COMMENT EVITER / SURVIVRE A UN BUST

Version 3

PARTIE I : EVITER DE SE FAIRE PRENDRE

Pourquoi ce document ?

Comme beaucoup dans le milieu du piratage vous ne vous contentez pas de lire des articles, sécuriser des machines ou sortir du code bien propre... Vous avez décidé de mettre en pratique vos connaissances sur les attaques, failles et compagnie et vous vous introduisez régulièrement dans des systèmes informatiques privés, vous codez des 'exploits', des backdoors... bref vous êtes ce que certains appellent un 'Blackhat'.
Si vous pensez que vos activités illégales n'intéressent pas la police qui doit certainement avoir des choses bien plus importantes à faire, vous vous trompez !
A notre époque il existe dans différents pays des polices spécialisées dans la lutte contre la cyber-criminalité, ce qui veut dire qu'ils n'ont "rien d'autre de mieux à faire" que de traquer et d'arrêter des pirates informatiques comme vous. Nombreux sont ceux qui ont pensé être invincibles derrière leur PC et qui s'en sont finalement mordu les doigts.
Une vague d'arrestations a eu lieu récemment en France et ce n'est qu'un début.

Ce texte est là pour éviter que d'autres se fassent prendre ou s'ils se font prendre pour qu'ils ne s'en tirent pas trop mal. Ce document a aussi pour objectif d'ouvrir les yeux de certains sur des à priori qui peuvent les mettre en danger... il se peut que vous utilisiez une méthode pour effacer vos traces qui en rajoute au lieu de les supprimer. L'erreur est humaine.
Enfin même si vous êtes sûr de prendre les précautions nécessaires et certain que jamais vous n'aurez affaire aux services de police, sachez que la délation, qu'elle soit voulue ou non est une des principales ressources utilisées par la police pour retrouver une personne... par conséquent même si vous êtes le meilleur pirate au monde, vous pouvez toujours être balancé comme une grosse merde.

L'objectif de ce document est clairement de vous rendre parano... mais juste le nécessaire pour éviter ou survivre à un bust.

Bases

Il y a des règles très simples à mettre en oeuvre pour protéger son anonymat sur le réseau des réseau. Si vous débutez dans le milieu il est bon de s'y mettre dès maintenant ! Sinon prenez le temps de faire le point 5 minutes sur les informations qu'une personne réellement motivée peut regrouper sur vous... si ces informations permettent de faire le lien, ne serait-ce que faiblement, avec votre vraie identité alors vous devrez impérativement prendre une nouvelle cyber-identité.

La première règle est donc de bien séparer son identité réelle de sa cyber identité. N'hésitez pas à dressez une liste des informations que vous avez déjà dévoilé, ou des informations que vous voulez bien dévoiler. Ensuite tenez-vous en à cette liste. Ne franchissez jamais la limite !!

Une autre règle primordiale est de ne jamais signer ses méfaits. Une intrusion réussie est une intrusion invisible. Signer un déface ou laisser un message, même si c'est uniquement avec votre pseudonyme, c'est faire un cadeau d'une valeur inestimable à la police.
Si vraiment vous désirez signer vos méfaits, changez de pseudonyme à chaque attaque.

Ne vous vantez jamais. Ne donnez pas d'infos sur vos cibles, que ce soit avant, pendant ou après l'intrusion. Si vous demandez de l'aide sur un forum du type "Comment je peux exploiter la faille truc

sur le serveur X", on remontra très facilement à vous. Dans le pire des cas quelqu'un de plus expérimenté profitera de la faille et les dégats vous retomberont dessus.
C'est entre autre pour cela qu'une nouvelle règle d'or s'applique : Ne faites confiance qu'à vous même ! Même une personne qui est avec vous peut se retourner sans le faire exprès contre vous. Dans une équipe il y a toujours un "maillon faible" qui peut tout foutre en l'air. Il se peut aussi que le maillon faible ce soit vous et vous n'en ayez pas conscience. Pensez aux autres : si vous tombez ils risquent de tomber avec vous.
Bref, agissez seul. Une autre possibilité est de former des équipes totalement anonymes où les différents membres n'échangeraient pas de discussions amicales entre eux pour éviter qu'un maillon faible ait trop de répercussions. Mais à ma connaissance ce type d'équipe n'existe pas.

Si vous utilisez un pseudonyme il est conseillé de prendre un mot utilisé couramment.
Sachez que la police aura entre autres recours aux même moyens que vous. Si une recherche de votre pseudo sur Google permet de savoir tout ce que vous avez piraté et tout ce que vous avez codé en moins de temps qu'il faut pour le dire, vous êtes très mal barré. Pensez aussi à changer de pseudonyme de façon régulière.

N'hésitez pas à donner des fausses pistes... Vous n'avez pas de chien ? Maintenant si ! Vous habitez dans le nord de la France ? Vous êtes maintenant au sud etc etc.

N'acceptez jamais d'interview, ne contribuez jamais a un reportage sur le hacking, surtout si le journaliste qui vous le propose a pour initiales D.K. ou D.M.

Si vous appliquez comme il faut ces règles, la police ne pourra pas vous retrouvez par une enquête basique (comprendre par regroupement d'informations).

Pas de traces

Si vous avez réussi à ne pas laisser d'informations vous concernant sur le web, ce sera peut-être une machine qui vous dénoncera. Soit parce que vous avez laissé des traces sur votre cible, soit parce que vous avez des preuves de l'intrusion sur votre machine, ou encore parce qu'une machine tiers s'est chargée de vous tracer.

Sur le réseau :

Pour ce qui concerne le web c'est simple : utilisez des proxys. Tout le monde sait configurer un navigateur web pour dissimuler son IP.
Le site www.freeproxy.ch semble proposer une liste de proxys (qui fonctionnent) et qui est mise régulièrement à jour.
proxy-list.org est pas mal du tout et donne plus d'infos sur les proxys.

Il existe deux plugins pour Firefox permettant de changer très facilement de proxy :
SwitchProxy Tool
XYZproxy

ProxyWeb est un web-proxy (à l'instar d'*anonymizer.com*, sauf que *ProxyWeb* offre le support du SSL) qui est très simple d'utilisation.
Evidemment il est déconseillé de ne passer que par lui (il garde sans aucun doute une bonne quantité de logs).
SnoopBlocker propose le même service et fait partie du même réseau (65.110.6.*)
https://www.megaproxy.com/
http://atunnel.com/
Et vous en trouverez probablement d'autres sur le net. Par exemple AplusProxy vous redirige vers un proxy pris au hazard dans sa liste.

N'accordez aucune confiance à votre fournisseur d'accès Internet. Si la police a des soupçons sur vous ils peuvent très facilement récupérer des logs vous conçernant, lire vos mails, visiter le contenu de votre espace web ou savoir les sites que vous visitez.

Soyez d'autant plus parano que les lois récentes facilitent la tâche des policiers pour récupérer ces logs.

N'allez pas sur IRC. Méfiez-vous en comme de la peste. Les serveurs IRC sont largement surveillés (y compris les canaux protégés par mots de passes et les discussions "privées"). De plus le protocole IRC n'est pas sûr.
Il existe une alternative sécurisée qui s'appelle SILC dont les caractéristiques sont les suivantes :
- conversations cryptées par un système de clé publique/privée
- authentification forte des utilisateurs (personne ne peut se faire passer pour quelqu'un d'autre)
- des modes de sécurisation variés sur les channels (notemment les takeovers sont impossibles)
http://silcnet.org/

Dans l'ensemble évitez tout de qui est du même pays que vous : hébergeurs, webmails, serveurs IRC... la police n'aura aucun mal à exercer ses pouvoirs sur les propiétaires.
Même des forums que vous pensez de confiance peuvent être réquisitionnés par la police afin de récupérer les logs ou les messages privés. Changez régulièrement de proxys pour brouiller les pistes.

Preferez les protocoles Peer2Peer ou Friend2Friend à ceux utilisant un système centralisé des données. P2PChat est un exemple de logiciel de communication P2P, vous en trouverez d'autres en fouillant sur Sourceforge.net

Le groupe *Hacktivismo* a developpé le logiciel ScatterChat basé sur *Gaim* qui permet de communiquer de façon securisé.

