

Version : **2020.03** - Consulter le Change Log en fin de module.

Dernière mise-à-jour : 2023/02/15 16:06

LCF307 - Gestion du Balayage des Ports

Contenu du Module

- **LCF307 - Gestion du Balayage des Ports**

- Contenu du Module
- Le Problématique
 - LAB #1 - Utilisation de nmap et de netcat
 - nmap
 - Installation
 - Utilisation
 - Fichiers de Configuration
 - Scripts
 - netcat
 - Utilisation
- Les Contre-Mesures
 - LAB #2 - Mise en place du Système de Détection d'Intrusion Snort
 - Installation
 - Configuration de Snort
 - Editer le fichier `/etc/snort/snort.conf`
 - Utilisation de snort en mode “packet sniffer”
 - Utilisation de snort en mode “packet logger”
 - Journalisation
 - LAB #3 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry
 - Installation
 - Configuration
 - Utilisation

- ChangeLog
 - 2020.01
 - 2020.02
 - 2020.03

Le Problématique

Un **Cheval de Troie** est un binaire qui se cache dans un autre. Il est exécuté suite à l'exécution du binaire hôte par la cible ou par un utilisateur. Le but principal du Cheval de Troie est d'ouvrir une *trappe* (*backdoor*). Les Chevaux de Troie les plus connus sont :

- Back Orifice 2000 - tcp/8787, tcp/54320-21,
- Backdoor - tcp/1999,
- Subseven - tcp/1243, tcp/ 2773, tcp/6711-6713, tcp/7215, tcp/27374, tcp/27573, tcp/54283,
- Socket de Troie - tcp/5001, tcp/30303, tcp/50505.

Le **scan** consiste à balayer les ports d'une machine afin de :

- connaître les ports qui sont ouverts,
- déterminer le système d'exploitation,
- identifier les services ouverts.

Plusieurs scanners existent dont :

- nmap
- netcat

LAB #1 - Utilisation de nmap et de netcat

nmap

Installation

Sous RHEL/CentOS 7, **nmap** n'est pas installé par défaut :

```
[root@centos7 ~]# which nmap
/usr/bin/which: no nmap in (/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin)
```

Installez donc nmap en utilisant yum :

```
[root@centos7 ~]# yum install nmap
Loaded plugins: fastestmirror, langpacks
Reposdata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
adobe-linux-x86_64           | 2.9 kB    00:00
base                        | 3.6 kB    00:00
extras                      | 3.4 kB    00:00
updates                     | 3.4 kB    00:00
(1/3): adobe-linux-x86_64/primary_db | 2.7 kB    00:00
(2/3): extras/7/x86_64/primary_db   | 191 kB    00:00
(3/3): updates/7/x86_64/primary_db  | 7.8 MB    00:04
Determining fastest mirrors
 * base: ftp.rezopole.net
 * extras: ftp.rezopole.net
 * updates: ftp.rezopole.net
Resolving Dependencies
--> Running transaction check
---> Package nmap.x86_64 2:6.40-7.el7 will be installed
--> Processing Dependency: nmap-ncat = 2:6.40-7.el7 for package: 2:nmap-6.40-7.el7.x86_64
--> Running transaction check
---> Package nmap-ncat.x86_64 2:6.40-7.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved
```

```
=====
Package           Arch           Version           Repository        Size
=====
Installing:
nmap              x86_64         2:6.40-7.el7      base              4.0 M
Installing for dependencies:
nmap-ncat         x86_64         2:6.40-7.el7      base              201 k

Transaction Summary
=====
Install 1 Package (+1 Dependent package)

Total download size: 4.2 M
Installed size: 17 M
Is this ok [y/d/N]: y
```

Options de la commande

Les options de cette commande sont :

```
[root@centos7 ~]# nmap --help
Nmap 6.40 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
```

- Pn: Treat all hosts as online -- skip host discovery
- PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
- PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
- PO[protocol list]: IP Protocol Ping
- n/-R: Never do DNS resolution/Always resolve [default: sometimes]
- dns-servers <serv1[,serv2],...>: Specify custom DNS servers
- system-dns: Use OS's DNS resolver
- traceroute: Trace hop path to each host

SCAN TECHNIQUES:

- sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
- sU: UDP Scan
- sN/sF/sX: TCP Null, FIN, and Xmas scans
- scanflags <flags>: Customize TCP scan flags
- sI <zombie host[:probeport]>: Idle scan
- sY/sZ: SCTP INIT/COOKIE-ECHO scans
- s0: IP protocol scan
- b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:

- p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
- F: Fast mode - Scan fewer ports than the default scan
- r: Scan ports consecutively - don't randomize
- top-ports <number>: Scan <number> most common ports
- port-ratio <ratio>: Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:

- sV: Probe open ports to determine service/version info
- version-intensity <level>: Set from 0 (light) to 9 (try all probes)
- version-light: Limit to most likely probes (intensity 2)
- version-all: Try every single probe (intensity 9)
- version-trace: Show detailed version scan activity (for debugging)

SCRIPT SCAN:

- sC: equivalent to --script=default
- script=<Lua scripts>: <Lua scripts> is a comma separated list of directories, script-files or script-categories

```
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma separated list of script-files or
    script-categories.
```

OS DETECTION:

```
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
```

TIMING AND PERFORMANCE:

```
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
    probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
```

FIREWALL/IDS EVASION AND SPOOFING:

```
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
```

--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

OUTPUT:

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:

-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.

EXAMPLES:

```
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
```

SEE THE MAN PAGE (<http://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES

Utilisation

Pour connaître la liste des ports ouverts sur votre machine virtuelle, saisissez la commande suivante :

```
[root@centos7 ~]# nmap 127.0.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2017-08-05 14:17 CEST
Nmap scan report for localhost.localdomain (127.0.0.1)
Host is up (-2100s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind
631/tcp   open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```



Important - Pour connaître les ports ouverts sur une machine distante, la procédure est identique sauf que vous devez utiliser l'adresse IP de votre cible.

Fichiers de Configuration

nmap utilise un fichier spécifique pour identifier les ports. Ce fichier est **/usr/share/nmap/nmap-services**:

```
[root@centos7 ~]# more /usr/share/nmap/nmap-services
# THIS FILE IS GENERATED AUTOMATICALLY FROM A MASTER - DO NOT EDIT.
# EDIT /nmap-private-dev/nmap-services-all IN SVN INSTEAD.
```

```
# Well known service port numbers -*- mode: fundamental; -*-
# From the Nmap Security Scanner ( http://nmap.org )
#
# $Id: nmap-services 31220 2013-07-03 04:30:43Z david $
#
# Derived from IANA data and our own research
#
# This collection of service data is (C) 1996-2011 by Insecure.Com
# LLC. It is distributed under the Nmap Open Source license as
# provided in the COPYING file of the source distribution or at
# http://nmap.org/data/COPYING . Note that this license
# requires you to license your own work under a compatible open source
# license. If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see http://nmap.org/book/man-legal.html
#
# Fields in this file are: Service name, portnum/protocol, open-frequency, optional comments
#
tcpmux 1/tcp 0.001995 # TCP Port Service Multiplexer [rfc-1078]
tcpmux 1/udp 0.001236 # TCP Port Service Multiplexer
compressnet 2/tcp 0.000013 # Management Utility
compressnet 2/udp 0.001845 # Management Utility
compressnet 3/tcp 0.001242 # Compression Process
compressnet 3/udp 0.001532 # Compression Process
unknown 4/tcp 0.000477
rje 5/udp 0.000593 # Remote Job Entry
unknown 6/tcp 0.000502
echo 7/sctp 0.000000
echo 7/tcp 0.004855
echo 7/udp 0.024679
unknown 8/tcp 0.000013
--More-- (0%)
```

Le répertoire **/usr/share/nmap** contient d'autres fichiers importants :

```
[root@centos7 ~]# ls -l /usr/share/nmap
total 6548
-rw-r--r--. 1 root root 10546 Nov 20 2015 nmap.dtd
-rw-r--r--. 1 root root 455371 Nov 20 2015 nmap-mac-prefixes
-rw-r--r--. 1 root root 3694559 Nov 20 2015 nmap-os-db
-rw-r--r--. 1 root root 11749 Nov 20 2015 nmap-payloads
-rw-r--r--. 1 root root 6631 Nov 20 2015 nmap-protocols
-rw-r--r--. 1 root root 49243 Nov 20 2015 nmap-rpc
-rw-r--r--. 1 root root 1727204 Nov 20 2015 nmap-service-probes
-rw-r--r--. 1 root root 622039 Nov 20 2015 nmap-services
-rw-r--r--. 1 root root 31935 Nov 20 2015 nmap.xsl
drwxr-xr-x. 3 root root 4096 Aug 5 14:16 nselib
-rw-r--r--. 1 root root 47190 Nov 20 2015 nse_main.lua
drwxr-xr-x. 2 root root 20480 Aug 5 14:16 scripts
```

Voici la liste des fichiers les plus importants :

Fichier	Description
/usr/share/nmap/nmap-protocols	Contient la liste des protocoles reconnus par nmap .
/usr/share/nmap/nmap-service-probes	Contient les règles de balayage utilisées par nmap pour identifier le service actif sur un port donné.
/usr/share/nmap/nmap-mac-prefixes	Contient une liste de préfix d'adresses MAC par fabricant reconnu par nmap .
/usr/share/nmap/nmap-rpc	Contient une liste des services RPC reconnus par nmap .

Scripts

nmap utilise des scripts pour accomplir certaines tâches allant de la découverte simple de ports ouverts jusqu'à l'intrusion :

