Version : **2026.01**

Dernière mise-à-jour : 2025/12/04 15:40

# LDF407 - Balayage des Ports

## Contenu du Module

# 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

### 1.1 - nmap

#### Installation

Sous Debian 12, **nmap** n'est pas installé par défaut :

```
root@debian12:~# which nmap
root@debian12:~#
```

Installez donc nmap en utilisant APT :

```
root@debian12:~# apt install nmap
```

### Utilisation

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

```
root@debian12:~# nmap 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-27 16:48 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
631/tcp  open  ipp
5900/tcp open  vnc

Nmap done: 1 IP address (1 host up) scanned in 0.10 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@debian12:~# 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 ( https://nmap.org/ )
#
# $Id: nmap-services 38442 2022-08-31 22:53:46Z dmiller $
#
# Derived from IANA data and our own research
#
# This collection of service data is (C) 1996-2020 by Insecure.Com
# LLC.  It is distributed under the Nmap Public Source license as
# provided in the LICENSE file of the source distribution or at
# https://svn.nmap.org/nmap/LICENSE .  Note that this license
# requires you to license your own work under a compatable 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 https://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] | TCP Port Service Multiplexer
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/tcp   0.000000        # Remote Job Entry
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
discard 9/sctp  0.000000        # sink null
discard 9/tcp   0.003764        # sink null
discard 9/udp   0.015733        # sink null
unknown 10/tcp  0.000063
systat  11/tcp  0.000075        # Active Users
systat  11/udp  0.000577        # Active Users
unknown 12/tcp  0.000063
daytime 13/tcp  0.003927
daytime 13/udp  0.004827
unknown 14/tcp  0.000038
netstat 15/tcp  0.000038
unknown 16/tcp  0.000050
qotd    17/tcp  0.002346        # Quote of the Day
qotd    17/udp  0.009209        # Quote of the Day
msp     18/tcp  0.000000        # Message Send Protocol | Message Send Protocol (historic)
msp     18/udp  0.000610        # Message Send Protocol
chargen 19/tcp  0.002559        # ttytst source Character Generator | Character Generator
chargen 19/udp  0.015865        # ttytst source Character Generator
ftp-data        20/sctp 0.000000        # File Transfer [Default Data] | FTP
--More--(0%)
```

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

```
root@debian12:~# ls -l /usr/share/nmap
total 9368
-rw-r--r-- 1 root root   10829 Jan 16  2023 nmap.dtd
-rw-r--r-- 1 root root  824437 Jan 16  2023 nmap-mac-prefixes
-rw-r--r-- 1 root root 5032815 Jan 16  2023 nmap-os-db
-rw-r--r-- 1 root root   21165 Jan 16  2023 nmap-payloads
-rw-r--r-- 1 root root    6845 Jan 16  2023 nmap-protocols
-rw-r--r-- 1 root root   43529 Jan 16  2023 nmap-rpc
```

```
-rw-r--r-- 1 root root 2506640 Jan 16  2023 nmap-service-probes
-rw-r--r-- 1 root root 1004557 Jan 16  2023 nmap-services
-rw-r--r-- 1 root root   31936 Jan 16  2023 nmap.xsl
drwxr-xr-x 3 root root    4096 Nov 27 16:46 nselib
-rw-r--r-- 1 root root   49478 Jan 16  2023 nse_main.lua
drwxr-xr-x 2 root root   36864 Nov 27 16:46 scripts
```

Voici la liste des fichiers les plus importants :

| Fichier | Description |
|---|---|
| /usr/share/nmap/nmap-protocols | Contient la liste des protocols 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@debian12:~# ls /usr/share/nmap/scripts/
acarsd-info.nse                       fcrdns.nse                              https-redirect.nse
ms-sql-info.nse                 smb-flood.nse
address-info.nse                      finger.nse                              http-stored-xss.nse
ms-sql-ntlm-info.nse            smb-ls.nse
afp-brute.nse                         fingerprint-strings.nse                 http-svn-enum.nse
ms-sql-query.nse                smb-mbenum.nse
afp-ls.nse                            firewalk.nse                            http-svn-info.nse
ms-sql-tables.nse               smb-os-discovery.nse
afp-path-vuln.nse                     firewall-bypass.nse                     http-title.nse
ms-sql-xp-cmdshell.nse          smb-print-text.nse
afp-serverinfo.nse                    flume-master-info.nse                   http-tplink-dir-traversal.nse
mtrace.nse                      smb-protocols.nse
afp-showmount.nse                     fox-info.nse                            http-trace.nse
```

```
murmur-version.nse              smb-psexec.nse
ajp-auth.nse                          freelancer-info.nse                     http-traceroute.nse
mysql-audit.nse                 smb-security-mode.nse
ajp-brute.nse                         ftp-anon.nse                            http-trane-info.nse
mysql-brute.nse                 smb-server-stats.nse
ajp-headers.nse                       ftp-bounce.nse                          http-unsafe-output-escaping.nse
mysql-databases.nse             smb-system-info.nse
ajp-methods.nse                       ftp-brute.nse                           http-useragent-tester.nse
mysql-dump-hashes.nse           smb-vuln-conficker.nse
ajp-request.nse                       ftp-libopie.nse                         http-userdir-enum.nse
mysql-empty-password.nse        smb-vuln-cve2009-3103.nse
allseeingeye-info.nse                 ftp-proftpd-backdoor.nse                http-vhosts.nse
mysql-enum.nse                  smb-vuln-cve-2017-7494.nse
amqp-info.nse                         ftp-syst.nse                            http-virustotal.nse
mysql-info.nse                  smb-vuln-ms06-025.nse
asn-query.nse                         ftp-vsftpd-backdoor.nse                 http-vlcstreamer-ls.nse
mysql-query.nse                 smb-vuln-ms07-029.nse
auth-owners.nse                       ftp-vuln-cve2010-4221.nse               http-vmware-path-vuln.nse
mysql-users.nse                 smb-vuln-ms08-067.nse
auth-spoof.nse                        ganglia-info.nse                        http-vuln-cve2006-3392.nse
mysql-variables.nse             smb-vuln-ms10-054.nse
backorifice-brute.nse                 giop-info.nse                           http-vuln-cve2009-3960.nse
mysql-vuln-cve2012-2122.nse     smb-vuln-ms10-061.nse
backorifice-info.nse                  gkrellm-info.nse                        http-vuln-cve2010-0738.nse
nat-pmp-info.nse                smb-vuln-ms17-010.nse
bacnet-info.nse                       gopher-ls.nse                           http-vuln-cve2010-2861.nse
nat-pmp-mapport.nse             smb-vuln-regsvc-dos.nse
banner.nse                            gpsd-info.nse                           http-vuln-cve2011-3192.nse
nbd-info.nse                    smb-vuln-webexec.nse
bitcoin-getaddr.nse                   hadoop-datanode-info.nse                http-vuln-cve2011-3368.nse
nbns-interfaces.nse             smb-webexec-exploit.nse
bitcoin-info.nse                      hadoop-jobtracker-info.nse              http-vuln-cve2012-1823.nse
nbstat.nse                      smtp-brute.nse
bitcoinrpc-info.nse                   hadoop-namenode-info.nse                http-vuln-cve2013-0156.nse
```