Des efforts de collaboration internationale sont fait pour lutter contre le piratage informatique. Il est conseillé d'éviter les pays frontaliers pour les mêmes raisons. Utilisez des relais hors de l'*Union Européenne*.

N'hésitez pas à utiliser des ordinateurs de particuliers comme relais pour vos attaques. Ils sont bien moins surveillés (très peu de logs) et régulièrement rebootés/déconnectés.

Veillez bien à ne pas vous attaquer à n'importe qui. Evitez tout ce qui touche de près ou de loin à l'Etat : Gouvernement, administration, justice, education, recherche, armée ainsi que la bourse, les grosses entreprises etc. N'allez pas laisser un message du style "coucou les gayzzzz!! rofl!!" sur le site de *Dassault*.

Si vous laissez une backdoor sur un système faites attention à ce qu'elle passe inaperçue. Mieux vaut quelques lignes perdues dans des logs apache qu'une connexion sortante vers un serveur IRC visible avec un simple *netstat*.
N'hésitez pas à utiliser le tunneling ou un système de canaux cachés (covert channel). Pour une backdoor PHP mieux vaut en système basé sur les entêtes HTTP que des paramêtres passés par URL.

Cryptez tout ce que vous pouvez !
Pour savoir vite fait ce qui passe en clair et ce qui est chiffré, la commande suivante est très pratique (en root) :

```
tcpdump -n -X
```

PGP/GPG est très simple d'utilisation. Beaucoup de clients mail proposent un support du cryptage très intuitif. Au final on se sert de *GPG* sans même s'en rendre compte.
Pour les Windowsiens :
http://openpgp.vie-privee.org/
Pour les Linuxiens :
http://www.lea-linux.org/cached/index/Reseau-secu-gpg-intro.html

L'extension Firefox freenigma permet de chiffrer vos messages avec *GPG* lorsque vous les rédigez sur

votre webmail.

Quand vous en avez la possibilité, utilisez SSL. Là encore, rien de plus simple à mettre en oeuvre.

Bon nombre de webmails proposent de se connecter en SSL. Hushmail prétend être le service de webmail le plus sur.
Nerdshack va dans le meme sens.

Pour ce qui est des mails, plusieurs générations de remailers se sont succédées :
Les *Cypherpunk* (type I), *Mixmaster* (type II) et les *Mixminion* (type III)
Jusqu'à présent l'utilisation des remailers était un vrai casse-tête, mais depuis l'implémentation officielle de *Mixminion* c'est extrêmement simple.
Il suffit de télécharger le logiciel sur http://mixminion.net/, de faire quelques tests et c'est parti !

En théorie comment ça marche :
Votre client choisi un chemin parmi une liste de serveurs *Mixminion* existants.
Votre message est ensuite encodé à l'aide de clé publique de chacun des serveurs.
Chaque serveur retire une couche de cryptage du message chiffré et passe au suivant.
Pour éviter que l'on retrouve trop facilement votre IP, le message va passer plusieurs fois par les même serveurs (faire des sortes de boucles...)
Au final votre destinataire reçoit bien le message.
L'implémentation de *Mixminion* permet aussi d'envoyer le message par morceaux, chaque morceau prend alors un chemin différent puis les morceaux sont réassemblés sur le dernier relais.
A noter que cette génération de remailers permet aussi d'avoir des réponses à ses messages. Toutefois le système de réponse reste expérimental et il n'est pas forcément conseillé de l'utiliser.

Jetez un coup d'oeil à l'adresse suivante pour avoir plus d'infos :
http://en.wikipedia.org/wiki/Anonymous_remailer

Il existe un site qui se propose de faire passer un mail par Mixmaster :
https://zerofreedom.homeip.net/cgi-bin/mixnews-user.cgi

Certains hacktivistes travaillent à rendre ces techniques à la portée de tous. On peut par exemple citer le projet Anonym.OS, un live CD qui permet de se connecter de façon anonyme sur le réseau.

Anonym.OS est basé sur *OpenBSD*, ce qui peut le rendre un peu difficile à manier pour ceux qui ne connaissent pas ce système.
A part ça, le système est bien configuré, la quasi-totalité des applications proposées passent par *Tor/Privoxy* lancé au démarrage. Les créateurs ont aussi fait en sorte d'empêcher (ou au pire de limiter) la génération des logs par les logiciels.

ELE : Everithing Leaves Encrypted
ELE est un live CD dans la même optique que *Anonym.OS*.
Le projet semble mort, la dernière version (0.0.2) date de 2005. L'avantage de *ELE* est qu'il se base sur une *DSL* (Linux) ce qui le rends plus accessible qu'*Anonym.OS*.
La encore la plupart des applications passent par un *Tor/Privoxy* lancé au démarrage.
Toutefois quelques applications n'ont pas été configurées et aucune attention n'a été portée sur la génération de fichiers journaux.

JanusVM
http://www.vmware.com/vmtn/appliances/directory/392
http://janusvm.peertech.org/
JanusVM est une image VMware d'un systeme Linux 2.6 configure pour etablir des connexions anonymes.
C'est l'une des solutions les plus efficaces actuellement.
VirtualPrivacyMachine est aussi un système à émuler qui anonymise les connections

Ces deux systèmes live ne contiennent aucun outil de piratage et permettent uniquement de surfer sur internet et de communiquer.

Deux autres live CDs crées par des goupes francais règlent le probleme :

LOTFREE Live
LiveSoH 0.1 Beta

TOR :

A l'heure actuelle, *Tor* est le projet le plus intéressant et le plus efficace. Basé sur le principe des onion-routers, les paquets sont cryptés suivant le meme principe que pour *Mixminion*. Le projet est en parti financé par l'*E.F.F.* (*Electronic Frontier Foundation*).

Deux vidéos de la conférence *What-The-Hack* (en anglais) visent à expliquer le fonctionnement du reseau *Tor* (vidéos à télécharger par *BitTorrent*) :
http://rehash.waag.org/WTH/wth-anonymous-communication-58.mp4.torrent
http://rehash.waag.org/WTH/wth_tor_hidden_services.mp4.torrent

Site officiel :
http://tor.eff.org/

Une fois lancé, *Tor* lance un proxy SOCKS (par defaut localement) qui écoute sur le port 9050. Toutes les connections qu'il reçoit sont relayées à d'autres 'nodes' du réseau.

Pour profiter de *Tor*, vous devez configurer vos applications afin qu'elles utilisent ce proxy. Certaines applications parviennent à utiliser directement un proxy SOCKS.
Pour d'autres il faudra utiliser un logiciel supplémentaire. Quelques solutions sont proposées sur le WiKi de *noreply.org* :
http://wiki.noreply.org/noreply/TheOnionRouter/TorifyHOWTO

Quelques outils permettent de "socksifier" une connection dont tsocks, socat, dsocks

Même *Tor* ne garanti pas un anonymat a 100%. Des fuites d'informations peuvent vous trahir, en particulier au niveau de votre fournisseur d'accès.
Le principal problème est que le protocole SOCKS ne permet que de faire passer les connections TCP. Par conséquent tout datagramme UDP ne sera pas anonyme. Cela est par exemple vrai pour les requêtes DNS.

Pour anonymiser les requetes DNS il est possible d'utiliser un proxy DNS local. Il existe actuellement deux implémentations :
tor-dns-proxy.py par *DugSong* (auteur de dsocks)
dns-proxy-tor par l'auteur de trans-proxy-tor

Pour résoudre des noms d'hôte de façon ponctuelle vous pouvez utiliser tor-resolve qui est fournit avec *Tor*.

