



SÉCURITÉ INFORMATIQUE ET HACKING PRATIQUE

HACKADEMY MANUEL

# the HACKADEMY #8 MANUEL



100% white hat hacking

# SHELLCODES

- **Initiation**  
aux buffer overflows
- **Codage d'exploits**  
compatibles WinXP/NT/9x

**Anti-piratage**  
**Détectez**  
les portscans

### état de l'art

Userland Exec,  
Syscall Proxying,  
InlineEgg, MOSDEF

### Mots de passe

- Les techniques de cracking à distance
- Les entreprises à la rue ?



**Solution Expert (bypasser PaX à distance) + Newbie**  
**LES NOUVELLES EPREUVES**

**Créer et comprendre**  
**et casser RSA**  
**Les cartes à puces vulnérables ?**

5,90€

IMESTRIEL MARS AVRIL 2004 - DOM 6,85 € - BEL - 6,95 € - CH 11,50 FS - CAN 9,50 \$ - MAR 45 DH - MAY 8,20 €

HACKADEMY MANUEL the HACKADEMY MANUEL

# EN VENTE EN KIOSQUE

## FREE SOFT FACTORY 1

Vous avez décidé d'utiliser des logiciels libres, toutes nos félicitations ! Ce premier CD-ROM Free Soft Factory marquera les esprits, puisqu'il inaugure notre collection de logiciels utiles et performants distribués près de chez vous, en kiosque, pour un coût quasiment nul. Finis les monopoles abusifs et sclérosants de certaines grandes compagnies américaines, le logiciel libre et indépendant apporte en force son dynamisme et ses innovations.

Dans une première partie, nous allons vous expliquer ce qu'est le mouvement du " Libre ", et comment installer les logiciels présents sur le CD-ROM. En bonus, sans supplément de prix, nous avons décidé de rajouter 50 pages d'explications et de tutoriels sur l'utilisation de certains de ces outils. Nous avons sélectionné en particulier ceux dont la prise en main diffère un peu de leur équivalent classique. Vous ne trouverez pas d'explications sur la création de PDF : celle-ci s'effectue en effet de manière simplissime, en ouvrant votre document avec OpenOffice et en sélectionnant " Exporter au format PDF " dans le menu Fichier !

Enfin, un grand merci aux auteurs des différents logiciels et des documents de ce livret, qui sont tous distribués sous une licence libre; et un merci tout particulier à Fabien ILLIDE et à son projet Free-OS, qui ont largement contribué à la réalisation de ce premier volet de Free Soft Factory.

<b>P.4</b>	<b>PRÉSENTATION DU LOGICIEL LIBRE ET GUIDE D'INSTALLATION DU CD</b>
<b>P.14</b>	<b>COMPRESSEZ VOS DOCUMENTS</b>
<b>P.17</b>	<b>CRÉER UNE PRÉSENTATION AVEC IMPRESS</b>
<b>P.22</b>	<b>TRANSFÉRER DES FICHIERS PAR FTP</b>
<b>P.25</b>	<b>UTILISER LE TABLEUR DE OPENOFFICE</b>
<b>P.31</b>	<b>PHOTOMONTAGE AVEC GIMP</b>
<b>P.52</b>	<b>GIMP FAQ</b>
<b>P.54</b>	<b>LE NAVIGATEUR WEB FIREBIRD</b>
<b>P.55</b>	<b>CAPTURER UN SITE INTERNET</b>

# The Hackademy présente :

# Free Soft'Factory numéro 1

**Vous trouverez sur le CD Free Soft'Factory numéro 1 de nombreux logiciels Libres pour Windows. Nous allons commencer par expliquer ce qu'est un logiciel Libre. Ensuite nous vous présenterons les différents logiciels du CD, et la façon – très simple – de lancer leur installation. Nous avons même décidé de vous offrir en version imprimée des explications détaillées sur certains de ces logiciels. C'est le cas pour The Gimp, dont la prise en main diffère un peu des logiciels de retouche photo auxquels vous êtes habitués. Une abondante documentation est disponibles sur le CD lui-même, y compris un livre de 700 pages sur la suite bureautique OpenOffice !**

Commençons par mieux comprendre ce que l'on appelle par "logiciel Libre", avec un extrait de la seconde édition du "livret du libre", un texte écrit par des acteurs de ce mouvement.