```
ncp-enum-users.nse              smtp-commands.nse
bittorrent-discovery.nse              hadoop-secondary-namenode-info.nse      http-vuln-cve2013-6786.nse
ncp-serverinfo.nse              smtp-enum-users.nse
bjnp-discover.nse                     hadoop-tasktracker-info.nse             http-vuln-cve2013-7091.nse
ndmp-fs-info.nse                smtp-ntlm-info.nse
broadcast-ataoe-discover.nse          hbase-master-info.nse                   http-vuln-cve2014-2126.nse
ndmp-version.nse                smtp-open-relay.nse
broadcast-avahi-dos.nse               hbase-region-info.nse                   http-vuln-cve2014-2127.nse
nessus-brute.nse                smtp-strangeport.nse
broadcast-bjnp-discover.nse           hddtemp-info.nse                        http-vuln-cve2014-2128.nse
nessus-xmlrpc-brute.nse         smtp-vuln-cve2010-4344.nse
broadcast-db2-discover.nse            hnap-info.nse                           http-vuln-cve2014-2129.nse
netbus-auth-bypass.nse          smtp-vuln-cve2011-1720.nse
broadcast-dhcp6-discover.nse          hostmap-bfk.nse                         http-vuln-cve2014-3704.nse
netbus-brute.nse                smtp-vuln-cve2011-1764.nse
broadcast-dhcp-discover.nse           hostmap-crtsh.nse                       http-vuln-cve2014-8877.nse
netbus-info.nse                 sniffer-detect.nse
broadcast-dns-service-discovery.nse   hostmap-robtex.nse                      http-vuln-cve2015-1427.nse
netbus-version.nse              snmp-brute.nse
broadcast-dropbox-listener.nse        http-adobe-coldfusion-apsa1301.nse      http-vuln-cve2015-1635.nse
nexpose-brute.nse               snmp-hh3c-logins.nse
broadcast-eigrp-discovery.nse         http-affiliate-id.nse                   http-vuln-cve2017-1001000.nse
nfs-ls.nse                      snmp-info.nse
broadcast-hid-discoveryd.nse          http-apache-negotiation.nse             http-vuln-cve2017-5638.nse
nfs-showmount.nse               snmp-interfaces.nse
broadcast-igmp-discovery.nse          http-apache-server-status.nse           http-vuln-cve2017-5689.nse
nfs-statfs.nse                  snmp-ios-config.nse
broadcast-jenkins-discover.nse        http-aspnet-debug.nse                   http-vuln-cve2017-8917.nse
nje-node-brute.nse              snmp-netstat.nse
broadcast-listener.nse                http-auth-finder.nse                    http-vuln-misfortune-cookie.nse
nje-pass-brute.nse              snmp-processes.nse
broadcast-ms-sql-discover.nse         http-auth.nse                           http-vuln-wnr1000-creds.nse
nntp-ntlm-info.nse              snmp-sysdescr.nse
broadcast-netbios-master-browser.nse  http-avaya-ipoffice-users.nse           http-waf-detect.nse
```

```
nping-brute.nse                 snmp-win32-services.nse
broadcast-networker-discover.nse      http-awstatstotals-exec.nse             http-waf-fingerprint.nse
nrpe-enum.nse                   snmp-win32-shares.nse
broadcast-novell-locate.nse           http-axis2-dir-traversal.nse            http-webdav-scan.nse
ntp-info.nse                    snmp-win32-software.nse
broadcast-ospf2-discover.nse          http-backup-finder.nse                  http-wordpress-brute.nse
ntp-monlist.nse                 snmp-win32-users.nse
broadcast-pc-anywhere.nse             http-barracuda-dir-traversal.nse        http-wordpress-enum.nse
omp2-brute.nse                  socks-auth-info.nse
broadcast-pc-duo.nse                  http-bigip-cookie.nse                   http-wordpress-users.nse
omp2-enum-targets.nse           socks-brute.nse
broadcast-pim-discovery.nse           http-brute.nse                          http-xssed.nse
omron-info.nse                  socks-open-proxy.nse
broadcast-ping.nse                    http-cakephp-version.nse                iax2-brute.nse
openflow-info.nse               ssh2-enum-algos.nse
broadcast-pppoe-discover.nse          http-chrono.nse                         iax2-version.nse
openlookup-info.nse             ssh-auth-methods.nse
broadcast-rip-discover.nse            http-cisco-anyconnect.nse               icap-info.nse
openvas-otp-brute.nse           ssh-brute.nse
broadcast-ripng-discover.nse          http-coldfusion-subzero.nse             iec-identify.nse
openwebnet-discovery.nse        ssh-hostkey.nse
broadcast-sonicwall-discover.nse      http-comments-displayer.nse             ike-version.nse
oracle-brute.nse                ssh-publickey-acceptance.nse
broadcast-sybase-asa-discover.nse     http-config-backup.nse                  imap-brute.nse
oracle-brute-stealth.nse        ssh-run.nse
broadcast-tellstick-discover.nse      http-cookie-flags.nse                   imap-capabilities.nse
oracle-enum-users.nse           sshv1.nse
broadcast-upnp-info.nse               http-cors.nse                           imap-ntlm-info.nse
oracle-sid-brute.nse            ssl-ccs-injection.nse
broadcast-versant-locate.nse          http-cross-domain-policy.nse            impress-remote-discover.nse
oracle-tns-version.nse          ssl-cert-intaddr.nse
broadcast-wake-on-lan.nse             http-csrf.nse                           informix-brute.nse
ovs-agent-version.nse           ssl-cert.nse
broadcast-wpad-discover.nse           http-date.nse                           informix-query.nse
```