```
[root@centos7 ~]# ls /usr/share/nmap/scripts/
acarsd-info.nse          http-domino-enum-passwords.nse    ndmp-version.nse
address-info.nse         http-drupal-enum-users.nse        nessus-brute.nse
afp-brute.nse            http-drupal-modules.nse          nessus-xmlrpc-brute.nse
```

afp-ls.nse	http-email-harvest.nse	netbus-auth-bypass.nse
afp-path-vuln.nse	http-enum.nse	netbus-brute.nse
afp-serverinfo.nse	http-exif-spider.nse	netbus-info.nse
afp-showmount.nse	http-favicon.nse	netbus-version.nse
ajp-auth.nse	http-fileupload-exploiter.nse	nexpose-brute.nse
ajp-brute.nse	http-form-brute.nse	nfs-ls.nse
ajp-headers.nse	http-form-fuzzer.nse	nfs-showmount.nse
ajp-methods.nse	http-frontpage-login.nse	nfs-statfs.nse
ajp-request.nse	http-generator.nse	nping-brute.nse
amqp-info.nse	http-git.nse	nrpe-enum.nse
asn-query.nse	http-gitweb-projects-enum.nse	ntp-info.nse
auth-owners.nse	http-google-malware.nse	ntp-monlist.nse
auth-spoof.nse	http-grep.nse	omp2-brute.nse
backorifice-brute.nse	http-headers.nse	omp2-enum-targets.nse
backorifice-info.nse	http-huawei-hg5xx-vuln.nse	openlookup-info.nse
banner.nse	http-icloud-findmyiphone.nse	openvas-otp-brute.nse
bitcoin-getaddr.nse	http-icloud-sendmsg.nse	oracle-brute.nse
bitcoin-info.nse	http-iis-webdav-vuln.nse	oracle-brute-stealth.nse
bitcoinrpc-info.nse	http-joomla-brute.nse	oracle-enum-users.nse
bittorrent-discovery.nse	http-litespeed-sourcecode-download.nse	oracle-sid-brute.nse
bjnp-discover.nse	http-majordomo2-dir-traversal.nse	ovs-agent-version.nse
broadcast-ataoe-discover.nse	http-malware-host.nse	p2p-conficker.nse
broadcast-avahi-dos.nse	http-methods.nse	path-mtu.nse
broadcast-bjnp-discover.nse	http-method-tamper.nse	pcanywhere-brute.nse
broadcast-db2-discover.nse	http-open-proxy.nse	pgsql-brute.nse
broadcast-dhcp6-discover.nse	http-open-redirect.nse	pjl-ready-message.nse
broadcast-dhcp-discover.nse	http-passwd.nse	pop3-brute.nse
broadcast-dns-service-discovery.nse	http-phpmyadmin-dir-traversal.nse	pop3-capabilities.nse
broadcast-dropbox-listener.nse	http-phpself-xss.nse	pptp-version.nse
broadcast-eigrp-discovery.nse	http-php-version.nse	qscan.nse
broadcast-igmp-discovery.nse	http-proxy-brute.nse	quake3-info.nse
broadcast-listener.nse	http-put.nse	quake3-master-getservers.nse
broadcast-ms-sql-discover.nse	http-qnap-nas-info.nse	rdp-enum-encryption.nse
broadcast-netbios-master-browser.nse	http-rfi-spider.nse	rdp-vuln-ms12-020.nse

broadcast-networker-discover.nse	http-robots.txt.nse	realvnc-auth-bypass.nse
broadcast-novell-locate.nse	http-robtex-reverse-ip.nse	redis-brute.nse
broadcast-pc-anywhere.nse	http-robtex-shared-ns.nse	redis-info.nse
broadcast-pc-duo.nse	http-sitemap-generator.nse	resolveall.nse
broadcast-pim-discovery.nse	http-slowloris-check.nse	reverse-index.nse
broadcast-ping.nse	http-slowloris.nse	rexec-brute.nse
broadcast-pppoe-discover.nse	http-sql-injection.nse	riak-http-info.nse
broadcast-rip-discover.nse	http-stored-xss.nse	rlogin-brute.nse
broadcast-ripng-discover.nse	http-title.nse	rmi-dumpregistry.nse
broadcast-sybase-asa-discover.nse	http-tplink-dir-traversal.nse	rmi-vuln-classloader.nse
broadcast-tellstick-discover.nse	http-trace.nse	rpcap-brute.nse
broadcast-upnp-info.nse	http-traceroute.nse	rpcap-info.nse
broadcast-versant-locate.nse	http-unsafe-output-escaping.nse	rpc-grind.nse
broadcast-wake-on-lan.nse	http-userdir-enum.nse	rpcinfo.nse
broadcast-wpad-discover.nse	http-vhosts.nse	rsync-brute.nse
broadcast-wsdd-discover.nse	http-virustotal.nse	rsync-list-modules.nse
broadcast-xmcp-discover.nse	http-vlcstreamer-ls.nse	rtsp-methods.nse
cassandra-brute.nse	http-vmware-path-vuln.nse	rtsp-url-brute.nse
cassandra-info.nse	http-vuln-cve2009-3960.nse	samba-vuln-cve-2012-1182.nse
cccam-version.nse	http-vuln-cve2010-0738.nse	script.db
citrix-brute-xml.nse	http-vuln-cve2010-2861.nse	servicetags.nse
citrix-enum-apps.nse	http-vuln-cve2011-3192.nse	sip-brute.nse
citrix-enum-apps-xml.nse	http-vuln-cve2011-3368.nse	sip-call-spoof.nse
citrix-enum-servers.nse	http-vuln-cve2012-1823.nse	sip-enum-users.nse
citrix-enum-servers-xml.nse	http-vuln-cve2013-0156.nse	sip-methods.nse
couchdb-databases.nse	http-waf-detect.nse	skypev2-version.nse
couchdb-stats.nse	http-waf-fingerprint.nse	smb-brute.nse
creds-summary.nse	http-wordpress-brute.nse	smb-check-vulns.nse
cups-info.nse	http-wordpress-enum.nse	smb-enum-domains.nse
cups-queue-info.nse	http-wordpress-plugins.nse	smb-enum-groups.nse
cvs-brute.nse	iax2-brute.nse	smb-enum-processes.nse
cvs-brute-repository.nse	iax2-version.nse	smb-enum-sessions.nse
daap-get-library.nse	icap-info.nse	smb-enum-shares.nse
daytime.nse	ike-version.nse	smb-enum-users.nse

db2-das-info.nse	imap-brute.nse	smb-flood.nse
db2-discover.nse	imap-capabilities.nse	smb-ls.nse
dhcp-discover.nse	informix-brute.nse	smb-mbenum.nse
dict-info.nse	informix-query.nse	smb-os-discovery.nse
distcc-cve2004-2687.nse	informix-tables.nse	smb-print-text.nse
dns-blacklist.nse	ip-forwarding.nse	smb-psexec.nse
dns-brute.nse	ip-geolocation-geobytes.nse	smb-security-mode.nse
dns-cache-snoop.nse	ip-geolocation-geoplugin.nse	smb-server-stats.nse
dns-check-zone.nse	ip-geolocation-ipinfodb.nse	smb-system-info.nse
dns-client-subnet-scan.nse	ip-geolocation-maxmind.nse	smbv2-enabled.nse
dns-fuzz.nse	ipidseq.nse	smb-vuln-ms10-054.nse
dns-ip6-arpa-scan.nse	ipv6-node-info.nse	smb-vuln-ms10-061.nse
dns-nsec3-enum.nse	ipv6-ra-flood.nse	smtp-brute.nse
dns-nsec-enum.nse	irc-botnet-channels.nse	smtp-commands.nse
dns-nsid.nse	irc-brute.nse	smtp-enum-users.nse
dns-random-srcport.nse	irc-info.nse	smtp-open-relay.nse
dns-random-txid.nse	irc-sasl-brute.nse	smtp-strangeport.nse
dns-recursion.nse	irc-unrealircd-backdoor.nse	smtp-vuln-cve2010-4344.nse
dns-service-discovery.nse	iscsi-brute.nse	smtp-vuln-cve2011-1720.nse
dns-srv-enum.nse	iscsi-info.nse	smtp-vuln-cve2011-1764.nse
dns-update.nse	isns-info.nse	sniffer-detect.nse
dns-zeustracker.nse	jdwp-exec.nse	snmp-brute.nse
dns-zone-transfer.nse	jdwp-info.nse	snmp-hh3c-logins.nse
domcon-brute.nse	jdwp-inject.nse	snmp-interfaces.nse
domcon-cmd.nse	jdwp-version.nse	snmp-ios-config.nse
domino-enum-users.nse	krb5-enum-users.nse	snmp-netstat.nse
dpap-brute.nse	ldap-brute.nse	snmp-processes.nse
drda-brute.nse	ldap-novell-getpass.nse	snmp-sysdescr.nse
drda-info.nse	ldap-rootdse.nse	snmp-win32-services.nse
duplicates.nse	ldap-search.nse	snmp-win32-shares.nse
eap-info.nse	lexmark-config.nse	snmp-win32-software.nse
epmd-info.nse	llmnr-resolve.nse	snmp-win32-users.nse
eppc-enum-processes.nse	lltd-discovery.nse	socks-auth-info.nse
finger.nse	maxdb-info.nse	socks-brute.nse

firewalk.nse	mcafee-epo-agent.nse	socks-open-proxy.nse
firewall-bypass.nse	membase-brute.nse	ssh2-enum-algos.nse
flume-master-info.nse	membase-http-info.nse	ssh-hostkey.nse
ftp-anon.nse	memcached-info.nse	sshv1.nse
ftp-bounce.nse	metasploit-info.nse	ssl-cert.nse
ftp-brute.nse	metasploit-msgrpc-brute.nse	ssl-date.nse
ftp-libopie.nse	metasploit-xmlrpc-brute.nse	ssl-enum-ciphers.nse
ftp-proftpd-backdoor.nse	mmouse-brute.nse	ssl-google-cert-catalog.nse
ftp-vsftpd-backdoor.nse	mmouse-exec.nse	ssl-known-key.nse
ftp-vuln-cve2010-4221.nse	modbus-discover.nse	sslv2.nse
ganglia-info.nse	mongodb-brute.nse	stun-info.nse
giop-info.nse	mongodb-databases.nse	stun-version.nse
gkrellm-info.nse	mongodb-info.nse	stuxnet-detect.nse
gopher-ls.nse	mrinfo.nse	svn-brute.nse
gpsd-info.nse	msrpc-enum.nse	targets-asn.nse
hadoop-datanode-info.nse	ms-sql-brute.nse	targets-ipv6-multicast-echo.nse
hadoop-jobtracker-info.nse	ms-sql-config.nse	targets-ipv6-multicast-invalid-
dst.nse		
hadoop-namenode-info.nse	ms-sql-dac.nse	targets-ipv6-multicast-mld.nse
hadoop-secondary-namenode-info.nse	ms-sql-dump-hashes.nse	targets-ipv6-multicast-slaac.nse
hadoop-tasktracker-info.nse	ms-sql-empty-password.nse	targets-sniffer.nse
hbase-master-info.nse	ms-sql-hasdbaccess.nse	targets-traceroute.nse
hbase-region-info.nse	ms-sql-info.nse	teamspeak2-version.nse
hddtemp-info.nse	ms-sql-query.nse	telnet-brute.nse
hostmap-bfk.nse	ms-sql-tables.nse	telnet-encryption.nse
hostmap-ip2hosts.nse	ms-sql-xp-cmdshell.nse	tftp-enum.nse
hostmap-robtex.nse	mtrace.nse	tls-nextprotoneg.nse
http-adobe-coldfusion-apsal301.nse	murmur-version.nse	traceroute-geolocation.nse
http-affiliate-id.nse	mysql-audit.nse	unusual-port.nse
http-apache-negotiation.nse	mysql-brute.nse	upnp-info.nse
http-auth-finder.nse	mysql-databases.nse	url-snarf.nse
http-auth.nse	mysql-dump-hashes.nse	ventrilo-info.nse
http-awstatstotals-exec.nse	mysql-empty-password.nse	versant-info.nse
http-axis2-dir-traversal.nse	mysql-enum.nse	vmauthd-brute.nse

http-backup-finder.nse	mysql-info.nse	vnc-brute.nse
http-barracuda-dir-traversal.nse	mysql-query.nse	vnc-info.nse
http-brute.nse	mysql-users.nse	voldemort-info.nse
http-cakephp-version.nse	mysql-variables.nse	vuze-dht-info.nse
http-chrono.nse	mysql-vuln-cve2012-2122.nse	wdb-version.nse
http-coldfusion-subzero.nse	nat-pmp-info.nse	whois.nse
http-comments-displayer.nse	nat-pmp-mapport.nse	wsdd-discover.nse
http-config-backup.nse	nbstat.nse	x11-access.nse
http-cors.nse	ncp-enum-users.nse	xmcp-discover.nse
http-date.nse	ncp-serverinfo.nse	xmpp-brute.nse
http-default-accounts.nse	ndmp-fs-info.nse	xmpp-info.nse

Les scripts sont regroupés dans des catégories : **auth**, **broadcast**, **brute**, **default**, **discovery**, **dos**, **exploit**, **external**, **fuzzer**, **intrusive**, **malware**, **safe**, **version** and **vuln**.



Important - Pour plus d'informations concernant ces catégories, consultez cette [page](#).

La catégorie la plus utilisée est **default** qui est appelée par l'utilisation de l'option **-sC**. Cette catégorie contient une liste de scripts par défaut.