## LE LIVRET DU LIBRE

<http://livretdulibre.org/>

À côté du monde de l'informatique propriétaire dominé par Microsoft, un autre modèle s'est développé. Les Logiciels Libres, développés par une communauté privilégiant le partage et l'entre-aide, n'ont plus rien à envier à leurs voisins propriétaires et les surpassent même souvent. La philosophie du Libre dépasse d'ailleurs aujourd'hui le cadre du logiciel : on la retrouve aussi dans l'art, la littérature ou l'électronique.

Ce texte commence par détailler les bases philosophiques et juridiques des Logiciels Libres, et explique ce que le Logiciel Libre peut apporter. Puis il aborde les autres formes d'expression libre et les menaces planant actuellement sur le monde du Libre. Il termine par quelques conseils permettant de vivre un peu plus libre au quotidien.

Ce "livret" est lui-même développé comme un projet Libre. Pour contribuer à son amélioration, ou en télécharger la dernière version, rendez vous sur <http://www.livretdulibre.org/>. Vous avez l'autorisation de distribuer des copies exactes de ce document tant que cette note de permission et le copyright apparaissent clairement. Vous avez l'autorisation de distribuer des versions modifiées de ce document tant que la totalité du document dérivé est distribuée sous les mêmes termes que celui-ci.

Voici quelques associations et personnes ayant contribué à ce texte :

- Club Lolut de l'UTBM - <http://lolut.utbm.info/>
- Association Librétudes - <http://www.libretudes.org/>
- Christophe Bliard - [christophe.bliard@netcourrier.com](mailto:christophe.bliard@netcourrier.com)
- Jean-Christophe Haessig - [jean-christophe.haessig@utbm.fr](mailto:jean-christophe.haessig@utbm.fr)
- Thomas Petazzoni - [thomas.petazzoni@enix.org](mailto:thomas.petazzoni@enix.org)
- Nicolas Bouillon - [bouil@bouil.org](mailto:bouil@bouil.org)
- Lucas Nussbaum - [lnu@gnu.org](mailto:lnu@gnu.org)

## LE LIBRE : UN RETOUR NATUREL AU PARTAGE DES CONNAISSANCES

### • Le principe de partage des connaissances

"Rien n'appartient à rien, tout appartient à tous" (Alfred de Musset)

Il était une fois un partage sans limite des connaissances. Une époque durant laquelle les progrès de la science et de la technique ont été tout à fait considérables, et la création artistique florissante. La majorité des scientifiques et techniciens échangeaient de l'information grâce à diverses publications, et les artistes diffusaient naturellement leurs œuvres.

Ce partage des connaissances naturel se situe dans la tradition du travail scientifique : la communauté scientifique a pour objectif l'avancée de son domaine, sans avoir à tenir compte d'une application directe, en particulier mercantile. Le partage des connaissances est au cœur même du progrès de la science, et de la construction d'un bien commun.

### • En informatique...

L'informatique était une de ces sciences dans laquelle les chercheurs échangeaient librement le code source de leur programmes. Le code source est la version intelligible et compréhensible par un humain d'un programme informatique. Il est écrit dans un langage dit de programmation, connu des programmeurs. Il décrit à l'aide de mots et de formules le fonctionnement précis d'un logiciel. Ce code source n'est pas directement utilisable par l'ordinateur, il est donc traduit en code machine, ou code exécutable.

Depuis les débuts de l'informatique, les chercheurs et étudiants échangeaient le code source de leurs programmes via le réseau Internet, de manière à ce que tout le monde puisse les étudier et les améliorer. La liberté d'utilisation des recherches en informatique et des codes sources des programmes était alors totale, et peu de chercheurs restreignaient la distribution de leurs résultats : rien ne nuisait à la recherche et au progrès de la technique.

Au début des années 80, cette règle tacite de partage des connaissances a changé : des éditeurs ont commencé à vendre leurs premiers logiciels, sans en distribuer le code source : c'est le logiciel propriétaire. Son système social est fondé sur l'isolement et la division des utilisateurs :

- il est livré sans son code source, il est donc impossible pour un programmeur de le modifier ou de l'améliorer ce qui rompt le principe de liberté ;
- il a un coût, et engendre donc une forme de discrimination par l'argent ce qui rompt le principe d'égalité ;
- leur copie est le plus souvent illégale, il est interdit d'aider son voisin ce qui rompt le principe de fraternité.