```
p2p-conficker.nse               ssl-date.nse
broadcast-wsdd-discover.nse           http-default-accounts.nse               informix-tables.nse
path-mtu.nse                    ssl-dh-params.nse
broadcast-xdmcp-discover.nse          http-devframework.nse                   ip-forwarding.nse
pcanywhere-brute.nse            ssl-enum-ciphers.nse
cassandra-brute.nse                   http-dlink-backdoor.nse                 ip-geolocation-geoplugin.nse
pcworx-info.nse                 ssl-heartbleed.nse
cassandra-info.nse                    http-dombased-xss.nse                   ip-geolocation-ipinfodb.nse
pgsql-brute.nse                 ssl-known-key.nse
cccam-version.nse                     http-domino-enum-passwords.nse          ip-geolocation-map-bing.nse
pjl-ready-message.nse           ssl-poodle.nse
cics-enum.nse                         http-drupal-enum.nse                    ip-geolocation-map-google.nse
pop3-brute.nse                  sslv2-drown.nse
cics-info.nse                         http-drupal-enum-users.nse              ip-geolocation-map-kml.nse
pop3-capabilities.nse           sslv2.nse
cics-user-brute.nse                   http-enum.nse                           ip-geolocation-maxmind.nse
pop3-ntlm-info.nse              sstp-discover.nse
cics-user-enum.nse                    http-errors.nse                         ip-https-discover.nse
port-states.nse                 stun-info.nse
citrix-brute-xml.nse                  http-exif-spider.nse                    ipidseq.nse
pptp-version.nse                stun-version.nse
citrix-enum-apps.nse                  http-favicon.nse                        ipmi-brute.nse
puppet-naivesigning.nse         stuxnet-detect.nse
citrix-enum-apps-xml.nse              http-feed.nse                           ipmi-cipher-zero.nse
qconn-exec.nse                  supermicro-ipmi-conf.nse
citrix-enum-servers.nse               http-fetch.nse                          ipmi-version.nse
qscan.nse                       svn-brute.nse
citrix-enum-servers-xml.nse           http-fileupload-exploiter.nse           ipv6-multicast-mld-list.nse
quake1-info.nse                 targets-asn.nse
clamav-exec.nse                       http-form-brute.nse                     ipv6-node-info.nse
quake3-info.nse                 targets-ipv6-map4to6.nse
clock-skew.nse                        http-form-fuzzer.nse                    ipv6-ra-flood.nse
quake3-master-getservers.nse    targets-ipv6-multicast-echo.nse
coap-resources.nse                    http-frontpage-login.nse                irc-botnet-channels.nse
```

```
rdp-enum-encryption.nse         targets-ipv6-multicast-invalid-dst.nse
couchdb-databases.nse                 http-generator.nse                      irc-brute.nse
rdp-ntlm-info.nse               targets-ipv6-multicast-mld.nse
couchdb-stats.nse                     http-git.nse                            irc-info.nse
rdp-vuln-ms12-020.nse           targets-ipv6-multicast-slaac.nse
creds-summary.nse                     http-gitweb-projects-enum.nse           irc-sasl-brute.nse
realvnc-auth-bypass.nse         targets-ipv6-wordlist.nse
cups-info.nse                         http-google-malware.nse                 irc-unrealircd-backdoor.nse
redis-brute.nse                 targets-sniffer.nse
cups-queue-info.nse                   http-grep.nse                           iscsi-brute.nse
redis-info.nse                  targets-traceroute.nse
cvs-brute.nse                         http-headers.nse                        iscsi-info.nse
resolveall.nse                  targets-xml.nse
cvs-brute-repository.nse              http-hp-ilo-info.nse                    isns-info.nse
reverse-index.nse               teamspeak2-version.nse
daap-get-library.nse                  http-huawei-hg5xx-vuln.nse              jdwp-exec.nse
rexec-brute.nse                 telnet-brute.nse
daytime.nse                           http-icloud-findmyiphone.nse            jdwp-info.nse
rfc868-time.nse                 telnet-encryption.nse
db2-das-info.nse                      http-icloud-sendmsg.nse                 jdwp-inject.nse
riak-http-info.nse              telnet-ntlm-info.nse
deluge-rpc-brute.nse                  http-iis-short-name-brute.nse           jdwp-version.nse
rlogin-brute.nse                tftp-enum.nse
dhcp-discover.nse                     http-iis-webdav-vuln.nse                knx-gateway-discover.nse
rmi-dumpregistry.nse            tls-alpn.nse
dicom-brute.nse                       http-internal-ip-disclosure.nse         knx-gateway-info.nse
rmi-vuln-classloader.nse        tls-nextprotoneg.nse
dicom-ping.nse                        http-joomla-brute.nse                   krb5-enum-users.nse
rpcap-brute.nse                 tls-ticketbleed.nse
dict-info.nse                         http-jsonp-detection.nse                ldap-brute.nse
rpcap-info.nse                  tn3270-screen.nse
distcc-cve2004-2687.nse               http-litespeed-sourcecode-download.nse  ldap-novell-getpass.nse
rpc-grind.nse                   tor-consensus-checker.nse
dns-blacklist.nse                     http-ls.nse                             ldap-rootdse.nse
```