```
[root@centos7 ~]# nmap -v -sC localhost
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2017-08-05 14:20 CEST
```

```
NSE: Loaded 95 scripts for scanning.
```

```
NSE: Script Pre-scanning.
```

```
Initiating SYN Stealth Scan at 14:20
```

```
Scanning localhost (127.0.0.1) [1000 ports]
```

```
Discovered open port 22/tcp on 127.0.0.1
```

```
adjust_timeouts2: packet supposedly had rtt of -1500757317045342 microseconds. Ignoring time.
```

```
adjust_timeouts2: packet supposedly had rtt of -1500757317045342 microseconds. Ignoring time.
```

```
Discovered open port 25/tcp on 127.0.0.1
```

```
adjust_timeouts2: packet supposedly had rtt of -1500757317045486 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1500757317045486 microseconds. Ignoring time.
Discovered open port 111/tcp on 127.0.0.1
adjust_timeouts2: packet supposedly had rtt of -1500757317045504 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1500757317045504 microseconds. Ignoring time.
Discovered open port 631/tcp on 127.0.0.1
adjust_timeouts2: packet supposedly had rtt of -1500757274107480 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1500757274107480 microseconds. Ignoring time.
Completed SYN Stealth Scan at 14:20, 0.01s elapsed (1000 total ports)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 14:20
Completed NSE at 14:20, 0.28s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey: 2048 17:21:e0:43:b1:66:22:22:b6:f8:2b:cc:08:68:38:59 (RSA)
|_ 256 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54 (ECDSA)
25/tcp    open  smtp
|_smtp-commands: centos7.fenestros.loc, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,
111/tcp   open  rpcbind
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4        111/tcp    rpcbind
|_  100000  2,3,4        111/udp    rpcbind
631/tcp   open  ipp
| http-methods: GET HEAD OPTIONS POST PUT
| Potentially risky methods: PUT
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-robots.txt: 1 disallowed entry
|_/_
```

```
|_http-title: Home - CUPS 1.6.3
```

```
NSE: Script Post-scanning.
```

```
Initiating NSE at 14:20
```

```
Completed NSE at 14:20, 0.00s elapsed
```

```
Read data files from: /usr/bin/../share/nmap
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

```
Raw packets sent: 1000 (44.000KB) | Rcvd: 2004 (84.176KB)
```

Attention - La catégorie par défaut **default** contient certains scripts de la catégorie **intrusive**. Vous ne devez donc jamais utiliser cette option sur un réseau sans avoir obtenu un accord au préalable.

netcat

netcat est un couteau suisse. Il permet non seulement de scanner des ports mais aussi de lancer la connexion lors de la découverte d'un port ouvert.

Options de la commande

Les options de cette commande sont :

```
[root@centos7 ~]# nc --help
```

```
Ncat 6.40 ( http://nmap.org/ncat )
```

```
Usage: ncat [options] [hostname] [port]
```

```
Options taking a time assume seconds. Append 'ms' for milliseconds,  
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
```

```
-4 Use IPv4 only
```

```
-6                Use IPv6 only
-U, --unixsock    Use Unix domain sockets only
-C, --crlf        Use CRLF for EOL sequence
-c, --sh-exec <command> Executes the given command via /bin/sh
-e, --exec <command> Executes the given command
    --lua-exec <filename> Executes the given Lua script
-g hop1[,hop2,...] Loose source routing hop points (8 max)
-G <n>            Loose source routing hop pointer (4, 8, 12, ...)
-m, --max-conns <n> Maximum <n> simultaneous connections
-h, --help        Display this help screen
-d, --delay <time> Wait between read/writes
-o, --output <filename> Dump session data to a file
-x, --hex-dump <filename> Dump session data as hex to a file
-i, --idle-timeout <time> Idle read/write timeout
-p, --source-port port Specify source port to use
-s, --source addr  Specify source address to use (doesn't affect -l)
-l, --listen       Bind and listen for incoming connections
-k, --keep-open    Accept multiple connections in listen mode
-n, --nodns        Do not resolve hostnames via DNS
-t, --telnet       Answer Telnet negotiations
-u, --udp          Use UDP instead of default TCP
    --sctp         Use SCTP instead of default TCP
-v, --verbose      Set verbosity level (can be used several times)
-w, --wait <time> Connect timeout
    --append-output Append rather than clobber specified output files
    --send-only     Only send data, ignoring received; quit on EOF
    --recv-only     Only receive data, never send anything
    --allow         Allow only given hosts to connect to Ncat
    --allowfile      A file of hosts allowed to connect to Ncat
    --deny          Deny given hosts from connecting to Ncat
    --denyfile       A file of hosts denied from connecting to Ncat
    --broker        Enable Ncat's connection brokering mode
    --chat          Start a simple Ncat chat server
    --proxy <addr[:port]> Specify address of host to proxy through
```

```
--proxy-type <type>    Specify proxy type ("http" or "socks4")
--proxy-auth <auth>    Authenticate with HTTP or SOCKS proxy server
--ssl                  Connect or listen with SSL
--ssl-cert             Specify SSL certificate file (PEM) for listening
--ssl-key              Specify SSL private key (PEM) for listening
--ssl-verify           Verify trust and domain name of certificates
--ssl-trustfile        PEM file containing trusted SSL certificates
--version              Display Ncat's version information and exit
```

See the ncat(1) manpage for full options, descriptions and usage examples

Utilisation

Dans l'exemple qui suite, un scan est lancé sur le port 80 puis sur le port 25 :

```
[root@centos7 ~]# nc 127.0.0.1 80 -w 1 -vv
Ncat: Version 6.40 ( http://nmap.org/ncat )
libnsock nsi_new2(): nsi_new (IOD #1)
libnsock nsock_connect_tcp(): TCP connection requested to 127.0.0.1:80 (IOD #1) EID 8
libnsock nsock_trace_handler_callback(): Callback: CONNECT ERROR [Connection refused (111)] for EID 8
[127.0.0.1:80]
Ncat: Connection refused.

[root@centos7 ~]# nc 127.0.0.1 25 -w 1 -vv
Ncat: Version 6.40 ( http://nmap.org/ncat )
libnsock nsi_new2(): nsi_new (IOD #1)
libnsock nsock_connect_tcp(): TCP connection requested to 127.0.0.1:25 (IOD #1) EID 8
libnsock nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.1:25]
Ncat: Connected to 127.0.0.1:25.
libnsock nsi_new2(): nsi_new (IOD #2)
libnsock nsock_read(): Read request from IOD #1 [127.0.0.1:25] (timeout: -1ms) EID 18
libnsock nsock_readbytes(): Read request for 0 bytes from IOD #2 [peer unspecified] EID 26
libnsock nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [127.0.0.1:25] (41 bytes): 220
```

```
centos7.fenestros.loc ESMTP Postfix..  
220 centos7.fenestros.loc ESMTP Postfix  
libnsock nsock_readbytes(): Read request for 0 bytes from IOD #1 [127.0.0.1:25] EID 34  
^C
```



Important - Notez que **netcat** se connecte au port 25 qui est ouvert.