L'astuce concernant les requêtes DNS et le protocole HTTP consiste à utiliser un proxy HTTP qui fera passer les connections sur le réseau *Tor* sans avoir à résoudre les noms DNS (c'est la node de sortie qui s'en charge).
Privoxy est capable d'une telle opération. La ligne à rajouter au fichier de configuration pour le faire utiliser *Tor* est la suivante :

```
forward-socks4a / 127.0.0.1:9050 .
```

Il est recommandé d'utiliser *Privoxy* pour un autre objectif : réduire le nombre d'informations envoyées par votre navigateur. Avec ses "actions files" vous pouvez modifier l'identité de votre navigateur ou encore supprimer le champ Referer.

Pour utiliser *Privoxy* dans votre navigateur vous devez fixez les parametres de proxy aux valeurs suivantes :

Hôte: localhost - Port: 8118

Pour cachez votre langue maternel vous devrez en revanche faire les modifications au sein de votre navigateur.

Les utilisateurs de *Firefox* auront le privilège de pouvoir utiliser l'extension FoxyProxy
ce qui leur dispensera d'installer *Privoxy*.

Il existe une solution "prête à utiliser" sur clé USB nommée TorPark
Même chose avec *Opera* au lieu de *Firefox* :
http://letwist.net/operator

D'autres fuites sont possibles par le biais du protocole HTTP. Avec une applet *Java* ou une animation *Flash* il est possible pour un site d'établir une connection directe avec vous et d'obtenir votre réelle adresse IP.
Quelques pages sur Internet parviennent à donner votre véritable adresse IP meme si vous utilisez *Tor* :
http://www.inet-police.com/cgi-bin/env.cgi
http://www.stayinvisible.com/cgi-bin/iptest.cgi
http://metasploit.com/research/misc/decloak/

Les deux premières pages se basent sur une méthode assez simple (une requête HTTP qui ne passe pas par le proxy).
La méthode de *Metasploit* est bien plus avancée et utilise un paquet UDP pour trouver l'ip du visiteur.

Solution la plus simple : désactiver *Java* et *Flash* dans votre navigateur.
Pour *Firefox* deux extensions sont disponibles permettant de bloquer les plugins :
http://www.noscript.net/whats
http://flashblock.mozdev.org/

Il va de soit que très peu de sites pensent à mettre de tels systèmes en place pour obtenir votre adresse IP.

Pour ceux qui désirent aller plus loin, il est possible de faire passer TOUS les paquets TCP de façon transparente à travers le réseau *Tor*. Le principe consiste à rediriger par iptables les connexions vers un proxy spécial afin d'anonymiser les applications les plus récalcitrantes à l'utilisation d'un proxy.

Deux implémentations :
TranSocks
trans-proxy-tor
Quelques documents pour utiliser *Transocks* :
http://wiki.noreply.org/noreply/TheOnionRouter/Transocks
http://wiki.noreply.org/noreply/TheOnionRouter/TransocksifyingTor

Les hiddens services
Les nodes présentes sur le réseau *Tor* ont la possibilité de faire tourner des services cachés. Ils sont accessibles par des noms de domaine spéciaux qui ne sont reconnus qu'à l'intérieur du reseau *Tor*. Il est donc en théorie impossible de retrouver la machine faisant tourner ce service.

Quelques hiddens services bien connus :
Le HiddenWiki ou vous pourrez trouver les addresses d'un bon nombre d'hidden services

Researchers Underground, forum pour paranos uniquement (discussions sur les gouvernements, les services secrets etc)

TorNet ORC : un serveur IRC

Quelques défauts d'implémentation ont été trouvé par le passé mais le développement de *Tor* est très rapide et les bugs sont fixés rapidement. Veillez à toujours avoir la dernière version.

Tor ne doit pas être utilisé à la va-vite. Si vous utilisez la même node *Tor* pour pirater et lire votre courrier et que cette node se fait réquisitionner par la police, ils n'auront pas de mal a faire le rapprochement.
N'hesitez pas a utiliser deux navigateurs webs, deux clients IRC etc. L'un anonymisé, l'autre non. L'ideal étant d'avoir deux machines, l'une d'elle étant intraçable.

Une node *Tor* est par défaut configurée en client. Personne d'autre que vous ne pourra l'utiliser. Si vous souhaitez partager votre connection (c'est tout à votre honneur) vous avez la possibilité de choisir si la node doit être une middle ou une exit.
Les nodes de sorties (exit node) sont les seules visibles de l'extérieur du réseau et les seules qui seront dans les logs des serveurs. Faites les tourner avec précaution (il est préférable de partager une machine dédiée chez un hebergeur plutôt que votre machine personnelle si vous ne souhaitez pas avoir une éventuelle visite de la police)

Gardez à l'esprit que si vous utilisez *Tor* pour pirater alors vous n'êtes certainement pas le seul. Ainsi un étudiant s'était fait arrêter pour avoir piraté une cible et avoir laissé des messages... désobligeants. Il s'est avéré qu'en fait il faisait gentiment tourner un Onion Router chez lui (ou alors il a bien réussi à baratiner).
Vous pouvez d'ailleurs, si vous le souhaitez, faire croire que votre machine a servi de relais... mais à vos risques et périls.

Vous êtes dans votre droit à faire fonctionner un service d'anonymat et jusqu'à présent les utilisateurs de *Tor* s'en sont tirés sans gros problèmes, juste quelques heures perdues.

Some legal trouble with TOR in France : http://archives.seul.org/or/talk/May-2006/msg00074.html
confiscating middleman-tor-nodes : http://archives.seul.org/or/talk/Sep-2006/msg00107.html

La deuxième affaire est récente et on attend toujours la conclusion de cette affaire. Ne vous fiez pas au titre du sujet, seules des nodes de sorties sont concernées.

Pour cloturer ce chapitre sur *Tor*, voici quelques outils supplementaires :
Deux interfaces graphiques
TorK
Vidalia
Différents outils relatifs à *Tor* :
http://board.planetpeer.de/index.php/topic,981.0.html

Toujours sur le concept des relais, on trouve *JAP* qui permet de se connecter de façon cryptée à travers des 'mixes' pour surfer sur le web.
http://anon.inf.tu-dresden.de/index_en.html
En revanche suite à une affaire, *JAP* indique clairement qu'en cas d'utilisation pour piratage il remettra comme il se doit les informations qu'il possède pour retrouver l'auteur du crime.
Ajoutons à ça le fait que les mixes se situent tous en Allemagne et que la dernière génération de mixes contient une backdoor permettant de détecter une éventuelle attaque :
http://sourceforge.net/forum/forum.php?thread_id=909637&forum_id=42120
Bref a utiliser seulement pour crypter son traffic web 'innocent' mais pas pour faire une intrusion. Le logiciel est extrêmement simple à utiliser et programmé en Java.

Un constructeur propose un routeur qui anonymisera vos connexions à travers *Tor*, *JAP* et *Freenet* :
http://www.gibraltar.at/content/view/19/32/lang,en/

P2P :

Les arrestations dans le milieu Warez, la loi *DADVSI*, les boards qui ferment... le P2P est un probleme

sérieux. Il est évident que les taggeurs de FTP ont une génération de retard. Pourquoi aller pirater des FTP d'entreprises quand il existe des moyens plus sûrs et plus persistants de partager des fichiers ?

En dehors des outils de téléchargements devenus classiques (*eMule*, *BitTorrent*) il existe des solutions permettant le cryptage des communications et preservant l'anonymat de l'internaute. La plupart de ces solutions peuvent être trouvées en visitant l'excellent site Open-Files

Si ces logiciels attirent peu de monde c'est parce qu'ils n'ont pas certaines fonctionnalités auxquelles nous nous sommes habitués, en particulier le multi-sourcing (télécharger differents morceaux d'un fichier sur plusieurs sources au même moment)

Parmi les logiciels existants :
GNUnet
Un système lent, avec tres peu de fichiers et un systeme de recherche à revoir complétement

ANts P2P
Déjà plus performant, basé sur Java mais toujours très peu de fichiers

MUTE
Kommute (version pour Linux)
Plus agréable et plus performant. Mais nécessite encore beaucoup d'améliorations

WASTE
Different outils se basant sur le principe du P2P

Freenet
Sur le même principe (un reseau et des logiciels qui tournent autour)

Share
Ce logiciel made in Japan est pas mal utilisé dans son pays d'origine. La communauté française a l'air assez bien developpée.