```
rpcinfo.nse                     traceroute-geolocation.nse
dns-brute.nse                         http-majordomo2-dir-traversal.nse       ldap-search.nse
rsa-vuln-roca.nse               tso-brute.nse
dns-cache-snoop.nse                   http-malware-host.nse                   lexmark-config.nse
rsync-brute.nse                 tso-enum.nse
dns-check-zone.nse                    http-mcmp.nse                           llmnr-resolve.nse
rsync-list-modules.nse          ubiquiti-discovery.nse
dns-client-subnet-scan.nse            http-methods.nse                        lltd-discovery.nse
rtsp-methods.nse                unittest.nse
dns-fuzz.nse                          http-method-tamper.nse                  lu-enum.nse
rtsp-url-brute.nse              unusual-port.nse
dns-ip6-arpa-scan.nse                 http-mobileversion-checker.nse          maxdb-info.nse
rusers.nse                      upnp-info.nse
dns-nsec3-enum.nse                    http-ntlm-info.nse                      mcafee-epo-agent.nse
s7-info.nse                     uptime-agent-info.nse
dns-nsec-enum.nse                     http-open-proxy.nse                     membase-brute.nse
samba-vuln-cve-2012-1182.nse    url-snarf.nse
dns-nsid.nse                          http-open-redirect.nse                  membase-http-info.nse
script.db                       ventrilo-info.nse
dns-random-srcport.nse                http-passwd.nse                         memcached-info.nse
servicetags.nse                 versant-info.nse
dns-random-txid.nse                   http-phpmyadmin-dir-traversal.nse       metasploit-info.nse
shodan-api.nse                  vmauthd-brute.nse
dns-recursion.nse                     http-phpself-xss.nse                    metasploit-msgrpc-brute.nse
sip-brute.nse                   vmware-version.nse
dns-service-discovery.nse             http-php-version.nse                    metasploit-xmlrpc-brute.nse
sip-call-spoof.nse              vnc-brute.nse
dns-srv-enum.nse                      http-proxy-brute.nse                    mikrotik-routeros-brute.nse
sip-enum-users.nse              vnc-info.nse
dns-update.nse                        http-put.nse                            mmouse-brute.nse
sip-methods.nse                 vnc-title.nse
dns-zeustracker.nse                   http-qnap-nas-info.nse                  mmouse-exec.nse
skypev2-version.nse             voldemort-info.nse
dns-zone-transfer.nse                 http-referer-checker.nse                modbus-discover.nse
```

```
smb2-capabilities.nse           vtam-enum.nse
docker-version.nse                    http-rfi-spider.nse                     mongodb-brute.nse
smb2-security-mode.nse          vulners.nse
domcon-brute.nse                      http-robots.txt.nse                     mongodb-databases.nse
smb2-time.nse                   vuze-dht-info.nse
domcon-cmd.nse                        http-robtex-reverse-ip.nse              mongodb-info.nse
smb2-vuln-uptime.nse            wdb-version.nse
domino-enum-users.nse                 http-robtex-shared-ns.nse               mqtt-subscribe.nse
smb-brute.nse                   weblogic-t3-info.nse
dpap-brute.nse                        http-sap-netweaver-leak.nse             mrinfo.nse
smb-double-pulsar-backdoor.nse  whois-domain.nse
drda-brute.nse                        http-security-headers.nse               msrpc-enum.nse
smb-enum-domains.nse            whois-ip.nse
drda-info.nse                         http-server-header.nse                  ms-sql-brute.nse
smb-enum-groups.nse             wsdd-discover.nse
duplicates.nse                        http-shellshock.nse                     ms-sql-config.nse
smb-enum-processes.nse          x11-access.nse
eap-info.nse                          http-sitemap-generator.nse              ms-sql-dac.nse
smb-enum-services.nse           xdmcp-discover.nse
enip-info.nse                         http-slowloris-check.nse                ms-sql-dump-hashes.nse
smb-enum-sessions.nse           xmlrpc-methods.nse
epmd-info.nse                         http-slowloris.nse                      ms-sql-empty-password.nse
smb-enum-shares.nse             xmpp-brute.nse
eppc-enum-processes.nse               http-sql-injection.nse                  ms-sql-hasdbaccess.nse
smb-enum-users.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@debian12:~# nmap -v -sC localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-27 16:51 CET
NSE: Loaded 125 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating SYN Stealth Scan at 16:51
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 5900/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed SYN Stealth Scan at 16:51, 0.03s elapsed (1000 total ports)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 16:51
Completed NSE at 16:51, 2.00s elapsed
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   256 738a4166831b9c8af2bfb567ed025c4d (ECDSA)
|_  256 86dcfbca68069284b2ddb0545cbc4e2b (ED25519)
80/tcp   open  http
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
```

```
|_http-title: Apache2 Debian Default Page: It works
631/tcp  open  ipp
| ssl-cert: Subject: commonName=debian12/organizationName=debian12/stateOrProvinceName=Unknown/countryName=US
| Subject Alternative Name: DNS:debian12, DNS:debian12.local, DNS:localhost
| Issuer: commonName=debian12/organizationName=debian12/stateOrProvinceName=Unknown/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-11-27T15:51:20
| Not valid after:  2035-11-25T15:51:20
| MD5:   508d6d5d71e72656eeda3082e4fcfde0
|_SHA-1: 0bda6fab805a00a5cdc863da5357a3791a58eca6
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Home - CUPS 2.4.2
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 1 disallowed entry
|_/
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|_    VNC Authentication (2)

NSE: Script Post-scanning.
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.45 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.

#### Options de la commande

Les options de cette commande sont :

```
root@debian12:~# nmap --help
Nmap 7.93 ( https://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
  -sO: 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
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - 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
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --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)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --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 (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

### 1.2 - 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.

**Utilisation**

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

```
root@debian12:~# nc 127.0.0.1 80 -w 1 -vv
localhost [127.0.0.1] 80 (http) open
[ENTREE] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> Appuyez sur la touche Entrée
HTTP/1.1 400 Bad Request
Date: Thu, 27 Nov 2025 15:53:56 GMT
Server: Apache/2.4.65 (Debian)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.65 (Debian) Server at 127.0.0.1 Port 80</address>
</body></html>
 sent 1, rcvd 483
```

**Important** - Notez que **netcat** se connecte au port 80 qui est ouvert.

**Options de la commande**

Les options de cette commande sont :

```
root@debian12:~# nc -h
[v1.10-47]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

# 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 **Prévention** 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.