Les Contre-Mesures

Les contre-mesures incluent l'utilisation d'un **S**ystème de **D**étection d'**I**ntrusion (**SDI** - **N**etwork **I**ntrusion **D**etection **S**ystem ou NIDS en anglais), par exemple **Snort** ou un **S**ystème de **D**étection et de **P**révention d'**I**ntrusion, par exemple **portsentry**.

LAB #2 - Mise en place du Système de Détection d'Intrusion Snort

Snort est un **S**ystème de **D**étection d'**I**ntrusion (SDI) qui surveille les requêtes entrantes, vous avertit en cas d'anomalie et enregistre les traces de toute tentative d'intrusion.

Installation

Sous RHEL/CentOS 7, **snort** n'est pas installé par défaut. Qui plus est **snort** ne se trouve pas dans les dépôts standards :

```
[root@centos7 ~]# yum provides snort  
Loaded plugins: fastestmirror, langpacks  
Loading mirror speeds from cached hostfile  
* base: ftp.rezopole.net  
* extras: ftp.rezopole.net
```

```
* updates: ftp.rezopole.net
adobe-linux-x86_64/filelists_db |
1.7 kB 00:00:00
extras/7/x86_64/filelists_db |
1.1 MB 00:00:00
updates/7/x86_64/filelists_db |
4.4 MB 00:00:01
No matches found
```

Commencez donc par installer les dépendances de snort à partir des dépôts standards :

```
[root@centos7 ~]# yum install gcc flex bison zlib libpcap pcre libdnet tcpdump
```

Snort a aussi besoin du paquet **libnghhttp2** :

```
[root@centos7 ~]# rpm -ivh https://www.dropbox.com/s/r3qtnvsteb6m96i/libnghhttp2-1.31.1-2.el7.x86_64.rpm
```

ainsi que le paquet **daq** :

```
[root@centos7 ~]# rpm -ivh https://www.dropbox.com/s/69wl0p0l0aqr0m/daq-2.0.6-1.el7.x86_64.rpm
```

Il est maintenant possible d'installer le paquet **snort** :

```
[root@centos7 ~]# rpm -ivh https://www.dropbox.com/s/appy4ddnpws17ux/snort-2.9.15.1-1.centos7.x86_64.rpm
```

Créez un lien symbolique pour la bibliothèque partagée **/usr/lib64/libdnet.1** :

```
[root@centos7 ~]# ln -s /usr/lib64/libdnet.so.1.0.1 /usr/lib64/libdnet.1
```

Dernièrement, modifiez les permissions sur le répertoire **/var/log/snort** :

```
[root@centos7 ~]# chmod ug+x /var/log/snort
```

Options de la commande

Les options de cette commande sont :

```
[root@centos7 ~]# snort --help
```

```
    _
   /  _
  /    _
 /      _
/        _
o"  _ )~
'    '

-*> Snort! <*-
Version 2.9.11.1 GRE (Build 268)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.5.3
Using PCRE version: 8.32 2012-11-30
Using ZLIB version: 1.2.7
```

USAGE: snort [-options] <filter options>

Options:

- A Set alert mode: fast, full, console, test or none (alert file alerts only)
"unsock" enables UNIX socket logging (experimental).
- b Log packets in tcpdump format (much faster!)
- B <mask> Obfuscated IP addresses in alerts and packet dumps using CIDR mask
- c <rules> Use Rules File <rules>
- C Print out payloads with character data only (no hex)
- d Dump the Application Layer
- D Run Snort in background (daemon) mode
- e Display the second layer header info
- f Turn off fflush() calls after binary log writes
- F <bpf> Read BPF filters from file <bpf>
- g <gname> Run snort gid as <gname> group (or gid) after initialization
- G <0xid> Log Identifier (to uniquely id events for multiple snorts)
- h <hn> Set home network = <hn>
(for use with -l or -B, does NOT change \$HOME_NET in IDS mode)
- H Make hash tables deterministic.

```
-i <if>      Listen on interface <if>
-I          Add Interface name to alert output
-k <mode>    Checksum mode (all,noip,notcp,noudp,noicmp,none)
-K <mode>    Logging mode (pcap[default],ascii,none)
-l <ld>      Log to directory <ld>
-L <file>    Log to this tcpdump file
-M          Log messages to syslog (not alerts)
-m <umask>   Set umask = <umask>
-n <cnt>     Exit after receiving <cnt> packets
-N          Turn off logging (alerts still work)
-O          Obfuscate the logged IP addresses
-p          Disable promiscuous mode sniffing
-P <snap>    Set explicit snaplen of packet (default: 1514)
-q          Quiet. Don't show banner and status report
-Q          Enable inline mode operation.
-r <tf>      Read and process tcpdump file <tf>
-R <id>      Include 'id' in snort_intf<id>.pid file name
-s          Log alert messages to syslog
-S <n=v>     Set rules file variable n equal to value v
-t <dir>     Chroots process to <dir> after initialization
-T          Test and report on the current Snort configuration
-u <uname>   Run snort uid as <uname> user (or uid) after initialization
-U          Use UTC for timestamps
-v          Be verbose
-V          Show version number
-X          Dump the raw packet data starting at the link layer
-x          Exit if Snort configuration problems occur
-y          Include year in timestamp in the alert and log files
-Z <file>    Set the performonitor preprocessor file path and name
-?          Show this information
```

<Filter Options> are standard BPF options, as seen in TCPDump

Longname options and their corresponding single char version

```
--logid <0xid>          Same as -G
--perfmon-file <file>   Same as -Z
```

```
--pid-path <dir>          Specify the directory for the Snort PID file
--snaplen <snap>          Same as -P
--help                    Same as -?
--version                 Same as -V
--alert-before-pass       Process alert, drop, sdrop, or reject before pass, default is pass before
alert, drop,...
--treat-drop-as-alert     Converts drop, sdrop, and reject rules into alert rules during startup
--treat-drop-as-ignore    Use drop, sdrop, and reject rules to ignore session traffic when not inline.
--process-all-events     Process all queued events (drop, alert,...), default stops after 1st action
group
--enable-inline-test      Enable Inline-Test Mode Operation
--dynamic-engine-lib <file> Load a dynamic detection engine
--dynamic-engine-lib-dir <path> Load all dynamic engines from directory
--dynamic-detection-lib <file> Load a dynamic rules library
--dynamic-detection-lib-dir <path> Load all dynamic rules libraries from directory
--dump-dynamic-rules <path> Creates stub rule files of all loaded rules libraries
--dynamic-preprocessor-lib <file> Load a dynamic preprocessor library
--dynamic-preprocessor-lib-dir <path> Load all dynamic preprocessor libraries from directory
--dynamic-output-lib <file> Load a dynamic output library
--dynamic-output-lib-dir <path> Load all dynamic output libraries from directory
--create-pidfile          Create PID file, even when not in Daemon mode
--nolock-pidfile          Do not try to lock Snort PID file
--no-interface-pidfile    Do not include the interface name in Snort PID file
--disable-attribute-reload-thread Do not create a thread to reload the attribute table
--pcap-single <tf>        Same as -r.
--pcap-file <file>        file that contains a list of pcaps to read - read mode is implied.
--pcap-list "<list>"       a space separated list of pcaps to read - read mode is implied.
--pcap-dir <dir>          a directory to recurse to look for pcaps - read mode is implied.
--pcap-filter <filter>    filter to apply when getting pcaps from file or directory.
--pcap-no-filter          reset to use no filter when getting pcaps from file or directory.
--pcap-loop <count>       this option will read the pcaps specified on command line continuously.
                           for <count> times. A value of 0 will read until Snort is terminated.
--pcap-reset             if reading multiple pcaps, reset snort to post-configuration state before
reading next pcap.
```

--pcap-reload	if reading multiple pcaps, reload snort config between pcaps.
--pcap-show	print a line saying what pcap is currently being read.
--exit-check <count>	Signal termination after <count> callbacks from DAQ_Acquire(), showing the time it
	takes from signaling until DAQ_Stop() is called.
--conf-error-out	Same as -x
--enable-mpls-multicast	Allow multicast MPLS
--enable-mpls-overlapping-ip	Handle overlapping IPs within MPLS clouds
--max-mpls-labelchain-len	Specify the max MPLS label chain
--mpls-payload-type	Specify the protocol (ipv4, ipv6, ethernet) that is encapsulated by MPLS
--require-rule-sid	Require that all snort rules have SID specified.
--daq <type>	Select packet acquisition module (default is pcap).
--daq-mode <mode>	Select the DAQ operating mode.
--daq-var <name=value>	Specify extra DAQ configuration variable.
--daq-dir <dir>	Tell snort where to find desired DAQ.
--daq-list[=<dir>]	List packet acquisition modules available in dir. Default is static modules only.
--dirty-pig	Don't flush packets and release memory on shutdown.
--cs-dir <dir>	Directory to use for control socket.
--ha-peer	Activate live high-availability state sharing with peer.
--ha-out <file>	Write high-availability events to this file.
--ha-in <file>	Read high-availability events from this file on startup (warm-start).
--suppress-config-log	Suppress configuration information output.