Kameleon
LE logiciel que tout le monde attend, avec support du multi-sourcing... si toutefois il sort un jour.

USENET :

USENET est un système de forums de discussions (les newsgroups) réseaux organisé en catégorie et sous-catégorie en fonction du thème des messages.
Quand un nouveau message est posté, celui-ci est automatiquement répliqué de serveur de news en serveur de news et très vite archivé par différents services (dont Google Groups).
Techniquement USENET est le meilleur moyen pour ceux qui souhaitent qu'un de leur document devienne immortel sur le réseau des réseaux.
Tous les forums ne sont pas modérés mais les serveurs filtrent les messages pour bloquer le spam.
L'accès au serveurs peut aussi demander un enregistrement de la part de l'utilisateur.
Dans le cas des forums binaires qui permettent d'échanger des fichiers (notamment utilisés pour le P2P), l'accès est souvent payant.

Plusieurs serveurs proposent un accès libre aux forums en texte seul. Citons par exemple BananaSplit qui donne un accès aux forums spécialisés dans l'anonymat et la vie privée. Un forum local dédié à *Tor* existe. La liste de diffusion de *Tor* est aussi lisible sous la forme d'un forum sur ce forum.
Une interface web pour poster des messages est disponible : https://www.bananasplit.info/cgi-bin/anon.cgi

Aioe.org donne accès à un grand nombre de forums text-only.

Motzarella requiert un enregistrement mais est gratuit.

USENET n'est pas anonyme. Les adresses IP sont sauvegardées dans les logs des serveurs et souvent visibles dans les entête des messages (le fonctionnement est très proche des mails). Pour poster de façon anonyme sur USENET vous devez utiliser un remailer, Tor ou encore un relais "Web2News" vous permettant de poster depuis une interface web (Google Groups est un web2news mais nécessite un enregistrement).

La façon la plus sûre de communiquer avec une personne est sans doute le forum *alt.anonymous.messages*. Ce dernier est dédié aux conversations chiffrées. Pour l'utiliser les participants doivent disposer d'une paire clé privée/clé publique non publiée. Ils peuvent alors s'envoyer des messages sans avoir besoin de communiquer directement (sauf pour l'échange des clés publiques). Pour que les participants retrouvent les messages qui leurs sont destinés dans le flux d'information du forum ils doivent se mettre d'accord sur un thème commun dans le titre des messages ou les adresses sources utilisées.
http://groups.google.com/group/alt.anonymous.messages/topics?hl=fr

Les codeurs de virus seront ravis d'apprendre qu'un groupe de discussion est dédié au postage de codes sources malveillants :
http://groups.google.com/group/alt.comp.virus.source.code/topics?hl=fr

Les groupes *fr.rec.radio* et *fr.rec.radio.amateur* pourront convenir aux pirates d'ondes radio.

Une alternative à USENET pour mettre en ligne des codes sources est le nombre croissant de sites "PasteBin". Ces sites proposent de stocker vos codes sources et appliquent en plus une coloration syntaxique.

Blogs anonymes :

Livelyblog vous aidera à créer un blog anonyme.
Le remailer *Eelbash* propose aussi un système de blogs anonymes :
http://groups.google.com/group/alt.privacy.anon-server/browse_thread/thread/78e430926ac8a887/fa1b02e4594230b7
ou plus simple :
http://eelbash.yi.org:8080/blogmain/

Sur son disque :

La première règle est "On ne garde pas de traces sur son disque".
La seconde règle est "Quoi qu'il arrive, ne gardez aucune trace sur votre disque pouvant prouver que vous êtes l'auteur d'une intrusion".
La troisième règle est "Ne conservez jamais de preuves sur votre disque".
C'est clair ? Votre PC doit être propre comme une jeune communiante.

Pour cela, **effacez vos données de manière sûre**.

En fonction du systeme de fichier utilisé, les résultats seront plus ou moins efficaces. Les systèmes de fichiers journalisés gardent une copie des métadonnés du fichier (nom de fichier, timestamp, permissions), certains gardent même des copies des blocks de données utilisés par le fichier. Renseignez-vous sur votre système de fichier avant de l'utiliser.
http://www.infoanarchy.org/en/File_wipe

Pour les systèmes non-journalisés, un écrasement des données suffira à se débarasser du contenu du fichier. Les métadonnées resteront jusqu'à ce qu'elles soient à leur tour écrasées.
Les outils d'effacement sécurisé des fichiers (shred, srm, wipe) ne fonctionnent à 100% que sur ext2 et fat32. Sur d'autres systèmes de fichiers, les logs mettront en évidence qu'une suppression a eu lieu en donnant plus ou moins d'informations.
En fait plus le système de fichier est récent, moins il est maitrisé, moins il existe d'outils pour le manipuler.

En fait il n'y a pas 36 façons pour ces systèmes de fichiers :
- soit vous wipez toute la partoche d'un coup

- soit vous utilisez un système de fichier crypté par dessus

Pour wiper une partition entière on peut utiliser tout simplement la commande dd plusieurs fois de suite avec comme source /dev/urandom ou /dev/zero.
Pour wiper la swap (important aussi), utilisez la commande suivante :

```
swapoff /dev/hdaX
dd if=/dev/zero of=/dev/hdaX
```

et pour la remettre en marche :

```
mkswap -c /dev/hdaX
swapon /dev/hdaX
```

Une clé du registre *Windows* permet d'activer l'écrasement automatique des pages mémoires inutilisées, empéchant ainsi les données sensibles d'être présentes en mémoire :
http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/regentry/29930.mspx?mfr=true
http://www.iusmentis.com/security/filewiping/wipeswap/

Pour *Linux* il faut avoir recours à des patch noyau comme *grsec*.
http://seccure.blogspot.com/2006/08/grsecurity-and-forensic-analysis.html

Enfin si vous avez du temps devant vous, vous pouvez utiliser *Darik's Boot and Nuke* (DBAN), une disquette ou CD de boot qui se chargera de wiper le disque proprement.
Projet similaire, le h9.DiskShredder développé par les créateurs du magazine *hakin9*
Jetico a crée un Live CD basé sur son wiper BCWipe

Une vidéo parlant de *DBAN* (pas très sérieuse) :
http://media.g4tv.com/video/ttv/thescreensavers/2003/ss030130b_165_0.asf

Dernières notes sur l'effacement sécurisé :
BCWipe a une excellente réputation et tourne sous *Linux* et *Windows*.
Eraser a lui aussi une très bonne réputation. Il se charge apparemment d'effacer l'espace libre sous *Windows* (à utiliser régulièrement avec une dégramentation).
http://www.tolvanen.com/eraser/
http://www.bugbrother.com/eraser/ (doc française)
La défragmentation peut être utilisée comme méthode innocente (mais peu efficace) pour effacer certaines données du disque.
Microsoft met à disposition un utilitaire nommé Cipher.exe qui joue le même rôle que *Eraser*. Il est disponible pour *Windows 2000*, *XP* (et probablement pour les versions plus récentes)

Sous *Linux* il est très facile d'effacer l'espace libre d'un disque. Il suffit de créer un fichier, remplis par des données aléatoires, qui va remplir tout l'espace libre. Ensuite un simple rm et le tour est joué :

```
# dd if=/dev/urandom of=itsakindofmagic
dd: écriture vers `itsakindofmagic': Aucun espace disponible sur le périphérique
9611+0 records in
9610+0 records out
4920320 bytes (4,9 MB) copied, 1,6279 seconde, 3,0 MB/s
```

Pour ce test le système de fichier était très petit. Sur une grosse partition il faut compter un certain temps.
Scrub permet entre autres de réaliser la même opération