### 2.1 - Installation

Sous Debian 12, **snort** n'est pas installé par défaut. Qui plus est **snort** ne se trouve pas dans les dépôts standards.

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

```
root@debian12:~# apt-get install -y build-essential libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev libssl-dev libluajit-5.1-dev pkg-config libhwloc-dev cmake libpcap-dev libdaq-dev libnetfilter-queue-dev libmnl-dev libnghttp2-dev autoconf libtool cmake git

apt install build-essential libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev luajit hwloc libdumbnet-dev bison flex liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev libmnl-dev autotools-dev libluajit-5.1-dev libunwind-dev libcrep2-dev git -y
```

Créez ensuite le fichier **/etc/ld.so.conf.d/local.conf** qui contient les chemins vers les bibliothèques pour **snort** :

```
root@debian12:~# vi /etc/ld.so.conf.d/local.conf

root@debian12:~# cat /etc/ld.so.conf.d/local.conf
/usr/local/lib
```

```
/usr/local/lib64
/usr/local/snort/bin
```

Créez le répertoire **~/snort-source-files** et clonez le dépôt **https://github.com/snort3/libdaq.git** :

```
root@debian12:~# mkdir ~/snort-source-files

root@debian12:~# cd snort-source-files/

root@debian12:~/snort-source-files# git clone https://github.com/snort3/libdaq.git
Cloning into 'libdaq'...
remote: Enumerating objects: 2617, done.
remote: Counting objects: 100% (239/239), done.
remote: Compressing objects: 100% (78/78), done.
remote: Total 2617 (delta 199), reused 169 (delta 161), pack-reused 2378 (from 2)
Receiving objects: 100% (2617/2617), 1.18 MiB | 13.31 MiB/s, done.
Resolving deltas: 100% (1891/1891), done.
```

Procédez à la compilation et à l'installation de **libdaq** :

```
root@debian12:~/snort-source-files# cd libdaq/

root@debian12:~/snort-source-files/libdaq# ./bootstrap
+ autoreconf -ivf --warnings=all
autoreconf: export WARNINGS=all
autoreconf: Entering directory '.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force -I m4
autoreconf: configure.ac: tracing
autoreconf: running: libtoolize --copy --force
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
```

```
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
autoreconf: configure.ac: not using Intltool
autoreconf: configure.ac: not using Gtkdoc
autoreconf: running: aclocal --force -I m4
autoreconf: running: /usr/bin/autoconf --force
configure.ac:27: warning: The macro `AC_PROG_CC_C99' is obsolete.
configure.ac:27: You should run autoupdate.
./lib/autoconf/c.m4:1659: AC_PROG_CC_C99 is expanded from...
configure.ac:27: the top level
autoreconf: running: /usr/bin/autoheader --force
autoreconf: running: automake --add-missing --copy --force-missing
configure.ac:29: installing './ar-lib'
configure.ac:26: installing './compile'
configure.ac:34: installing './config.guess'
configure.ac:34: installing './config.sub'
configure.ac:19: installing './install-sh'
configure.ac:19: installing './missing'
api/Makefile.am: installing './depcomp'
parallel-tests: installing './test-driver'
autoreconf: Leaving directory '.'

root@debian12:~/snort-source-files/libdaq# ./configure
...
config.status: executing libtool commands

    libdaq 3.0.23

    prefix:         /usr/local
    sysconfdir:     ${prefix}/etc
    libdir:         ${exec_prefix}/lib
    includedir:     ${prefix}/include
    cc:             gcc
    cppflags:
    am_cppflags:     -fvisibility=hidden -Wall -Wmissing-declarations -Wpointer-arith -Wcast-align -Wcast-qual -
Wformat -Wformat-nonliteral -Wformat-security -Wundef -Wwrite-strings -Wextra -Wsign-compare -Wno-unused-
parameter -fno-strict-aliasing -fdiagnostics-show-option
    cflags:         -g -O2
    am_cflags:       -Wstrict-prototypes -Wmissing-prototypes -Wold-style-definition -Wnested-externs
    ldflags:
    am_ldflags:
    libs:

    code_coverage_enabled:  no
    code_coverage_cppflags:
    code_coverage_cflags:
    code_coverage_ldflags:

    Build AFPacket DAQ module.. : yes
    Build BPF DAQ module....... : yes
    Build Divert DAQ module.... : no
    Build Dump DAQ module...... : yes
    Build FST DAQ module....... : yes
    Build netmap DAQ module.... : no
    Build NFQ DAQ module....... : yes
    Build PCAP DAQ module...... : yes
    Build Savefile DAQ module.. : yes
    Build Trace DAQ module..... : yes
    Build GWLB DAQ module...... : yes

root@debian12:~/snort-source-files/libdaq# make
...
make[2]: Leaving directory '/root/snort-source-files/libdaq/example'
Making all in test
make[2]: Entering directory '/root/snort-source-files/libdaq/test'
make[2]: Nothing to be done for 'all'.
```

```
make[2]: Leaving directory '/root/snort-source-files/libdaq/test'
make[2]: Entering directory '/root/snort-source-files/libdaq'
make[2]: Leaving directory '/root/snort-source-files/libdaq'
make[1]: Leaving directory '/root/snort-source-files/libdaq'

root@debian12:~/snort-source-files/libdaq# make install
...
----------------------------------------------------------------------
 /usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
 /usr/bin/install -c -m 644 afpacket/libdaq_static_afpacket.pc bpf/libdaq_static_bpf.pc
dump/libdaq_static_dump.pc fst/libdaq_static_fst.pc nfq/libdaq_static_nfq.pc pcap/libdaq_static_pcap.pc
savefile/libdaq_static_savefile.pc trace/libdaq_static_trace.pc gwlb/libdaq_static_gwlb.pc
'/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/root/snort-source-files/libdaq/modules'
make[1]: Leaving directory '/root/snort-source-files/libdaq/modules'
Making install in example
make[1]: Entering directory '/root/snort-source-files/libdaq/example'
make[2]: Entering directory '/root/snort-source-files/libdaq/example'
 /usr/bin/mkdir -p '/usr/local/bin'
  /bin/bash ../libtool   --mode=install /usr/bin/install -c daqtest daqtest-static '/usr/local/bin'
libtool: install: /usr/bin/install -c .libs/daqtest /usr/local/bin/daqtest
libtool: install: /usr/bin/install -c daqtest-static /usr/local/bin/daqtest-static
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/root/snort-source-files/libdaq/example'
make[1]: Leaving directory '/root/snort-source-files/libdaq/example'
Making install in test
make[1]: Entering directory '/root/snort-source-files/libdaq/test'
make[2]: Entering directory '/root/snort-source-files/libdaq/test'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/root/snort-source-files/libdaq/test'
make[1]: Leaving directory '/root/snort-source-files/libdaq/test'
make[1]: Entering directory '/root/snort-source-files/libdaq'
make[2]: Entering directory '/root/snort-source-files/libdaq'
```

```
make[2]: Nothing to be done for 'install-exec-am'.
 /usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
 /usr/bin/install -c -m 644 libdaq.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/root/snort-source-files/libdaq'
make[1]: Leaving directory '/root/snort-source-files/libdaq'
```