Configuration de Snort

Snort a besoin de règles pour fonctionner correctement. Ces règles sont disponibles sous trois formes différentes :

- **Community** - règles de base disponibles à tout le monde,
- **Registered** - règles disponibles à toute personne possédant un compte gratuit sur le site <http://www.snort.org>,
- **Subscription** - règles les plus efficaces disponibles uniquement aux utilisateurs enregistrés **et** abonnés à un plan payant.

Le répertoire rules est donc vide lors de l'installation de Snort :

```
[root@centos7 ~]# ls /etc/snort/rules/
[root@centos7 ~]#
```

Téléchargez les règles **Registered** grâce au lien suivant contenant un **oinkcode** :

```
[root@centos7 ~]# wget https://www.dropbox.com/s/zaooREV33j5wqgk/registered.tar.gz
```

Ensuite, saisissez les commandes suivantes :

```
[root@centos7 ~]# tar -xvf ~/registered.tar.gz -C /etc/snort
[root@centos7 ~]# ls /etc/snort/rules
```

app-detect.rules	file-image.rules	netbios.rules	protocol-other.rules	server-
samba.rules				
attack-responses.rules	file-java.rules	nnntp.rules	protocol-pop.rules	server-
webapp.rules				
backdoor.rules	file-multimedia.rules	oracle.rules	protocol-rpc.rules	
shellcode.rules				
bad-traffic.rules	file-office.rules	os-linux.rules	protocol-scada.rules	smtp.rules
blacklist.rules	file-other.rules	os-mobile.rules	protocol-services.rules	snmp.rules
botnet-cnc.rules	file-pdf.rules	os-other.rules	protocol-snmp.rules	specific-
threats.rules				
browser-chrome.rules	finger.rules	os-solaris.rules	protocol-telnet.rules	spyware-
put.rules				
browser-firefox.rules	ftp.rules	os-windows.rules	protocol-tftp.rules	sql.rules
browser-ie.rules	icmp-info.rules	other-ids.rules	protocol-voip.rules	
telnet.rules				
browser-other.rules	icmp.rules	p2p.rules	pua-adware.rules	tftp.rules
browser-plugins.rules	imap.rules	phishing-spam.rules	pua-other.rules	
virus.rules				
browser-webkit.rules	indicator-compromise.rules	policy-multimedia.rules	pua-p2p.rules	voip.rules
chat.rules	indicator-obfuscation.rules	policy-other.rules	pua-toolbars.rules	VRT-
License.txt				
content-replace.rules	indicator-scan.rules	policy.rules	rpc.rules	web-
activex.rules				

ddos.rules	indicator-shellcode.rules	policy-social.rules	rservices.rules	web-
attacks.rules				
deleted.rules	info.rules	policy-spam.rules	scada.rules	web-
cgi.rules				
dns.rules	local.rules	pop2.rules	scan.rules	web-
client.rules				
dos.rules	malware-backdoor.rules	pop3.rules	server-apache.rules	web-
coldfusion.rules				
experimental.rules	malware-cnc.rules	protocol-dns.rules	server-iis.rules	web-
frontpage.rules				
exploit-kit.rules	malware-other.rules	protocol-finger.rules	server-mail.rules	web-
iis.rules				
exploit.rules	malware-tools.rules	protocol-ftp.rules	server-mssql.rules	web-
misc.rules				
file-executable.rules	misc.rules	protocol-icmp.rules	server-mysql.rules	web-
php.rules				
file-flash.rules	multimedia.rules	protocol-imap.rules	server-oracle.rules	x11.rules
file-identify.rules	mysql.rules	protocol-nntp.rules	server-other.rules	



Important - Si vous utilisez **snort** régulièrement, vous devez prendre un abonnement sur le site <http://www.snort.org> afin de pouvoir télécharger les mises à jour des règles.

Editer le fichier `/etc/snort/snort.conf`

Lancez vi pour éditer le fichier `/etc/snort/snort.conf` :

Modifiez la ligne qui commence par **ipvar HOME_NET** pour que celle-ci comporte l'adresse de votre réseau :

...

```
ipvar HOME_NET 10.0.2.0/24
...
```

Dans le cas où vous êtes connecté à deux ou à plusieurs réseaux directement, la ligne devrait prendre la forme suivante :

```
ipvar HOME_NET [adresse_réseau_1 ( p.e. 10.0.2.0/24 ), adresse_réseau_2 ( p.e. 10.0.0.0/8 )]
```

Vérifiez la présence de les lignes qui commencent par **var RULE_PATH**, **Var SO_RULE_PATH** et **var PREPROC_RULE_PATH**. Celles-ci comportent les chemin relatifs des répertoires **rules** :

```
...
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH ../preproc_rules
...
```

Modifiez les deux lignes suivantes afin d'utiliser des chemins absolus :

```
...
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
...
```

Décommentez la ligne qui commence par **output unified2** concernant la journalisation et supprimez le mot **nostamp** :

```
...
# unified2
# Recommended for most installs
output unified2: filename merged.log, limit 128, mpls_event_types, vlan_event_types
...
```

Commentez ensuite la ligne commençant par **dynamicdetection directory** :

```
# path to dynamic rules libraries
# dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Créez ensuite les deux fichiers ci-dessous :

```
[root@centos7 ~]# touch /etc/snort/rules/white_list.rules
[root@centos7 ~]# touch /etc/snort/rules/black_list.rules
```

Modifiez maintenant le fichier **/etc/sysconfig/snort** :

```
...
#### General Configuration

# What interface should snort listen on? [Pick only 1 of the next 3!]
# This is -i {interface} on the command line
# This is the snort.conf config interface: {interface} directive
# INTERFACE=eth0
INTERFACE=enp0s3
#
# The following two options are not directly supported on the command line
# or in the conf file and assume the same Snort configuration for all
# instances
...
```

Vérifiez le fichier de configuration :

```
[root@centos7 ~]# snort -T -c /etc/snort/snort.conf
...
    --== Initialization Complete ==--

    ,,_      -*> Snort! <*-
o"  )~  Version 2.9.9.0 GRE (Build 56)
    '    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
```

```
Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.5.3  
Using PCRE version: 8.32 2012-11-30  
Using ZLIB version: 1.2.7
```

```
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>  
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
Preprocessor Object: SF_SSH Version 1.1 <Build 3>  
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
Preprocessor Object: SF_SIP Version 1.1 <Build 1>  
Preprocessor Object: SF_SDF Version 1.1 <Build 1>  
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>  
Preprocessor Object: SF_POP Version 1.0 <Build 1>  
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>  
Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
```

```
Snort successfully validated the configuration!  
Snort exiting
```

Utilisation de snort en mode "packet sniffer"

Pour visualiser les paquets à l'aide de snort, saisissez la commande suivante :

```
[root@centos7 ~]# snort -vde -c /etc/snort/snort.conf -l /var/log/snort  
...  
[root@centos7 ~]# ^C
```



Important - Notez l'utilisation de la combinaison de touches  pour arrêter la visualisation des paquets.

Pour surveiller une interface réseau en particulier, saisissez la commande suivante :

```
[root@centos7 ~]# snort -vd -i enp0s3 -c /etc/snort/snort.conf
...
[root@centos7 ~]# ^C
```

Utilisation de snort en mode "packet logger"

Pour rediriger la sortie à l'écran vers le fichier log **/var/log/snort**, saisissez la commande suivante :

```
[root@centos7 ~]# snort -de -l /var/log/snort -c /etc/snort/snort.conf
...
[root@centos7 ~]# ^C
```

Journalisation

Constatez le contenu de **/var/log/snort** :

```
[root@centos7 ~]# ls /var/log/snort/
merged.log  snort.log.1501937132  snort.log.1501937470  snort.log.1501943548
```

Constatez le contenu du fichier de journalisation :

```
[root@centos7 ~]# tail /var/log/snort/snort.log.1501943548
[]
```

```

000000;0003P0000oY&0000RT5'0E0000@@00
0
0000K00300;P00000I0N00yE00K00=00!0-0U0KuD}0[00c000K00^300uNy0@0M0o(9000000c000n00]00`G000000LJ0
00oYJ00Z'00RT05EL=j@0%2
00
000000;0003P000..00000jV000
0000000]l00S00000W0h000oY000<'00RT05E(=k@0%U
00
000000_000000oY0000RT05'0E0000@@00k
0
0000K0000_P000000G}&20!~000000I000000AR000!0F|0?000A00"X00-V_0Ь40000"00Ab0b0000bb0}0K0Dd[root@centos7 ~]#
000000]0Xh-et0000qB0000000

```

Ce fichier étant au format **PCAP binaire**, vous pouvez le lire avec la commande suivante :

```
[root@centos7 ~]# snort -r /var/log/snort/snort.log.1501943548 | more
```

Notez que ce fichier peut aussi être lu par la commande **tcpdump** :