Si le logiciel propriétaire était un plat cuisiné, il serait impossible de connaître sa composition, ni la façon dont il a été cuisiné. Il serait bien entendu interdit d'essayer de le deviner. Il serait impossible d'améliorer la recette, et il vous serait interdit d'en donner un morceau à votre ami qui meurt de faim. L'idée de privatisation du logiciel, et des autres formes d'expression est donc une idée allant à l'encontre du partage des connaissances [1].

A l'heure actuelle, le grand public utilise en majorité des logiciels propriétaires.

#### • Le projet GNU

Afin de faire perdurer l'esprit de partage des connaissances, Richard M. Stallman, un chercheur en informatique au MIT (Institut de Technologie du Massachusetts, États-Unis) décide de quitter son laboratoire en 1984, et de se consacrer à l'écriture d'un système informatique complet et libre, appelé GNU [2].

Dans le même temps, Richard M. Stallman crée la Free Software Foundation visant à supporter le projet GNU. Les premiers travaux de cette fondation sont de définir le concept de Logiciel Libre et de rédiger une licence adaptée à sa distribution, la GPL [3] (Licence Publique Générale GNU), fondant ainsi les bases éthiques, politiques et juridiques du mouvement du libre.

## LE LOGICIEL LIBRE

#### • Qu'est-ce que le Logiciel Libre ?

Les logiciels propriétaires réduisent la liberté de l'utilisateur. Par contre, le Logiciel Libre [4] est spécialement conçu pour préserver la liberté des utilisateurs en garantissant quatre libertés fondamentales :

- La liberté d'utiliser le logiciel pour n'importe quel usage et par toute personne ;
- La liberté d'étudier le logiciel, et de l'adapter à ses besoins. Pour ceci l'accès au code source est une condition requise ;
- La liberté de redistribuer des copies ;
- La liberté d'améliorer le programme et de publier vos améliorations, pour en faire profiter toute la communauté. Pour ceci l'accès au code source est une condition requise.

On peut voir une analogie entre ces quatre libertés et la devise de la république française : l'utilisateur est libre de choisir son logiciel, libre d'en changer. Les utilisateurs sont égaux car il n'y a pas de discrimination. L'esprit de fraternité est respecté car l'utilisateur peut aider ses proches.

Toutefois, la notion de liberté du logiciel n'a aucun rapport avec le prix. En effet, une société peut commercialiser un Logiciel Libre et réaliser des bénéfices sur cette vente.

#### • L'idée de copyleft

Le copyleft est une utilisation particulière du droit d'auteur (copyright) qui consiste à autoriser la copie, la modification, la diffusion et l'exploitation de son œuvre par n'importe qui. Mais toutes les versions modifiées de cette œuvre doivent être distribuées sous la même licence : c'est la particularité du copyleft, qui permet à ce qui est libre de rester libre.

Le copyleft est un concept inventé par la Free Software Foundation et constitue donc l'expression d'un acte militant en faveur du libre accès aux connaissances. Ce concept ne se limite d'ailleurs pas qu'au logiciel.

Le copyleft permet à la fois à l'auteur de garder le contrôle de son œuvre, et à l'utilisateur de l'utiliser librement. Il permet de créer un fond commun de ressources libres, considérant que la connaissance scientifique fait partie du patrimoine de l'humanité. Tout en respectant le droit d'auteur, l'idée de copyleft est donc de garantir les libertés de l'utilisateur en s'assurant que les œuvres copyleftées resteront libres.

La FAQ de la Licence Art Libre [5], donnera de plus amples informations sur la différence entre copyright, copyleft, et droits d'auteur.

- **Les différences entre Logiciel Libre, Domaine Public, Freeware, et Open Source**

On confond souvent à tort le Logiciel Libre et d'autres types de logiciels.

Tout d'abord, il ne faut pas confondre Logiciel Libre et domaine public. Une œuvre dans le domaine public est libre de droits, c'est-à-dire que l'on peut en faire ce que l'on souhaite. Les logiciels libres ne sont pas dans le domaine public : ils sont uniquement une utilisation différente du droit d'auteur.

Les freeware sont une version gratuite des logiciels propriétaires, donc n'assurent pas les libertés associées au Logiciel Libre.

En anglais, Logiciel Libre se dit Free Software. Free signifiant libre ou gratuit. Dans le cas du Logiciel Libre, il faut comprendre free dans le sens libre : un Logiciel Libre n'est pas forcément gratuit. Afin de gommer cette confusion, certains acteurs du Logiciel Libre ont introduit le terme Open Source [6] qui distingue l'accès au code source de la gratuité. Ce terme n'a finalement fait

qu'ajouter à la confusion. En effet, ce terme a été exploité par des sociétés diffusant leur code source mais sans toutes les libertés du Logiciel Libre, et tout particulièrement celle de modifier le code source et d'en diffuser les modifications.