Téléchargez et désarchivez**snort** :

```
root@debian12:~/snort-source-files/libdaq# cd ..

root@debian12:~/snort-source-files# git clone https://github.com/snort3/snort3.git
Cloning into 'snort3'...
remote: Enumerating objects: 123479, done.
remote: Counting objects: 100% (12552/12552), done.
remote: Compressing objects: 100% (1884/1884), done.
remote: Total 123479 (delta 11054), reused 10808 (delta 10668), pack-reused 110927 (from 5)
Receiving objects: 100% (123479/123479), 91.19 MiB | 26.35 MiB/s, done.
Resolving deltas: 100% (104744/104744), done.
```

Procédez à la compilation et à l'installation de **snort3** :

```
root@debian12:~/snort-source-files# cd snort3/

root@debian12:~/snort-source-files/snort3# ./configure_cmake.sh
...
-------------------------------------------------------
snort version 3.10.0.0

Install options:
    prefix:     /usr/local/snort
    includes:   /usr/local/snort/include/snort
    plugins:    /usr/local/snort/lib/snort

```

```
Compiler options:
    CC:             /usr/bin/cc
    CXX:            /usr/bin/c++
    CFLAGS:            -fvisibility=hidden   -DNDEBUG -g -ggdb    -O2 -g -DNDEBUG
    CXXFLAGS:          -fvisibility=hidden   -DNDEBUG -g -ggdb    -O2 -g -DNDEBUG
    EXE_LDFLAGS:
    MODULE_LDFLAGS:

Feature options:
    DAQ Modules:    Static (afpacket;bpf;dump;fst;gwlb;nfq;pcap;savefile;trace)
    libatomic:      System-provided
    Hyperscan:      OFF
    ICONV:          ON
    Libunwind:      ON
    LZMA:           ON
    RPC DB:         Built-in
    SafeC:          OFF
    TCMalloc:       OFF
    JEMalloc:       OFF
    UUID:           ON
    NUMA:           ON
    LibML:          OFF
-------------------------------------------------------

-- Configuring done
-- Generating done
-- Build files have been written to: /root/snort-source-files/snort3/build

root@debian12:~/snort-source-files/snort3# cd build

root@debian12:~/snort-source-files/snort3/build# make
...
[ 98%] Built target preprocessor_states
[ 98%] Building CXX object tools/snort2lua/CMakeFiles/snort2lua.dir/snort2lua.cc.o
[ 98%] Building CXX object tools/snort2lua/CMakeFiles/snort2lua.dir/init_state.cc.o
[ 98%] Linking CXX executable snort2lua
[ 98%] Built target snort2lua
[ 98%] Building C object daqs/CMakeFiles/daq_file.dir/daq_file.c.o
[ 98%] Linking C shared module daq_file.so
[ 98%] Built target daq_file
[ 98%] Building C object daqs/CMakeFiles/daq_hext.dir/daq_hext.c.o
[100%] Linking C shared module daq_hext.so
[100%] Built target daq_hext

root@debian12:~/snort-source-files/snort3/build# make install
...
-- Up-to-date: /usr/local/snort/share/doc/snort/overview.txt
-- Installing: /usr/local/snort/share/doc/snort/snort2lua.txt
-- Installing: /usr/local/snort/share/doc/snort/snort_upgrade.txt
-- Installing: /usr/local/snort/share/doc/snort/config_changes.txt
-- Installing: /usr/local/snort/share/doc/snort/snort_upgrade.text
-- Installing: /usr/local/snort/share/doc/snort/snort_devel.txt
-- Installing: /usr/local/snort/share/doc/snort/extending.txt
-- Installing: /usr/local/snort/share/doc/snort/style.txt
-- Installing: /usr/local/snort/share/doc/snort/versions.txt
```

Dernièrement, modifiez la valeur $PATH de root :

```
root@debian12:~/snort-source-files/snort3/build# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

root@debian12:~/snort-source-files/snort3/build# PATH="/usr/local/snort/bin:$PATH"

root@debian12:~/snort-source-files/snort3/build# echo $PATH
/usr/local/snort/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

root@debian12:~/snort-source-files/snort3/build# vi /root/.profile
```

```
root@debian12:~/snort-source-files/snort3/build# cat /root/.profile
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi

PATH=/usr/local/snort/bin:$PATH:$HOME/bin
export $PATH

mesg n 2> /dev/null || true
```