```

[root@centos7 ~]# tcpdump -r /var/log/snort/snort.log.1501943548 | more
reading from file /var/log/snort/snort.log.1501943548, link-type EN10MB (Ethernet)
16:32:28.316281 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 2695230935:2695231611,
ack 28164311, win 534
40, length 676
16:32:28.316485 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 676, win 65535, length
0
16:32:28.318511 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 676:768, ack 1, win
53440, length 92
16:32:28.318706 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 768, win 65535, length
0
16:32:28.318799 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 768:860, ack 1, win
53440, length 92
16:32:28.318963 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 860, win 65535, length

```

0

16:32:28.319081 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 860:952, ack 1, win 53440, length 92

16:32:28.319220 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 952, win 65535, length 0

16:32:28.319278 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 952:1044, ack 1, win 53440, length 92

16:32:28.319373 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1044, win 65535, length 0

16:32:28.319457 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1044:1136, ack 1, win 53440, length 92

16:32:28.319544 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1136, win 65535, length 0

16:32:28.319624 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1136:1228, ack 1, win 53440, length 92

16:32:28.319734 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1228, win 65535, length 0

16:32:28.319787 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1228:1320, ack 1, win 53440, length 92

16:32:28.319972 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1320, win 65535, length 0

16:32:28.320041 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1320:1412, ack 1, win 53440, length 92

16:32:28.320186 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1412, win 65535, length 0

16:32:28.320240 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1412:1504, ack 1, win 53440, length 92

16:32:28.320397 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1504, win 65535, length 0

16:32:28.320451 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1504:1596, ack 1, win 53440, length 92

16:32:28.320606 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1596, win 65535, length 0

16:32:28.320659 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1596:1688, ack 1, win

```
53440, length 92
16:32:28.320816 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1688, win 65535, length
0
16:32:28.320869 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1688:1780, ack 1, win
53440, length 92
16:32:28.320991 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1780, win 65535, length
0
16:32:28.321047 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1780:1872, ack 1, win
53440, length 92
16:32:28.321161 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1872, win 65535, length
0
16:32:28.321232 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1872:1964, ack 1, win
53440, length 92
16:32:28.321355 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 1964, win 65535, length
0
16:32:28.321426 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 1964:2056, ack 1, win
53440, length 92
16:32:28.321533 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 2056, win 65535, length
0
16:32:28.321589 IP 15.2.0.10.rev.sfr.net.ssh > 2.2.0.10.rev.sfr.net.48338: Flags [P.], seq 2056:2148, ack 1, win
53440, length 92
16:32:28.321695 IP 2.2.0.10.rev.sfr.net.48338 > 15.2.0.10.rev.sfr.net.ssh: Flags [.], ack 2148, win 65535, length
0
--More--
```



Important - Vous pouvez utiliser le logiciel Wireshark pour visualiser le contenu du fichier en mode graphique.

Dernièrement, notez qu'il est aussi possible de ne journaliser le trafic que sur un seul réseau :

```
# snort -de -l /var/log/snort -h 10.0.2.0/24
```



Important - Notez l'utilisation des options suivantes : **-l** indique le fichier de journalisation, **-h** indique le **home-net**.

Pour lancer snort en arrière plan afin de surveiller l'interface **enp0s3**, utilisez la commande suivante :

```
[root@centos7 ~]# /usr/sbin/snort -A fast -b -d -D -i enp0s3 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort &
[1] 19281
[root@centos7 ~]# Spawning daemon child...
My daemon child 19401 lives...
Daemon parent exiting (0)
^C
[1]+  Done                  /usr/sbin/snort -A fast -b -d -D -i enp0s3 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort
[root@centos7 ~]# ps aux | grep snort
snort    19401  0.0  24.6 850984 504544 ?        Ssl  11:03   0:00 /usr/sbin/snort -A fast -b -d -D -i enp0s3 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort
root     19688  0.0   0.0 114692   964 pts/0    R+   11:04   0:00 grep --color=auto snort
```

Pour arrêter ce processus, utilisez la commande **kill**:

```
[root@centos7 ~]# ps aux | grep snort
snort    19401  0.0  24.6 850984 504692 ?        Ssl  11:03   0:00 /usr/sbin/snort -A fast -b -d -D -i enp0s3 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort
root     20521  0.0   0.0 114692   964 pts/0    R+   11:07   0:00 grep --color=auto snort
[root@centos7 ~]# kill 19401
[root@centos7 ~]# ps aux | grep snort
root     20568  0.0   0.0 114692   968 pts/0    R+   11:07   0:00 grep --color=auto snort
```

LAB #3 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry

Portsentry est un **S**ystème de **D**étection et de **P**révention d'Intrusion (SDPI) qui surveille les requêtes entrantes et en cas d'anomalie bloque l'adresse IP de l'attaquant en inscrivant une règle dans le pare-feu NetFilter (Iptables).

Installation

Sous RHEL/CentOS 7, **portsentry** n'est pas installé par défaut. Qui plus est **portsentry** ne se trouve pas dans les dépôts standards. Installez donc le paquet **portsentry-1.2-1.el5.x86_64.rpm** à partir de l'URL ci-dessous :

```
[root@centos7 ~]# rpm -ivh https://www.dropbox.com/s/6pr45m9mkq7n2tn/portsentry-1.2-1.el5.x86_64.rpm
Loaded plugins: fastestmirror, langpacks
portsentry-1.2-1.el5.x86_64.rpm
53 kB 00:00:00
Examining /var/tmp/yum-root-qpYJaP/portsentry-1.2-1.el5.x86_64.rpm: portsentry-1.2-1.el5.x86_64
Marking /var/tmp/yum-root-qpYJaP/portsentry-1.2-1.el5.x86_64.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package portsentry.x86_64 0:1.2-1.el5 will be installed
--> Finished Dependency Resolution

adobe-linux-x86_64
2.9 kB 00:00:00
base/7/x86_64
3.6 kB 00:00:00
extras/7/x86_64
3.4 kB 00:00:00
updates/7/x86_64
3.4 kB 00:00:00
```

Dependencies Resolved

=====

```
=====
Package                               Arch                Version            Repository
Size
=====
Installing:
 portsentry                          x86_64              1.2-1.el5           /portsentry-1.2-1.el5.x86_64
114 k

Transaction Summary
=====
Install 1 Package

Total size: 114 k
Installed size: 114 k
Is this ok [y/d/N]: y
```

Configuration

Modifiez le fichier **/etc/portsentry/portsentry.conf** en ajoutant la ligne **237** :

```
[root@centos7 ~]# nl /etc/portsentry/portsentry.conf
 1  # PortSentry Configuration
 2  #
 3  # $Id: portsentry.conf,v 1.25 2003/05/23 16:15:39 crowland Exp crowland $
 4  #
 5  # IMPORTANT NOTE: You CAN NOT put spaces between your port arguments.
 6  #
 7  # The default ports will catch a large number of common probes
 8  #
 9  # All entries must be in quotes.
10  #####
```

```
11 # Port Configurations #
12 #####
13 #
14 #
15 # Some example port configs for classic and basic Stealth modes
16 #
17 # I like to always keep some ports at the "low" end of the spectrum.
18 # This will detect a sequential port sweep really quickly and usually
19 # these ports are not in use (i.e. tcpmux port 1)
20 #
21 # ** X-Windows Users **: If you are running X on your box, you need to be sure
22 # you are not binding PortSentry to port 6000 (or port 2000 for OpenWindows users).
23 # Doing so will prevent the X-client from starting properly.
24 #
25 # These port bindings are *ignored* for Advanced Stealth Scan Detection Mode.
26 #
27 # Un-comment these if you are really anal:
28
#TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,4000,400
1,5742,6000,6001,6667,12345,12346,20034,27665,30303,32771,32772,32773,32774,31337,40421,40425,49724,54320"
29
#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,3277
0,32771,32772,32773,32774,31337,54321"
30 #
31 # Use these if you just want to be aware:
32
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,3277
3,32774,40421,49724,54320"
33
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321"
34 #
35 # Use these for just bare-bones
36
#TCP_PORTS="1,11,15,110,111,143,540,635,1080,1524,2000,12345,12346,20034,32771,32772,32773,32774,49724,54320"
```

```
37 #UDP_PORTS="1,7,9,69,161,162,513,640,700,32770,32771,32772,32773,32774,31337,54321"
38 #####
39 # Advanced Stealth Scan Detection Options #
40 #####
41 #
42 # This is the number of ports you want PortSentry to monitor in Advanced mode.
43 # Any port *below* this number will be monitored. Right now it watches
44 # everything below 1024.
45 #
46 # On many Linux systems you cannot bind above port 61000. This is because
47 # these ports are used as part of IP masquerading. I don't recommend you
48 # bind over this number of ports. Realistically: I DON'T RECOMMEND YOU MONITOR
49 # OVER 1024 PORTS AS YOUR FALSE ALARM RATE WILL ALMOST CERTAINLY RISE. You've been
50 # warned! Don't write me if you have have a problem because I'll only tell
51 # you to RTFM and don't run above the first 1024 ports.
52 #
53 #
54 ADVANCED_PORTS_TCP="1024"
55 ADVANCED_PORTS_UDP="1024"
56 #
57 # This field tells PortSentry what ports (besides listening daemons) to
58 # ignore. This is helpful for services like ident that services such
59 # as FTP, SMTP, and wrappers look for but you may not run (and probably
60 # *shouldn't* IMHO).
61 #
62 # By specifying ports here PortSentry will simply not respond to
63 # incoming requests, in effect PortSentry treats them as if they are
64 # actual bound daemons. The default ports are ones reported as
65 # problematic false alarms and should probably be left alone for
66 # all but the most isolated systems/networks.
67 #
68 # Default TCP ident and NetBIOS service
69 ADVANCED_EXCLUDE_TCP="21,22,25,53,80,110,113,135,137,138,139,443"
70 # Default UDP route (RIP), NetBIOS, bootp broadcasts.
```