The Grugq est le pionnier sur les techniques d'anti-forensics. Selon lui l'objectif de l'anti-forensics n'est pas vraiment d'effacer ses traces à 100% mais de les effacer suffisemment pour occuper la police tout le temps de la garde à vue (24 voir 48 heures) afin qu'ils vous laisse partir tranquillement à la fin. L'objectif est de ralonger le temps d'investigation.
Il est a l'origine d'un kit anti-forensics nommé *The Defiler's Toolkit* (*TDT*) qui permet d'anonymiser un système ext2 en effacant les informations rémanentes.
necrofile se charge d'écraser le contenu des anciens fichiers sur une partition (ceux effaces par un simple rm)
klismafile se charge d'écraser les métadonnées dans un répertoire (nom du fichier et timestamps qui ne sont pas supprimés par rm)

Plus d'informations :
http://www.blackhat.com/presentations/bh-europe-04/bh-eu-04-grugq.pdf
http://www.dhs-team.org/root/~viriiz/ELF/docs/grugq/p59-0x06.txt
Les binaires de *klismafile* et *necrofile* sont trouvables ici :
http://membres.lycos.fr/lotfree/tools/

Une méthode rapide pour rendre difficile l'exploitation des données consiste à n'écraser que les entêtes des fichiers.
Avec *shred* on peut facilement utiliser cette méthode de secours avec les options -s (nombre d'octets à effacer) et -n (nombre d'écrasements).
Combiné avec la commande find pour effacer tous les fichiers dans un répertoire :

```
find /home/hacker -type f -exec shred -u -s 15 -n 1 {} \;
```

on supprime ensuite les répertoires :

```
rm -rf /home/hacker
```

Le résultat n'est pas instantané mais c'est le meilleur compromis entre vitesse et résultat. Les entêtes des fichiers ne dépassent généralement pas les 15 octets.

SDelete peut être considéré comme l'équivalent *Windows* de *shred*

Windows propose quelques astuces permettant de rendre son système moins parlant.
Désactiver la date de dernier accès à un fichier sur NTFS :
http://www.winguides.com/registry/display.php/50/

Les systèmes de fichier cryptés

Certaines distributions *Linux* proposent de chiffrer les partitions lors de l'installation, c'est le cas par exemple de *Mandriva* et *openSUSE*. Presque toutes les distributions intègrent des modules cryptographiques (*CryptoLoop*, *Loop-AES*, *TrueCrypt*...) *TrueCrypt* permet également de créer des partitions cachées.

CryptoLoop est encore souvent présent par défaut dans les distributions malgré ses défauts d'implémentation. *dm-crypt*, son successeur, est bien plus performant et sera sans doute le nouveau standard d'ici quelques temps.
Il est conseillé de lire les tutoriaux suivants :
http://www.saout.de/tikiwiki/tiki-index.php
http://www.saout.de/tikiwiki/tiki-index.php?page=EncryptExistingDevice
http://www.saout.de/tikiwiki/tiki-index.php?page=EncryptedSwap

Sous *Windows* vous n'aurez aucun mal à crypter vous données, notemment avec *EFS* sous *Windows XP*. Petite démonstration en vidéo :
http://www.laboratoire-microsoft.org/videos/1900/

Avec FreeOTFE, vous pouvez créer des disques chiffrés virtuels sous *XP* et *2000.*
Scramdisk est une autre solution de chiffrement des données au vol.

Windows Vista propose un système de chiffrement du disque baptisé *BitLocker* :
http://www.microsoft.com/france/technet/produits/windowsvista/security/bitlockr.mspx

Pour *Linux* et *Windows* il existe BestCrypt qui est très simple d'utilisation et très agréable à utiliser.

Un article de *Vulnerabilite.com* sur les outils de chiffrement Open-Source *Windows* et *Linux* :
http://www.vulnerabilite.com/actu/20061003155340outils_programme_cryptage_chiffrement_open-source.html

Toutefois retenez une bonne chose : si les policiers remarquent un fichier crypté sur votre disque, ils vont vous demander le mot de passe ou avec quel logiciel ils peuvent le lire. Tout refus à divulguer le password sera perçu comme un refus de collaborer et ça c'est très mauvais pour vous. Quand vous vous retrouverez face à un juge d'instruction qui dressera de vous un portrait de dangereux cyber-terroriste vous donnerez alors votre phrase de passe sans broncher, peut-être même avec soulagement.

Conclusion : si vous avez des informations compromettantes (par exemple IP, login et pass de vos cibles) dissimulez les à l'aide de la stéganographie.
De plus si vous tenez à ces informations, ne les gardez pas sur votre dur puisque votre matériel sera réquisitionné. Uploadez le fichier stéganographié sur le web à un endroit dont vous vous rapellerez.

Il n'est pas difficile de retrouver une aiguille dans une botte de foin en informatique. Mais il est beaucoup plus difficile de retrouver une paille de foin précise dans une botte de foin.
Quand vous cachez un document prenez soin de le mettre au milieu d'un bon nombre de documents anodins et de même type. Vous pouvez aussi encoder tout et n'importe quoi (photos de votre chien, mp3, support de cours...) afin de décourager les enquêteurs.

Désactivez la génération des logs sur votre propre machine. Le plus important est sans doute votre *.bash_history* qui peut être très dangereux pour vous.
Le faire pointer vers */dev/null* donne une bonne alternative entre sécurité et confort (les commandes sont gardées en mémoire uniquement pour la session bash courante).
Bien entendu assurez vous que vos logiciels de chats (IRC, IM, clients mails) ne génèrent pas de logs.
Une bonne façon de découvrir des fichiers de logs consiste à utiliser la commande *lsof* pour voir quels fichiers sont ouverts par quels programmes.
Ne gardez pas non plus d'adresses de contacts (adresses réelles ou adresses mails etc) sur votre disque. De cette façon vous éviterez la propagation des emmerdes sur vos amis et vous ne serez pas "ratachés" à d'autres personnes peut-être déjà connus des services de police.
Pensez aussi à configurer votre navigateur Internet pour qu'il vide son cache à chaque fermeture.
Pour résumer, utilisez le moins possible votre disque.
Attention aux logiciels qui font une copie de vos fichiers lorsque vous travaillez dessus (Les outils de la suite *MS Office*, *VIM*...)

L'Internet est assez gros pour contenir certaines de vos données.
Par exemple il existe des sites Internet vous permettant d'avoir un "bureau" en ligne où stocker vos bookmarks, laisser des notes... On peut citer par exemple Netvibes.

Google Docs (anciennement Writely) vous permet d'écrire des documents en ligne et de les sauvegarder sur leur site. N'oubliez pas d'utiliser le support SSL !

Il existe des services d'espace disque virtuel qui proposent de stocker jusqu'à 25Go de données. Ce qui les différencie est entre autre les méthodes de transfert des fichiers.
http://www.50megs.com/ (50Mo)

http://www.drivehq.com/ (1Go)
http://www.streamload.com/ (25Go)
http://foreversafe.com/ (10Go)
http://box.net/ (1Go)

Flickr peut vous servir à mettre en ligne vos images stéganographiées.

Si vous pensez être capable de vous débrouiller sans disque dûr, débranchez-le et utilisez un Live CD.

Pour finir sur la cryptographie, voici un Wiki très intéressant sur le sujet :
http://www.infoanarchy.org/en/Main_Page
ainsi que des live CDs qui font apparemment tourner un FS crypté :
https://systemausfall.org/trac/cryptobox/wiki/CryptoBox/en
http://www.brum2600.net/projects/LSL/brumix.html
http://www.nongnu.org/k-mib/ (français)
Il existe une distribution Linux qui semble installer par défaut un système de fichier cryptée. Elle a été crée afin de satisfaire les besoins en sécurité du gouvernement allemand :
http://distrowatch.com/table.php?distribution=erposs
http://www.bsi.de/produkte/erposs/

Sur papier :

On peut être né avec un clavier dans les mains, on a toujours tendance à utiliser des feuilles de papier pour gribouiller quelques infos, dessiner une carte d'un réseau, faire l'ébauche d'un projet...
Les même dangers s'appliquent donc sur papier et les précautions à prendre sont les même que pour les supports informatiques.
Cela peut sembler excessif mais pourquoi ne pas avoir recours à une forme de cryptographie sur papier ? Avoir par exemple recours à des moyens mnémotechniques.
Pour effacer vos traces il peut être utile d'investir dans un broyeur...
Une chose est sûre : plus vous utiliserez votre propre mémoire et moins vous aurez de problèmes.