Vérifiez la bonne installation de snort3 :

```
root@debian12:~/snort-source-files/snort3/build# snort --version

   ,,_     -*> Snort++ <*-
  o"  )~   Version 3.10.0.0
   ''''    By Martin Roesch & The Snort Team
           http://snort.org/contact#team
           Copyright (C) 2014-2025 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using DAQ version 3.0.23
           Using libpcap version 1.10.3 (with TPACKET_V3)
           Using LuaJIT version 2.1.0-beta3
           Using LZMA version 5.4.1
           Using OpenSSL 3.0.17 1 Jul 2025
           Using PCRE2 version 10.42 2022-12-11
           Using ZLIB version 1.2.13
```

**Options de la commande**

```
root@debian12:~/snort-source-files/snort3/build# snort --help

Snort has several options to get more help:

-? list command line options (same as --help)
--help this overview of help
--help-commands [<module prefix>] output matching commands
--help-config [<module prefix>] output matching config options
--help-counts [<module prefix>] output matching peg counts
--help-limits print the int upper bounds denoted by max*
--help-module <module> output description of given module
--help-modules list all available modules with brief help
--help-modules-json dump description of all available modules in JSON format
--help-plugins list all available plugins with brief help
--help-options [<option prefix>] output matching command line options
--help-signals dump available control signals
--list-buffers output available inspection buffers
--list-builtin [<module prefix>] output matching builtin rules
--list-gids [<module prefix>] output matching generators
--list-modules [<module type>] list all known modules
--list-plugins list all known modules
--show-plugins list module and plugin versions

--help* and --list* options preempt other processing so should be last on the
command line since any following options are ignored.  To ensure options like
--markup and --plugin-path take effect, place them ahead of the help or list
options.

Options that filter output based on a matching prefix, such as --help-config
won't output anything if there is no match.  If no prefix is given, everything
matches.
```

```
Report bugs to bugs@snort.org.
```

Snort 3 utilise des modules. Pour consulter la liste des modules, utilisez la commande suivante :

```
root@debian12:~/snort-source-files/snort3/build# snort --help-modules | more
ac_bnfa (search_engine): Aho-Corasick Binary NFA (low memory, low performance) MPSE
ac_full (search_engine): Aho-Corasick Full (high memory, best performance), implements search_all()
ack (ips_option): rule option to match on TCP ack numbers
active (basic): configure responses
address_space_selector (policy_selector): configure traffic processing based on address space
alert (ips_action): manage the counters for the alert action
alert_csv (logger): output event in csv format
alert_fast (logger): output event with brief text format
alert_full (logger): output event with full packet dump
alert_json (logger): output event in json format
alert_syslog (logger): output event to syslog
alert_talos (logger): output event in Talos alert format
alert_unixsock (logger): output event over unix socket
alerts (basic): configure alerts
appid (inspector): application and service identification
appids (ips_option): detection option for application ids
arp (codec): support for address resolution protocol
arp_spoof (inspector): detect ARP attacks and anomalies
attribute_table (basic): configure hosts loading
auth (codec): support for IP authentication header
back_orifice (inspector): back orifice detection
base64_decode (ips_option): rule option to decode base64 data - must be used with base64_data option
ber_data (ips_option): rule option to move to the data for a specified BER element
ber_skip (ips_option): rule option to skip BER element
binder (inspector): configure processing based on CIDRs, ports, services, etc.
block (ips_action): manage the counters for the block action
bufferlen (ips_option): rule option to check length of current buffer
byte_extract (ips_option): rule option to convert data to an integer variable
byte_jump (ips_option): rule option to move the detection cursor
```

```
byte_math (ips_option): rule option to perform mathematical operations on extracted value and a specified value
or existing variable
byte_test (ips_option): rule option to convert data to integer and compare
cip (inspector): cip inspection
cip_attribute (ips_option): detection option to match CIP attribute
cip_class (ips_option): detection option to match CIP class
cip_conn_path_class (ips_option): detection option to match CIP Connection Path Class
cip_instance (ips_option): detection option to match CIP instance
cip_req (ips_option): detection option to match CIP request
cip_rsp (ips_option): detection option to match CIP response
cip_service (ips_option): detection option to match CIP service
cip_status (ips_option): detection option to match CIP response status
ciscometadata (codec): support for cisco metadata
classifications (basic): define rule categories with priority
classtype (ips_option): general rule option for rule classification
content (ips_option): payload rule option for basic pattern matching
cvs (ips_option): payload rule option for detecting specific attacks
daq (basic): configure packet acquisition interface
dce_http_proxy (inspector): dce over http inspection - client to/from proxy
dce_http_server (inspector): dce over http inspection - proxy to/from server
dce_iface (ips_option): detection option to check dcerpc interface
dce_opnum (ips_option): detection option to check dcerpc operation number
dce_smb (inspector): dce over smb inspection
dce_stub_data (ips_option): sets the cursor to dcerpc stub data
dce_tcp (inspector): dce over tcp inspection
dce_udp (inspector): dce over udp inspection
decode (basic): general decoder rules
--More--
```

Pour obtenir une aide sur un module spécifique, utilisez la commande **snort –help-module <nom_module>** :

```
root@debian12:~/snort-source-files/snort3/build# snort --help-module ac_bnfa

ac_bnfa
```

```
Help: Aho-Corasick Binary NFA (low memory, low performance) MPSE

Type: search_engine

Usage: global

Peg counts:

ac_bnfa.searches: number of search attempts (sum)
ac_bnfa.matches: number of times a match was found (sum)
ac_bnfa.bytes: total bytes searched (sum)
```

