a>
Sam Spade	<a href="http://www.samspade.org/">http://www.samspade.org/</a>
Luma	<a href="http://luma.sourceforge.net/">http://luma.sourceforge.net/</a> Navigateur

Énumération d'Info (zones, reverses lookups, etc.)  
 Scan NETBIOS  
 Navigateur SMB avec GUI pour nux  
 Explorateurs réseau + outils  
 Explorateur réseau + scanner de port  
 Explorateur SNMP  
 Parser/Manipuler des MIB (SNMP)  
 Pris d'info multi-fonctions pour Windows  
 LDAP et outils

## Exploits, vulnérabilités, Pen-testing

### 1. Scanners de vulnérabilités

Sql Power Injector	<a href="http://www.sqlpowerinjector.com/index.htm">http://www.sqlpowerinjector.com/index.htm</a>
Nessus	<a href="http://www.nessus.org/Nessus">http://www.nessus.org/Nessus</a>
Nikto	<a href="http://www.cirt.net/code/nikto.shtml">http://www.cirt.net/code/nikto.shtml</a>
Shadow Security Scanner	<a href="http://www.safety-lab.com">http://www.safety-lab.com</a>
Retina	<a href="http://www.eeye.com/">http://www.eeye.com/</a>
Microsoft Baseline Security Analyser	<a href="http://www.microsoft.com/technet/security/tools/mbsahome.mspx">http://www.microsoft.com/technet/security/tools/mbsahome.mspx</a>
CISCO Torch	<a href="http://www.arhont.com/">http://www.arhont.com/</a>
Yersina	<a href="http://www.yersinia.net/">http://www.yersinia.net/</a>

Test d'injections SQL  
 Scanner de vulnérabilités  
 Scanner de vulnérabilités web  
 Scanner de vulnérabilités  
 Scanner commercial (gestion de risques, etc)  
 Outil local de Microsoft

Scanner et prise d'info CISCO  
 Scanner de vulnérabilités (protocoles)

### 2. Mots de passe

Hydra	<a href="http://www.thc.org/">http://www.thc.org/</a>
Brutus	<a href="http://www.hoobie.net/brutus/">http://www.hoobie.net/brutus/</a>
Mezcal	<a href="http://www.0x90.org/releases/mezcal/">http://www.0x90.org/releases/mezcal/</a>
thc-pptp-bruter	<a href="http://thc.org">http://thc.org</a> Brutforceur PPTP
ADMSnmp	<a href="http://www.freshports.org/security/ADMSnmp">http://www.freshports.org/security/ADMSnmp</a>
Guess-who	<a href="http://www.team-teso.net/">http://www.team-teso.net/</a>
Obiwan III	<a href="http://www.phenoelit.de/obiwan/oIII.pl.txt">http://www.phenoelit.de/obiwan/oIII.pl.txt</a>
VNCCrack	<a href="http://www.randombit.net/projects/vnccrack/">http://www.randombit.net/projects/vnccrack/</a>
RainbowCrack	<a href="http://www.antsight.com/zsl/rainbowcrack/">http://www.antsight.com/zsl/rainbowcrack/</a>
Fcrackzip	<a href="http://www.gooof.com/pgc/marc/fcrackzip.html">http://www.gooof.com/pgc/marc/fcrackzip.html</a>
Nasty	<a href="http://www.vanheusden.com/">http://www.vanheusden.com/</a>
OpenWall	<a href="ftp://ftp.openwall.com/pub/wordlists/">ftp://ftp.openwall.com/pub/wordlists/</a>
PacketStorm	<a href="http://packetstormsecurity.org/Crackers/wordlists/">http://packetstormsecurity.org/Crackers/wordlists/</a>

Brutforceur FTP,POP,IMAP,TeInet,HTTP,LDAP,etc.etc.  
 Brutforceur multi-fonctions pour Windows  
 Brutforceur HTTPS

Brutforceur SNMP  
 Brutforceur SSH  
 Brutforceur HTTP  
 Brutforceur VNC (offline : après sniffing)  
 Rainbow tables  
 Cracker de ZIP  
 Cracker de pass GPG/PGP  
 Petite collection de wordlists  
 (généralistes et différentes langues)  
 Énorme collection de wordlists