Certains utiliseront le terme Open Source en parlant de Logiciels Libres sans faire l'amalgame avec les logiciels gratuits. D'autres chercheront simplement à profiter de la popularité grandissante des Logiciels Libres. Il n'est pas toujours simple de faire la différence.

La meilleure façon de savoir dans quel domaine se place le logiciel que l'on utilise est de se référer à la licence d'utilisation sous laquelle est distribué le logiciel. Le site Web de la Free Software Foundation donne de plus amples explications sur les licences ([7] et [8]).

- **GNU/Linux : un système abouti**

Le projet GNU a permis de créer un ensemble de logiciels, permettant d'utiliser un ordinateur pour de nombreuses applications. Toutefois, jusqu'en 1991, il était impossible d'utiliser un ordinateur sans utiliser de logiciels propriétaires. Un composant manquait : le noyau du système d'exploitation. C'est un projet initié par un étudiant Finlandais, Linus Torvalds, qui a comblé ce manque avec le noyau Linux. Le système GNU/Linux était né. Il est constitué de divers logiciels du projet GNU, du noyau Linux et de bien d'autres Logiciels Libres.

A l'heure actuelle, le système GNU/Linux peut être utilisé quotidiennement à la fois pour des usages courants tels que la bureautique, l'Internet, le multimédia, mais aussi pour des usages plus professionnels comme les serveurs Internet et le développement logi-

ciel. C'est d'ailleurs dans le domaine professionnel que GNU/Linux a acquis ses lettres de noblesses. Le Logiciel Libre est donc une alternative techniquement viable et crédible pour l'utilisateur.

## POURQUOI UTILISER LE LOGICIEL LIBRE ?

### • Éthique

Tout d'abord, utiliser le Logiciel Libre est une démarche éthique : c'est la volonté d'utiliser des logiciels réalisés avec l'objectif de créer un bien commun dans l'intérêt général, et non pas des logiciels créés pour des intérêts privés.

Ensuite, l'idée de partage des connaissances, véhiculée par la philosophie du Logiciel Libre, est en adéquation avec les valeurs de l'enseignement public [9]. Il semblerait donc plus cohérent d'utiliser de tels logiciels dans le cadre de l'éducation.

### • Libre accès

Les Logiciels Libres sont des logiciels librement accessibles, copiables et diffusables. L'utilisation de tels logiciels n'engendre donc pas de discrimination par l'argent, dans la mesure où tout le monde peut se les procurer.

De plus, leur coût est significativement plus faible que celui des logiciels propriétaires, ce qui permet d'engendrer des économies sur l'achat des licences. Par exemple, en utilisant des Logiciels Libres, l'État pourrait investir dans des développements logiciels au niveau national, dont le résultat serait accessible à tout citoyen.

Pour le responsable informatique d'une grande structure, la gestion des licences est simplifiée avec le Logiciel Libre : on peut le copier sans compter.

### • Indépendance

La disponibilité du code source des Logiciels Libres permet d'être indépendant du fournisseur de logiciel. Ceci a plusieurs avantages :

- si le fournisseur de logiciels ferme ou change son offre, il est possible de faire appel à un autre fournisseur, en conservant la solution technique actuelle ;
- il est possible de modifier soi-même le code source du logiciel, ou d'employer des développeurs, afin d'ajouter des fonctionnalités ou de corriger des erreurs.

En général, les Logiciels Libres utilisent des formats ouverts, c'est-à-dire des formats de fichiers ou des protocoles dont les spécifications sont disponibles. À l'inverse, les sociétés commerciales utilisent trop souvent des formats fermés, qu'elles changent régulièrement pour des raisons mercantiles. L'utilisation de formats et de protocoles ouverts offre plusieurs avantages :

- **Pérennité** : Elle permet de garantir la pérennité des informations, qui est une question importante pour les administrations et les entreprises. En effet, que se passerait-il si dans 10 ans on ne pouvait plus lire les registres de l'état civil, parce que la société qui éditait le logiciel a fermé ou que le format de fichier est devenu obsolète ? Dans le cas où un Logiciel Libre utiliserait un format de fichier non décrit, il est possible d'en connaître le fonctionnement grâce à l'étude du code source.