Sur cds, clés, disquettes :

Quand vous sauvegardez vos données sur support amovible, prenez soin de dissimuler les documents (stéganographie).
Sous *Linux* avec le programme aespipe vous pouvez chiffrer une image iso avec une clé secrète avant de la graver :
http://www.geekcomix.com/cgi-bin/classnotes/wiki.pl?UNIX03/Encryption_With_Aespipe
Sur un CD (ou DVD) réinscriptible il sera difficile de déterminer s'il s'agit de données chiffrées ou d'un disque vierge.
Pour tromper la police vous pouvez aussi donner un faux libellé à vos CDs, par exemple en écrivant dessus le nom d'une distribution *Linux* au marqueur... voire pourquoi pas, créer une arborescence qui fera croire qu'il s'agit effectivement d'un CD d'install ou d'un Live CD.

PARTIE II : COMMENT SURVIVRE A UN BUST

Boum Boumm

Ca frappe, ils sont à votre porte... Visiblement vous n'avez pas tenu compte de la première partie de ce document ou n'avez pas pris les mesures nécessaires pour vous refaire une cyber-identité bien propre.
Ou encore vous avez été dénoncé... et là... plus grand chose à faire.

Dans tous les cas une règle stricte :
TOUJOURS REGARDER DE QUI IL S'AGIT AVANT D'OUVRIR !!
Si vous voyez plusieurs personnes en civil avec des armes à la ceinture ou un écusson de la police quelque part... ce sera probablement eux.

Posez-vous une question : Est-ce qu'ils savent si vous êtes ou non chez vous ?
Si vous écoutiez de la musique à fond et que les fenêtres sont grandes ouvertes aucun doute qu'ils se doutent de votre présence.
Réfléchissez à autre chose : est-ce que vous avez reçu un petit coup de fil récemment ? Du genre vous décrochez puis personne ne réponds de l'autre côté de la ligne !?

Si vous ne leur avez pas ouvert sans avoir vérifié avant qui c'était vous avez le temps de lancer quelques commandes rapides. C'est pour cela que vous devez impérativement avoir pris le temps de mettre en pratique ce qui est décrit dans la première partie.
Gardez à l'esprit que vous ne pouvez pas vous accorder plus de 5 minutes. Au delà vous êtes bon pour un sacré interrogatoire sur ce que vous avez fait pendant ce laps de temps.
Il est important de s'être préparé AVANT. Par exemple en ayant crée une petite partition de quelques Mo sur laquelle vous conservez vos documents dangereux.
Il vous suffira alors de passer *dd* plusieurs fois dessus pour effacer vos traces.
Je vous conseille aussi d'utiliser une partition spéciale pour /home.
Si vous utilisiez un volume crypté il vous suffira alors de l'effacer avec un simple rm.
Quoiqu'il arrive ne causez pas de dégats à votre matériel. Cela prouverait que vous avez des informations à cacher.

Qui sont-ils ?

Vos pires cauchemards portent un nom.
L'*O.C.L.C.T.I.C* (*Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication*) que l'on prononcera "Oh c'est elle c'est tique".
Site Internet :
http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

ou encore la *B.E.F.T.I.* (*Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information*.)

Ces deux là travaillent à priori main dans la main. On pourrait aussi ajouter la *D.S.T.* (*Direction de la Surveillance du Territoire*) mais son rôle est tout autre comme écrit sur sa page web :

> Concrètement, les missions de la *D.S.T.* sont traditionnellement de trois types : contre-espionnage, contre-terrorisme, protection du patrimoine économique et scientifique.

Quelle est la différence entre *OCLCTIC* et *BEFTI* ?
La circonscription géographique de compétence de la *BEFTI* comprend la ville de *Paris* (75) ainsi que trois départements de la région parisienne (92, 93, 94).
L'*OCLCTIC* mène des enquêtes de portée nationale (le reste de la *France*) ou internationale.

Toutes deux font parti de la Police Judiciaire, elles travaillent essentiellement suite à des plaintes. Donc en règle générale il faut qu'une plainte soit portée pour l'une de vos intrusions pour qu'ils s'intéressent à vous. Notez bien le "en règle générale".

Leur mission est d'enquêter sur les infractions visant ou utilisant des systèmes informatiques ainsi que les modes de traitement, de stockage et de communication de l'information.

L'ancêtre de l'*OCLCTIC* se nommait la *BCRCI* (*Brigade Centrale de Répression de la Criminalité Informatique*) dont la création remonte à 1994. Elle disposait d'un nombre d'effectifs très limité (une dizaine) alors que l'*OCLCTIC* devrait compter 600 cyber-flics à la fin de l'année 2007.

L'ancêtre de la *BEFTI* n'est autre que le *SEFTI* (*Service* etc).

Sinon aussi :
Le *STRJD* (*Service Technique de Recherche Judiciaire et de Documentation*)
Ce service est chargé de l'exploitation et de la centralisation de différents fichiers policiers.

Il intégre une division de lutte contre la cybercriminalité. La mission de cette division est principalement de constater les infractions sur les sites Internet (diffamation, incitations au crime, menaces mais aussi mise en téléchargement de documents protégés par le droit d'auteur)
Elle a aussi une mission de surveillance des réseaux et analyse sites, forums, channels IRC, réseaux P2P etc)

L'*Institut de Recherche Criminelle de la Gendarmerie Nationale* (*IRCGN*) chargée de l'expertise judiciaire en matière de preuve numérique.

La coopération Européenne en matière de cyberciminalité se nomme l'*ENISA* (agence européenne chargée de la sécurité des réseaux) :
http://www.enisa.europa.eu/
Ces coopérations ont principalement été décidées à la *convention de Budapest* le 23 novembre 2001.
Au niveau mondial, le G8 s'est penché sur le problème avec sa *"Charte d'Okinawa sur la société mondiale de l'information"*

Sites et documents traitant de la lutte contre la cyber-criminalité :

Un blog sur la cyber-police : http://www.cyber-police.org/
(Attention, même si le site prétend ne pas être rattaché à un service de police, voir ici il est toutefois préférable d'avoir un certain recul là dessus).

Document plus ou moins officiel sur le rôle de l'*OCLCTIC* :
http://www.meleenumerique.com/annexeven/archmn6/Pres/OCLCTIC.pdf

Rapport d'une policière stagiaire au *BEFTI* (donne de bonnes informations sur les rôles de chaque service) :
http://dess-droit-internet.univ-paris1.fr/bibliotheque/IMG/doc/2003_sept_OK_Dine_Dominique_Rap_Stage_BEFTI_lutte_contre_cyb.doc

Un article sur le *STRJD* :
http://www.zataz.com/reportages-securite/9050/gendarme-du-net.html

Interview de *Catherine Chambon*, chef de l'*OCLCTIC* :
http://www.magsecurs.com/IMG/pdf/MAG_SECURS_INTER_N3.pdf

News sur l'arrestation de *ReYn0* par l'*OCLCTIC* :
http://www.zataz.com/index.php?action=news&id=1687

L'*OCLCTIC* et les yescards :
http://www.echosdunet.net/news/index.php?id_news=147

Arrestation de *DKD[*|| par l'*OCLCTIC* :
http://www.zone-h.org/en/news/read/id=2954/
http://www.zone-h.org/en/news/read/id=2962/
http://www.zone-h.fr/fr/news/read/id=0014/

L'affaire des blogs pour appel à émeute :
http://www.silicon.fr/getarticle.asp?ID=12311

Renforcement de la lutte contre la cyber-criminalité en France :
http://www.whynet.org/actualites/index.php/2005/04/13/585-dominique-de-villepin-lutte-contre-la-cybercriminalite

HZV et l'*OCLCTIC* :
http://www.paranos.com/internet/hackerzvoice.html

Les services français contre la cyber-criminalité :
http://www.fr.ixus.net/modules.php?name=News&sid=560

Satbidouille et l'*OCLCTIC* :
http://zataz.com/index.php?action=news&id=5643

Yanis et l'*OCLCTIC* :
http://zataz.com/news/10587/Premiere-arrestation-d_un-pirate-informatique-ayant-agi-lors-de-la-diffusion-des-caricatures-du-prophete-Mahomet.html

Témoignage anonyme d'un pirate ayant eu affaire à l'*OCLCTIC* :
http://www.zone-h.fr/forum/viewtopic.php?p=381

Emission intéressante sur les menaces du net avec notamment la commissaire Marie Lajus de l'OCLCTIC parmis les invités (dure une heure) :
http://www.zdnet.fr/partenaires/8-fi/0,50008420,39307139,00.htm

m0rtix et l'*OCLCTIC*
http://www.01net.com/editorial/338943/

A lire également
http://www.fr.ixus.net/modules.php?name=News&file=article&sid=9
http://www.legalis.net/breves-article.php3?id_article=976

A noter un message 'amusant' qui s'affiche sur les pages de Google quand l'on fait des recherches sur certains services :

> En réponse à une demande légale adressée à Google, nous avons retiré 1 résultat(s) de cette page. Si vous souhaitez en savoir plus sur cette demande, vous pouvez consulter le site ChillingEffects.org.