```
71  ADVANCED_EXCLUDE_UDP="520,517,518,513,138,137,123,68,67,53"
72  #####
73  # Configuration Files#
74  #####
75  #
76  # Hosts to ignore
77  IGNORE_FILE="/etc/portsentry/portsentry.ignore"
78  # Hosts that have been denied (running history)
79  HISTORY_FILE="/etc/portsentry/portsentry.history"
80  # Hosts that have been denied this session only (temporary until next restart)
81  BLOCKED_FILE="/etc/portsentry/portsentry.blocked"
82  #####
83  # Misc. Configuration Options#
84  #####
85  #
86  # DNS Name resolution - Setting this to "1" will turn on DNS lookups
87  # for attacking hosts. Setting it to "0" (or any other value) will shut
88  # it off.
89  RESOLVE_HOST = "1"
90  #####
91  # Response Options#
92  #####
93  # Options to dispose of attacker. Each is an action that will
94  # be run if an attack is detected. If you don't want a particular
95  # option then comment it out and it will be skipped.
96  #
97  # The variable $TARGET$ will be substituted with the target attacking
98  # host when an attack is detected. The variable $PORT$ will be substituted
99  # with the port that was scanned.
100 #
101 #####
102 # Ignore Options #
103 #####
104 # These options allow you to enable automatic response
```

```
105 # options for UDP/TCP. This is useful if you just want
106 # warnings for connections, but don't want to react for
107 # a particular protocol (i.e. you want to block TCP, but
108 # not UDP). To prevent a possible Denial of service attack
109 # against UDP and stealth scan detection for TCP, you may
110 # want to disable blocking, but leave the warning enabled.
111 # I personally would wait for this to become a problem before
112 # doing though as most attackers really aren't doing this.
113 # The third option allows you to run just the external command
114 # in case of a scan to have a pager script or such execute
115 # but not drop the route. This may be useful for some admins
116 # who want to block TCP, but only want pager/e-mail warnings
117 # on UDP, etc.
118 #
119 #
120 # 0 = Do not block UDP/TCP scans.
121 # 1 = Block UDP/TCP scans.
122 # 2 = Run external command only (KILL_RUN_CMD)
123 BLOCK_UDP="1"
124 BLOCK_TCP="1"
125 #####
126 # Dropping Routes:#
127 #####
128 # This command is used to drop the route or add the host into
129 # a local filter table.
130 #
131 # The gateway (333.444.555.666) should ideally be a dead host on
132 # the *local* subnet. On some hosts you can also point this at
133 # localhost (127.0.0.1) and get the same effect. NOTE THAT
134 # 333.444.555.66 WILL *NOT* WORK. YOU NEED TO CHANGE IT!!
135 #
136 # ALL KILL ROUTE OPTIONS ARE COMMENTED OUT INITIALLY. Make sure you
137 # uncomment the correct line for your OS. If you OS is not listed
138 # here and you have a route drop command that works then please
```

```
139 # mail it to me so I can include it. ONLY ONE KILL_ROUTE OPTION
140 # CAN BE USED AT A TIME SO DON'T UNCOMMENT MULTIPLE LINES.
141 #
142 # NOTE: The route commands are the least optimal way of blocking
143 # and do not provide complete protection against UDP attacks and
144 # will still generate alarms for both UDP and stealth scans. I
145 # always recommend you use a packet filter because they are made
146 # for this purpose.
147 #
148 # Generic
149 #KILL_ROUTE="/sbin/route add $TARGET$ 333.444.555.666"
150 # Generic Linux
151 #KILL_ROUTE="/sbin/route add -host $TARGET$ gw 333.444.555.666"
152 # Newer versions of Linux support the reject flag now. This
153 # is cleaner than the above option.
154 #KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
155 # Generic BSD (BSDI, OpenBSD, NetBSD, FreeBSD)
156 #KILL_ROUTE="/sbin/route add $TARGET$ 333.444.555.666"
157 # Generic Sun
158 #KILL_ROUTE="/usr/sbin/route add $TARGET$ 333.444.555.666 1"
159 # NEXTSTEP
160 #KILL_ROUTE="/usr/etc/route add $TARGET$ 127.0.0.1 1"
161 # FreeBSD
162 #KILL_ROUTE="route add -net $TARGET$ -netmask 255.255.255.255 127.0.0.1 -blackhole"
163 # Digital UNIX 4.0D (OSF/1 / Compaq Tru64 UNIX)
164 #KILL_ROUTE="/sbin/route add -host -blackhole $TARGET$ 127.0.0.1"
165 # Generic HP-UX
166 #KILL_ROUTE="/usr/sbin/route add net $TARGET$ netmask 255.255.255.0 127.0.0.1"
167 ##
168 # Using a packet filter is the PREFERRED. The below lines
169 # work well on many OS's. Remember, you can only uncomment *one*
170 # KILL_ROUTE option.
171 ##
172 # ipfwadm support for Linux
```

```
173 #KILL_ROUTE="/sbin/ipfwadm -I -i deny -S $TARGET$ -o"
174 #
175 # ipfwadm support for Linux (no logging of denied packets)
176 #KILL_ROUTE="/sbin/ipfwadm -I -i deny -S $TARGET$"
177 #
178 # ipchain support for Linux
179 #KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -l"
180 #
181 # ipchain support for Linux (no logging of denied packets)
182 #KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY"
183 #
184 # iptables support for Linux
185 KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"
186 # For those of you running FreeBSD (and compatible) you can
187 # use their built in firewalling as well.
188 #
189 #KILL_ROUTE="/sbin/ipfw add 1 deny all from $TARGET$:255.255.255.255 to any"
190 #
191 #
192 # For those running ipfilt (OpenBSD, etc.)
193 # NOTE THAT YOU NEED TO CHANGE external_interface TO A VALID INTERFACE!!
194 #
195 #KILL_ROUTE="/bin/echo 'block in log on external_interface from $TARGET$/32 to any' | /sbin/ipf -f -"
196 #####
197 # TCP Wrappers#
198 #####
199 # This text will be dropped into the hosts.deny file for wrappers
200 # to use. There are two formats for TCP wrappers:
201 #
202 # Format One: Old Style - The default when extended host processing
203 # options are not enabled.
204 #
205 #KILL_HOSTS_DENY="ALL: $TARGET$"
206 # Format Two: New Style - The format used when extended option
```

```
207 # processing is enabled. You can drop in extended processing
208 # options, but be sure you escape all '%' symbols with a backslash
209 # to prevent problems writing out (i.e. \%c \%h )
210 #
211 #KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"
212 #####
213 # External Command#
214 #####
215 # This is a command that is run when a host connects, it can be whatever
216 # you want it to be (pager, etc.). This command is executed before the
217 # route is dropped or after depending on the KILL_RUN_CMD_FIRST option below
218 #
219 #
220 # I NEVER RECOMMEND YOU PUT IN RETALIATORY ACTIONS AGAINST THE HOST SCANNING
221 # YOU!
222 #
223 # TCP/IP is an *unauthenticated protocol* and people can make scans appear out
224 # of thin air. The only time it is reasonably safe (and I *never* think it is
225 # reasonable) to run reverse probe scripts is when using the "classic" -tcp mode.
226 # This mode requires a full connect and is very hard to spoof.
227 #
228 # The KILL_RUN_CMD_FIRST value should be set to "1" to force the command
229 # to run *before* the blocking occurs and should be set to "0" to make the
230 # command run *after* the blocking has occurred.
231 #
232 #KILL_RUN_CMD_FIRST = "0"
233 #
234 #
235 #KILL_RUN_CMD="/some/path/here/script $TARGET$ $PORT$"
236 #KILL_RUN_CMD="/bin/mail -s 'Portscan from $TARGET$ on port $PORT$' user@host < /dev/null"
237 KILL_RUN_CMD="/bin/mail -s 'Portscan from $TARGET$ on port $PORT$' root@localhost < /dev/null" <-----
-----AJOUTEZ cette ligne
238 #####
239 # Scan trigger value#
```

```
240 #####
241 # Enter in the number of port connects you will allow before an
242 # alarm is given. The default is 0 which will react immediately.
243 # A value of 1 or 2 will reduce false alarms. Anything higher is
244 # probably not necessary. This value must always be specified, but
245 # generally can be left at 0.
246 #
247 # NOTE: If you are using the advanced detection option you need to
248 # be careful that you don't make a hair trigger situation. Because
249 # Advanced mode will react for *any* host connecting to a non-used
250 # below your specified range, you have the opportunity to really
251 # break things. (i.e someone innocently tries to connect to you via
252 # SSL [TCP port 443] and you immediately block them). Some of you
253 # may even want this though. Just be careful.
254 #
255 SCAN_TRIGGER="2"
256 #####
257 # Port Banner Section#
258 #####
259 #
260 # Enter text in here you want displayed to a person tripping the PortSentry.
261 # I *don't* recommend taunting the person as this will aggravate them.
262 # Leave this commented out to disable the feature
263 #
264 # Stealth scan detection modes don't use this feature
265 #
266 #PORT_BANNER="** UNAUTHORIZED ACCESS PROHIBITED *** YOUR CONNECTION ATTEMPT HAS BEEN LOGGED. GO AWAY."
267 # EOF
```

Pour rendre le service SysVinit compatible avec Systemd, éditez le fichier **/etc/init.d/portsentry** en supprimant la ligne **11** :