# le web profond

## 3. Frameworks

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

## 4. Fuzzers

Spike	<a href="http://www.immunitysec.com/resources/freesoftware.shtml">http://www.immunitysec.com/resources/freesoftware.shtml</a>	Framework générique
Bed	<a href="http://www.snake-basket.de/bed/">http://www.snake-basket.de/bed/</a>	Fuzzer de protocoles
Peach	<a href="http://peachfuzz.sourceforge.net">http://peachfuzz.sourceforge.net</a>	Framework Python cross-platform
SNMP Fuzzer	<a href="http://www.arhont.com/">http://www.arhont.com/</a>	Fuzzer SNMP

## 5. Sniffers/MITM

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

## 6. Spoofing/Forging

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

## Sans-fil

### 1. WiFi

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

### 2. Bluetooth

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

## Challenges

Pull The Plug	<a href="http://www.pulltheplug.org/">http://www.pulltheplug.org/</a>	Plusieurs machines dédiées
Hackers Lab	<a href="http://www.hackerslab.org/">http://www.hackerslab.org/</a>	
Securitech	<a href="http://www.challenge-securitech.com/">http://www.challenge-securitech.com/</a>	Challenge Coréen avec 17 niveaux de difficulté croissante
3564020356	<a href="http://3564020356.org/">http://3564020356.org/</a>	Concours annuel (solutions en ligne)
Security-Challenge	<a href="http://www.security-challenge.com">http://www.security-challenge.com</a>	Challenge de reversing
Python Challenge	<a href="http://www.pythionchallenge.com/">http://www.pythionchallenge.com/</a>	100 failles web à trouver
HackerGames	<a href="http://hackergames.net/">http://hackergames.net/</a>	Challenge de programmation
		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](http://www.hackdefined.com),

The screenshot shows the 'remote-exploit.org' website. The main heading is 'Tutorials'. Below it is a 'Table of contents (Print)' section listing various tutorials such as 'Customizing BackTrack', 'Cisco Flirt', 'Remote Auditor Traffic Sniffing', 'Wireshark', 'WiFi Cracking', 'Nmap3: Basic Co-Authentication', 'Web Cracking', 'Bluelight', 'Bluelight & Bluetooth enabled Mobile Phone', 'Network & Vulnerability Scanning', 'Basic Introduction to the Nessus security scanner using Auditor Security Collection', 'Basic Introduction network mapping using nmap', 'Link fingerprint analysis', 'Exploiting weakness of PPTP vms', 'Decompiling SSL Traffic using Man In The Middle technique (MITM)', 'Password recovery', 'Cracking Windows Passwords with BackTrack and Mini-TestAnd', 'Cracking System and the Sudo on windows Using RemoteExploit', 'Local Password Cracking Presentation', and 'Hardware modification: external antenna modification'. There is also a search bar and a 'Tutorials' section at the bottom with a disclaimer: 'Most of the tutorials describing how to use the Auditor Security Collection CD-ROM for a pc. We put in here some tutorials provided by users. We don't have control about the content of it.'

cette vidéo fait office de précurseur dans le domaine : on y voit comment, en quelques minutes, des outils distribués depuis BackTrack, téléchargeable chez [www.remote-exploit.org](http://www.remote-exploit.org) peuvent cracker une clé de protection wifi (à noter qu'il s'agit alors de clé de 64 bits).

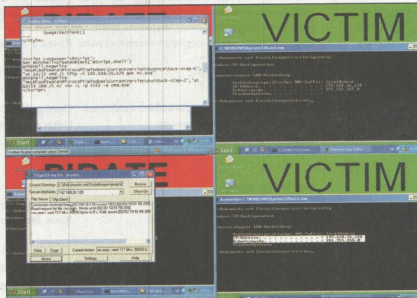
## La relève

Près de 40 vidéos composent la bibliothèque d'IronGeek. Certaines d'entre elles sont issues d'autres sites, et d'autres ne sont pas vraiment des vidéos pédagogiques ; malgré cela, toutes sont intéressantes. Deux vidéos 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 scanners 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'elles



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'à se renseigner sur les différentes fonctions que l'on y trouve.

# NET *libre*

N°2 • Mars-Avril 2008 • 4,50 euros

## Ne **payez plus** vos **logiciels !**

**Les versions libres  
et gratuites  
des plus grands softs  
du commerce**

**Où les trouver ?  
Comment les utiliser ?**

*Bureautique • Photo-montage • PDF • 3D*

**EN VENTE EN KIOSQUE**

**LINUX**SCHOOL  
M a g a z i n e



Nouveau

N° 2 / FEVRIER-MARS 2008 / 4.50 EUROS

# HACKING LINUX

Sécurisation

2

Crypter fichiers et e-mails

Heavy Firewalling

En vente en kiosque