En *Suisse*, la cyberpolice se nomme le *SCOCI* :
http://www.scoci.ch/f/index.htm
http://fr.wikipedia.org/wiki/Service_national_de_coordination_de_la_lutte_contre_la_criminalité_sur_Internet

En *Belgique* ils ont le *C.C.U.* (*Computer Crime Unit*)
http://www.polfed-fedpol.be/org/org_dgj_orga_fr.php

Les différents moyens législatifs et judiciaires pour luter contre la cybercriminalité dans les pays de l'Union Européenne :
http://www.csirt-handbook.org.uk/app/index.php?table_name=app_countries

La fouille / perquisition

> Les perquisitions, visites domiciliaires et saisies de pièces à conviction ne peuvent être effectuées sans l'assentiment exprès de la personne chez laquelle l'opération a lieu. Cet assentiment doit faire l'objet d'une déclaration écrite de la main de l'intéressé ou, si celui-ci ne sait écrire, il en est fait mention au procès verbal ainsi que de son assentiment. Les dispositions prévues par les articles 56 et 59 (premier alinéa) sont applicables.

Référence: Article 76 du Code de procédure pénale : Perquisitions dans le cadre de l'enquête préliminaire.

http://lexinter.net/PROCPEN/index.htm

Vous avez donc le droit de ne pas signer... mais les conséquence de ce refus ne sont visiblement pas présentes dans les lois. L'expression qui revient est "en cas de refus de signer, le procès-verbal en fait mention".

Une fois que la police sera entrée dans votre domicile vous ne ferez peut-être pas le "poids" pour refuser la perquisition, d'où l'importance de connaître l'identité des personnes, voire leur poser des questions, avant de les faire entrer.

> A moins que vous mettiez la sono à fond (ce qui est considéré comme du tapage nocturne) ou que la police ait reçu un appel au secours, elle n'a rien à faire chez vous et vous avez le droit de ne pas lui ouvrir. La Constitution le dit clairement, le domicile est un espace inviolable. Les perquisitions doivent avoir lieu entre 6h du matin et 21 heures (art. 62 du code de procédure pénale), sauf pour les cas d'urgence ou de lutte anti-terrorisme. Là, il faut qu'il y ait atteinte à la sûreté de l'État (c'est quand même gros) et encore, l'officier de police doit disposer d'une autorisation écrite du Parquet. Si au cours de la perquisition (pour les raisons que nous avons citées), l'officier fait "une découverte incidente" d'un délit, il dresse un PV et doit normalement quitter les lieux. Sauf s'il décide d'en alerter tout de suite le Parquet qui peut ordonner une interpellation.

Référence :
http://www.selwane.com/index.php?option=com_content&task=view&id=449&Itemid=47

Je ne pense pas qu'un policier qui s'installe devant votre ordinateur et fouille pour finalement y trouver une preuve d'intrusion puisse être considéré comme "une découverte incidente"... pensez-y.

Une fois que vous avez signé l'autorisation de perquisitionner, la police procède à une fouille très minutieuse. Il est très improbable que des documents cachés le restent très longtemps. Ils ont l'habitude de ce genre de chose et savent exactement où chercher et sont très organisés.

Le coup de fil

Vous avez le droit de faire passer un coup de fil par l'intermédiaire de la police. Ce droit est relatif à la garde à vue mais il vous sera peut-être proposé avant d'être amené au commisariat (voire la partie sur la GAV)

La procédure d'analyse forensics

La fouille s'accompagne (si l'une ou plusieurs de vos machines sont allumées) d'une procédure de figeage de l'activité en cours de vos ordinateurs.
La méthodologie utilisée n'est ni plus ni moins celle d'une analyse post-intrusion mis à part que l'analyse concerne ici la machine attaquante et non la machine attaquée.
Les données recueillies sont les informations dites "volatiles" comme les connexions et les processus en cours ou encore le listing des dernières commandes que vous avez tappé.
S'ensuit alors une extinction sauvage de votre matériel (débranchage) visant à garder intact sur le disque la swap ou l'arboresnce /proc (pour Linux).

Les commandes les plus utilisées pour une telle analyse sont *lsof*, *netstat*, *ps* et *history*.
Pour obtenir des infos complètes, la P.J. aura besoin de connaître votre mot de passe root, autrement dit, elle passera par la commande *su*.
Installer un piège dans cette commande peut être votre dernier recours.
Par exemple la saisie d'un mot de passe spécial pourrait engendrer l'effacement rapide d'une petite partition...
Le comportement de *su* ne doit pas différer (en dehors d'une procédure spéciale lançée en background) de la version originale pour ne pas que cela se retourne contre vous.

Vous pouvez aussi rootkiter votre machine pour rendre certaines commandes moins bavardes.

Pour réaliser l'analyse du disque dûr la police a recours a un ordinateur qui ressemble à une grosse valise noire :
http://www.sacasa.fr/medias/pdf/Liberation%2016%20Nov%20Sacasa.pdf
Site du fournisseur :
http://www.sacasa.fr/

La saisie

Signer l'autorisation de perquisition revient à autoriser la saisie de ce qui pourra éventuellement servir de preuves. Globalement il s'agit de tout matériel de stockage de données informatiques (ordinateur, clés usb, cd gravés, console de jeu, appareil photo numérique, lecteur mp3...) ainsi que divers documents papiers vous concernant.

La garde à vue

Vous avez droit à différentes choses :
- droit de voir un médecin
- droit de voir un avocat
- droit de FAIRE prévenir un proche

Pour ce qui est de la durée, elle est de 24 heures minimum. Un magistrat peut ensuite la faire prolonger jusqu'à 48 heures s'il estime que cela peut être profitable à l'enquête.

La garde à vue est bien entendue entrecoupée entre mise en cellule et interrogatoires.
Profitez des périodes d'isolement pour faire le point sur ce que les inspecteurs savent sur vous et pour essayer de vous reposer.
L'objectif de la garde à vue est clairement de vous affaiblir et de vous mettre dans un état de fatigue.
Les cellules sont constamment éclairées et vous ne mangerez pas à votre faim.
Le principe est que dans un tel état vous êtes plus prompt à faire des révélations ou à "craquer" pour mettre un terme à une durée qui semble interminable (perte de notion du temps...)

Sources :
http://www.paxatagore.org/index.php?2006/02/11/608-la-place-de-la-garde-a-vue-dans-le-systeme-inquisitoire

Les interrogatoires

La police va étudier le contenu de votre disque et rechercher des informations vous concernant sur Internet.
Chaque fois qu'ils trouveront des informations qu'ils jugent importantes ils vous feront passer un interrogatoire pour en savoir plus.

Ne tentez pas de cacher certaines informations si vous savez pertinemment qu'elles sont facilement lisibles sur votre disque dur, cela risque de se retourner contre vous.
Plus vous aurez l'air de collaborer, plus les interrogatoires se passeront bien. Mais évitez tout de même d'en dire trop et d'aggraver votre cas. Si vous le pouvez, faites en sorte que votre affaire ne se propage pas trop sur d'autres personnes du milieu.