```
[root@centos7 ~]# nl /etc/init.d/portsentry
 1 #!/bin/bash
 2 #
```

```
3 # Startup script for the Portsentry portscan detector
4 #
5 # chkconfig: 345 98 02
6 # description: PortSentry Port Scan Detector is part of the Abacus Project \
7 #               suite of tools. The Abacus Project is an initiative to release \
8 #               low-maintenance, generic, and reliable host based intrusion \
9 #               detection software to the Internet community.
10 # processname: portsentry
11 # pidfile: /var/run/portsentry.pid <-----SUPPRIMEZ cette ligne
12 # config: /etc/portsentry/portsentry.conf
13 # Source function library.
...

```

Puis ajoutez la ligne **80** :

```
...
77 stop() {
78     echo -n "Stopping $prog: "
79     killproc portsentry
80     killall portsentry <-----AJOUTEZ cette ligne
81     RETVAL=$?
82     echo
83     [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/portsentry
84 }
85 # See how we were called.
...

```

Dernièrement, installez le paquet **initscripts** :

```
[root@centos7 ~]# yum install -y initscripts
```

Utilisation

Démarrez le service **portsentry** :

```
[root@centos7 ~]# systemctl start portsentry
[root@centos7 ~]# systemctl status portsentry
● portsentry.service - SYSV: PortSentry Port Scan Detector is part of the Abacus Project suite of tools. The
Abacus Project is an initiative to release low-maintenance, generic, and reliable host based intrusion detection
software to the Internet community.
   Loaded: loaded (/etc/rc.d/init.d/portsentry; bad; vendor preset: disabled)
   Active: active (running) since Sun 2017-08-06 14:48:18 CEST; 6s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 6487 ExecStart=/etc/rc.d/init.d/portsentry start (code=exited, status=0/SUCCESS)
    CGroup: /system.slice/portsentry.service
            └─6511 /usr/sbin/portsentry -atcp
            └─6513 /usr/sbin/portsentry -audp

Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...: 517
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...: 518
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...: 513
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...: 138
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...: 137
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...: 123
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...t: 68
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode
activated. Ignored UDP...t: 67
```

```
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP...t: 53
```

```
Aug 06 14:48:18 centos7.fenestros.loc portsentry[6513]: adminalert: PortSentry is now active and listening. Hint: Some lines were ellipsized, use -l to show in full.
```

```
[root@centos7 ~]# ps aux | grep portsentry
```

```
root      6511  0.0  0.0   6364   460 ?        Ss   14:48   0:00 /usr/sbin/portsentry -atcp
root      6513  0.0  0.0   6364   460 ?        Ss   14:48   0:00 /usr/sbin/portsentry -audp
root      6687  0.0  0.0  114692   972 pts/0    R+   14:48   0:00 grep --color=auto portsentry
```

Editez le fichier **/etc/portsentry/portsentry.ignore** en commentant la ligne contenant votre adresse IP :

```
[root@centos7 ~]# nl /etc/portsentry/portsentry.ignore
```

```
 1 # Put hosts in here you never want blocked. This includes the IP addresses
 2 # of all local interfaces on the protected host (i.e virtual host, mult-home)
 3 # Keep 127.0.0.1 and 0.0.0.0 to keep people from playing games.
 4 #
 5 # PortSentry can support full netmasks for networks as well. Format is:
 6 #
 7 # <IP Address>/<Netmask>
 8 #
 9 # Example:
10 #
11 # 192.168.2.0/24
12 # 192.168.0.0/16
13 # 192.168.2.1/32
14 # Etc.
15 #
16 # If you don't supply a netmask it is assumed to be 32 bits.
17 #
18 #
19 127.0.0.1/32
20 0.0.0.0
21 #####
22 # Do NOT edit below this line, if you #
```

```
23 # do, your changes will be lost when      #
24 # portentry is restarted via the          #
25 # initscript. Make all changes above     #
26 # this box.                               #
27 #####
28 # Exclude all local interfaces
29 #172.YY+20.0.3      <-----EDITEZ cette ligne
30 fe80::94b9:ef1e:8c65:97c6
31 127.0.0.1
32 ::1
33 # Exclude the default gateway(s)
34 10.0.2.2
35 # Exclude the nameservers
36 10.0.2.3
37 # And last but not least...
38 0.0.0.0
```

Sans re-démarrez le service portentry, lancez un scan des ports avec nmap :

```
[root@centos7 ~]# nmap -sC 172.YY+20.0.3
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2017-08-06 14:52 CEST
```

```
^C
```

```
You have new mail in /var/spool/mail/root
```



Important - Notez l'utilisation de la combinaison de touches **CtrlC** pour arrêter nmap.

Consultez les règles d'iptables :

```
[root@centos7 ~]# iptables -L
```

```
Chain INPUT (policy ACCEPT)
target      prot opt source                destination
DROP        all  --  15.2.0.10.rev.sfr.net  anywhere    <-----REGARDEZ cette ligne, elle
sera différente en fonction de votre adresse IP
ACCEPT      all  --  anywhere              anywhere     ctstate RELATED,ESTABLISHED
ACCEPT      all  --  anywhere              anywhere
INPUT_direct all  --  anywhere              anywhere
INPUT_ZONES_SOURCE all  --  anywhere              anywhere
INPUT_ZONES all  --  anywhere              anywhere
DROP        all  --  anywhere              anywhere     ctstate INVALID
REJECT      all  --  anywhere              anywhere     reject-with icmp-host-prohibited
...
```

Dernièrement, consultez les messages destinés à root :

```
[root@centos7 ~]# mail
Heirloom Mail version 12.5 7/5/10.  Type ? for help.
"/var/spool/mail/root": 6 messages 6 new
>N 1 trainee@centos7.fene Sat Apr 30 12:38 16/688  "*** SECURITY information for centos7.fenestros.loc ***"
  N 2 user@localhost.fenes Tue May 9 15:21 1238/86160 "[abrt] firefox: plugin-container killed by SIGSEGV"
  N 3 (Cron Daemon)        Sun Aug 6 11:28 25/1061 "Cron <root@centos7> /sbin/service portsentry restart
>/dev/null && /sbin/ser"
  N 4 (Cron Daemon)        Sun Aug 6 14:27 26/1328 "Cron <root@centos7> /sbin/service portsentry restart
>/dev/null && /sbin/ser"
  N 5 (Cron Daemon)        Sun Aug 6 14:43 25/1168 "Cron <root@centos7> /sbin/service portsentry restart
>/dev/null && /sbin/ser"
  N 6 root                 Sun Aug 6 14:52 18/658  "Portscan from 10.0.2.15 on port 143"
& 6
Message 6:
From root@centos7.fenestros.loc Sun Aug 6 14:52:43 2017
Return-Path: <root@centos7.fenestros.loc>
X-Original-To: root@localhost
Delivered-To: root@localhost.fenestros.loc
Date: Sun, 06 Aug 2017 14:52:43 +0200
```

```
To: root@localhost.fenestros.loc
Subject: Portscan from 10.0.2.15 on port 143
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
From: root@centos7.fenestros.loc (root)
Status: R
```

```
& q
Held 6 messages in /var/spool/mail/root
You have mail in /var/spool/mail/root
[root@centos7 ~]#
```

Pour nettoyer la règle, re-démarrez le service **firewalld** :

```
[root@centos7 ~]# systemctl restart firewalld
[root@centos7 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
INPUT_direct all  --  anywhere              anywhere
INPUT_ZONES_SOURCE all  --  anywhere              anywhere
INPUT_ZONES all  --  anywhere              anywhere
DROP       all  --  anywhere              anywhere              ctstate INVALID
REJECT     all  --  anywhere              anywhere              reject-with icmp-host-prohibited
...
```

ChangeLog

2020.01

Backup 2019.beta restauré en 2020.01.

2020.02

- **Fixed** - Erreur dans un lien dans le LAB #2 :
<https://www.snort.org/rules/snortrules-snapshot-2990.tar.gz?oinkcode=b4415c0d8774585162b5a22283d36f2d035755c7> >
<https://www.snort.org/rules/snortrules-snapshot-2983.tar.gz?oinkcode=5069d3725c7a71ff8b32198307e830eac7470687>

2020.03

- **Fixed** - Erreur dans un lien dans le LAB #2 :
https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/l/libnhttp2-1.31.1-2.el7.x86_64.rpm >
https://www.dropbox.com/s/r3qtnvsteb6m96i/libnhttp2-1.31.1-2.el7.x86_64.rpm
- **Fixed** - Erreur dans un lien dans le LAB #2 :
http://download-ib01.fedoraproject.org/pub/epel/7/x86_64/Packages/d/daq-2.0.6-1.el7.x86_64.rpm >
https://www.dropbox.com/s/69wl0p010aqr0m/daq-2.0.6-1.el7.x86_64.rpm
- **Fixed** - Erreur dans un lien dans le LAB #2 : https://www.snort.org/downloads/snort/snort-2.9.15.1-1.centos7.x86_64.rpm >
https://www.dropbox.com/s/appy4ddnpws17ux/snort-2.9.15.1-1.centos7.x86_64.rpm
- **Fixed** - Erreur dans un lien dans le LAB #2 :
<https://www.snort.org/rules/snortrules-snapshot-2983.tar.gz?oinkcode=5069d3725c7a71ff8b32198307e830eac7470687> >
<https://www.dropbox.com/s/zaoorev33j5wqgk/registered.tar.gz>
- **Fixed** - Erreur dans un lien dans le LAB #3 : http://flexbox.sourceforge.net/centos/5/x86_64//portsentry-1.2-1.el5.x86_64.rpm >
https://www.dropbox.com/s/6pr45m9mkq7n2tn/portsentry-1.2-1.el5.x86_64.rpm