Le compromis entre les deux est extrémement difficile.

S'ils se doutent que vous leur cachez quelque chose ou que vous leur mentez ils vous mettront la pression (cela fait partie des techniques d'interrogatoire) en haussant le ton et en lachant des paroles plus ou moins provocatrices.

Une fois libre

Bien que l'affaire semble temporairement close jusqu'à convocation devant la justice, rien ne prouve que vous ne serez pas surveillé d'une façon où d'une autre...
Malheureusement les documents disponibles sur le sujet ne sont pas bien parlants.
http://www.foruminternet.org/documents/codes/lire.phtml?id=51

Prenez ce fait en considération et trouvez un moyen sûr de prévenir les personnes sur qui votre affaire pourrait avoir des conséquences néfastes afin qu'ils effacent vite fait le contenu de leurs disques dûr.

Les peines

Rappelons les articles du code pénal relatifs au piratage informatique :

Article 323-1
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2
Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3
Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3-1
Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4
La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5
Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

- L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
- L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

- La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
- La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
- L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
- L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6
Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.
Les peines encourues par les personnes morales sont :

- L'amende, suivant les modalités prévues par l'article 131-38 ;
- Les peines mentionnées à l'article 131-39.

Article 323-7
La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

Infos :
http://www.legifrance.gouv.fr/WAspad/VisuArticleCode?commun=&code=&h0=CPENALLL.rcv&h1=3&h3=30
Veuillez vous reportez aux lois de votre pays.

Certes les peines sont lourdes mais elles n'atteignent tout de même pas celles encouruent pour un viol ou d'autres actes violents (il reste encore une certaine logique).
Certains points peuvent parraître stupides, notamment conçernant la "modification" de données puisque la simple consultation d'un site Internet suffit à ajouter des lignes dans un fichier de log ou ajouter des entrées dans une base de donnée...
La loi interdit clairement la création d'exploits ou d'autres programmes de piratage... tout ce que vous avez codé jusqu'au jour de votre arrestation peut donc être utilisé contre vous.
Si vous tenez vraiment à releaser vos codes faites le dans l'anonymat total.
Les peines qui peuvent s'ajouter, comme l'interdiction d'exercer un travail dans la sécurité informatique, ou l'informatique tout court sont également très dures.

Il est inutile de dire que la meilleure façon d'éviter ces peines c'est de ne rien faire d'illégal. Le piratage c'est "fun", ok, mais l'informatique c'est vaste et en cherchant un peu vous trouverez bien un moyen

propre d'utiliser votre cervelle et votre ordinateur.

Les peines données çi-dessus peuvent être largement allégées ou alourdies en fonction de différents paramêtres :

- Vous avez un casier judiciaire vierge (opposé : vous êtes récidiviste)
- Vous êtes mineur
- Vos intentions n'étaient pas réellement néfastes (pour le "challenge"... n'utilisez pas un tel argument si vous faites des DDoS)
- Vous ne recherchiez pas à tirer profit (économiquement ou pas) de vos attaques

Les peines peuvent aussi être allégées pour les jeunes qui sont dans un contexte social ou familial difficile (du moins cela peut-être utilisé par votre avocat).

Evitez tout de même de plaider que vous êtes mentalement attardé... les pirates ont toujours la réputation d'être des personnes intelligentes donc ça risquerait de ne pas passer.

Après

Une fois la mésaventure du bust avec la gav, les interrogatoires, le procès et les peines passés, vous avez deux choix :

- trouver des activités légales dans la sécu info
- reprendre au début de ce paper

Ne faites pas les idiots, si vous vous faites choper une seconde fois vous aurez tout le temps pour le regretter.

Un bétisier des gaffes à ne pas faire ?

Allez, pour rire un peu voici quelques exemples à ne pas suivre :

AloneTrio qui défaçait des sites en laissant son C.V.

ChinaHacker qui passe ses journées à défacer des sites gouvernementaux Chinois alors qu'il l'est probablement lui-même (c'est la potence qui l'attends)

Tous ceux qui publient des comptes-rendu d'intrusion, des listes de logins/pass ou demandent publiquement de l'aide pour pirater un serveur spécifique.

Le gamin qui avait mis en circulation une version d'un ver informatique et qui s'en était vanté auprès de ses "amis" qui l'ont ensuite dénonçé contre de l'argent.

Archiver toutes ses intrusions sur son disque avec une galerie de défaces.

Le mec qui upload une page d'index avec son nom et son prénom dans une balise méta.

... beaucoup trop d'exemples...

Réflexions

Que pouvons nous faire avec nos petits moyens pour diminuer le nombre de busts ?

- Le présent document est "ouvert", vous êtes libre (et c'est fortement conseille) de le faire circuler sur différentess boards de hacking et vous êtes aussi libre de le modifier pour ajouter ou corriger des informations.

- Organiser une contre surveillance semble plutôt difficile à mettre en oeuvre toutefois ce n'est pas inutile d'y réfléchir.

- Connaître son ennemi en se tenant informé de ses actions, ses pouvoirs et ses techniques. (Toute info conçernant le software utilisé par les services de police serait d'une grande aide, merci de diffuser ces infos de façon anonyme si vous les possedez)

- Utiliser/imaginer des techniques permettant de savoir si l'on est ou non sous surveillance.

  Le site suivant propose par exemple un service permettant de pister vos emails :
  http://www.readnotify.com/

- Développer des programmes permettant le chiffrage des données et des communications ainsi que l'anonymisation des techniques actuelles de piratage.
- Réléchir au problème de la libre diffusion des données et à leur persistance sur Internet afin de protéger la liberté d'expression et combattre la censure.
- Le droit ça a beau être chiant, on en est tous concernés. Il est important de se tenir informé des changements dans les lois, notemment concernant la cyber-surveillance et les restrictions qui risquent d'apparaître sur le net.

Quelques sites de news (dans un ordre quelconque) :

Le forum des droits sur l'Internet
http://www.foruminternet.org/

Site de news sur le droit d'auteur
http://eucd.info/

Spyworld
http://www.spyworld-actu.com/

Big Brother Awards France
http://bigbrotherawards.eu.org/

Le site de *Kitetoa*
http://www.kitetoa.com/

Les nouvelles d'*Hacktivismo* (un projet du *cDc*)
http://www.hacktivismo.com/news/

La ligue *Odebi*
http://www.odebi.org/
et la surveillance de l'Internet à la Française
http://www.odebi.org/lct/Leslogspourlesnuls.html

Commission Nationale de l'Informatique et des Libertés
http://www.cnil.fr/

L'*Electronic Frontier Foundation*

http://www.eff.org/

Le Droit des Techniques d'Information et de Communication
http://www.droit-tic.com/

FFII France
http://www.ffii.fr/

Homo-Numericus rubrique Cybercratie
http://www.homo-numericus.net/rubrique23.html

Privacy International
http://www.privacyinternational.org/

Souriez vous êtes filmés
http://souriez.info/

Dataretention is no solution
http://www.dataretentionisnosolution.com/index.php?lang=fr

Reporters sans frontières - rubrique Internet
http://www.rsf.org/rubrique.php3?id_rubrique=272

d4 n3wS
http://lotfree.next-touch.com/news/

Les archives de *Transfert.net*
http://transfert.net/

Les archives de la liste de discussion *Onion Routing*
http://archives.seul.org/or/talk/

Des documents dans la même optique que le présent document :

Panta Rhei Remailer WiKi
http://www.panta-rhei.eu.org/pantawiki/FrontPage

Exit The Matrix : Anonymous connexions
http://exitthematrix.dod.net/matrixmirror/ar01s07.html

HOWTO bypass Internet Censorship
http://www.zensur.freerk.com/

Merci d'apporter des améliorations à ce document.
Prenez soin de votre anonymat et bon wipage de disque à tous.
Bob.

On crée vos sites Internet, on développe vos logiciels, on défend votre liberté d'expression... Jouez pas au cons avec nous.