Dernièrement, vous pouvez obtenir de l'aide sur la configuration de snort avec la commande suivante :

```
root@debian12:~/snort-source-files/snort3/build# snort --help-config | more
interval ack.~range: check if TCP ack value is 'value | min<>max | <max | >min' { 0: }
int active.attempts = 0: number of TCP packets sent per response (with varying sequence numbers) { 0:255 }
string active.device: use 'ip' for network layer responses or 'eth0' etc for link layer
string active.dst_mac: use format '01:23:45:67:89:ab'
int active.max_responses = 0: maximum number of responses { 0:255 }
int active.min_interval = 255: minimum number of seconds between responses { 1:255 }
string address_space_selector[].addr_spaces: list of address space IDs to match
string address_space_selector[].file: use configuration in given file
bool alert_csv.file = false: output to alert_csv.txt instead of stdout
multi alert_csv.fields = 'timestamp pkt_num proto pkt_gen pkt_len dir src_ap dst_ap rule action': selected fields
will be output in given order left to right { action | class | b64_data | client_bytes | client_
pkts | dir | dst_addr | dst_ap | dst_port | eth_dst | eth_len | eth_src | eth_type | flowstart_time | geneve_vni
| gid | icmp_code | icmp_id | icmp_seq | icmp_type | iface | ip_id | ip_len | msg | mpls | pkt_ge
n | pkt_len | pkt_num | priority | proto | rev | rule | seconds | server_bytes | server_pkts | service | sgt| sid
| src_addr | src_ap | src_port | target | tcp_ack | tcp_flags | tcp_len | tcp_seq | tcp_win | ti
mestamp | tos | ttl | udp_len | vlan }
int alert_csv.limit = 0: set maximum size in MB before rollover (0 is unlimited) { 0:maxSZ }
string alert_csv.separator = ', ': separate fields with this character sequence
bool alert_fast.file = false: output to alert_fast.txt instead of stdout
bool alert_fast.packet = false: output packet dump with alert
enum alert_fast.buffers = 'none': output IPS buffer dump (evaluated by IPS rule or an inspector) { 'none' |
'rule' | 'inspector' | 'both' }
int alert_fast.buffers_depth = 0: number of IPS buffer bytes to dump per buffer (0 is unlimited) { 0:maxSZ }
int alert_fast.limit = 0: set maximum size in MB before rollover (0 is unlimited) { 0:maxSZ }
bool alert_full.file = false: output to alert_full.txt instead of stdout
int alert_full.limit = 0: set maximum size in MB before rollover (0 is unlimited) { 0:maxSZ }
bool alert_json.file = false: output to alert_json.txt instead of stdout
multi alert_json.fields = 'timestamp pkt_num proto pkt_gen pkt_len dir src_ap dst_ap rule action': selected
fields will be output in given order left to right { action | class | b64_data | client_bytes | client
_pkts | dir | dst_addr | dst_ap | dst_port | eth_dst | eth_len | eth_src | eth_type | flowstart_time | geneve_vni
| gid | icmp_code | icmp_id | icmp_seq | icmp_type | iface | ip_id | ip_len | msg | mpls | pkt_g
en | pkt_len | pkt_num | priority | proto | rev | rule | seconds | server_bytes | server_pkts | service | sgt|
sid | src_addr | src_ap | src_port | target | tcp_ack | tcp_flags | tcp_len | tcp_seq | tcp_win | t
imestamp | tos | ttl | udp_len | vlan }
int alert_json.limit = 0: set maximum size in MB before rollover (0 is unlimited) { 0:maxSZ }
string alert_json.separator = ', ': separate fields with this character sequence
enum alert_syslog.facility = 'auth': part of priority applied to each message { 'auth' | 'authpriv' | 'daemon' |
'user' | 'local0' | 'local1' | 'local2' | 'local3' | 'local4' | 'local5' | 'local6' | 'local7' }
enum alert_syslog.level = 'info': part of priority applied to each message { 'emerg' | 'alert' | 'crit' | 'err' |
'warning' | 'notice' | 'info' | 'debug' }
multi alert_syslog.options: used to open the syslog connection { cons | ndelay | perror | pid }
bool alerts.alert_with_interface_name = false: include interface in alert info (fast, full, or syslog only)
int alerts.detection_filter_memcap = 1048576: set available MB of memory for detection_filters { 0:max32 }
int alerts.event_filter_memcap = 1048576: set available MB of memory for event_filters { 0:max32 }
bool alerts.log_references = false: include rule references in alert info (full only)
string alerts.order: change the order of rule action application
int alerts.rate_filter_memcap = 1048576: set available MB of memory for rate_filters { 0:max32 }
string alerts.reference_net: set the CIDR for homenet (for use with -l or -B, does NOT change $HOME_NET in IDS
mode)
string alerts.tunnel_verdicts: let DAQ handle non-allow verdicts for
gtp|teredo|6in4|4in6|4in4|6in6|gre|mpls|vxlan traffic
int appid.memcap = 1048576: max size of the service cache before we start pruning the cache { 1024:maxSZ }
bool appid.log_stats = false: enable logging of appid statistics
```

```
int appid.app_stats_period = 300: time period for collecting and logging appid statistics { 1:max32 }
int appid.app_stats_rollover_size = 20971520: max file size for appid stats before rolling over the log file {
0:max32 }
string appid.app_detector_dir: directory to load appid detectors from
bool appid.list_odp_detectors = false: enable logging of odp detectors statistics
string appid.tp_appid_path: path to third party appid dynamic library
string appid.tp_appid_config: path to third party appid configuration file
bool appid.tp_appid_stats_enable: enable collection of stats and print stats on exit in third party module
bool appid.tp_appid_config_dump: print third party configuration on startup
bool appid.log_all_sessions = false: enable logging of all appid sessions
bool appid.enable_rna_filter = false: monitor only the networks specified in rna configuration
string appid.rna_conf_path: path to rna configuration file
string appids.~: comma separated list of application names
ip4 arp_spoof.hosts[].ip: host ip address
--More--
```

### 2.2 - Configuration de Snort

Pour vérifier la configuration actuelle de snort, exécutez la commande suivante :

```
root@debian12:~/snort-source-files/snort3/build# cd ~

root@debian12:~# snort -c /usr/local/snort/etc/snort/snort.lua
--------------------------------------------------
o")~   Snort++ 3.10.0.0
--------------------------------------------------
Loading /usr/local/snort/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        output
        active
        alerts
        daq
        decode
        host_cache
        host_tracker
        hosts
        network
        packets
        process
        search_engine
        so_proxy
        stream
        stream_ip
        stream_icmp
        stream_udp
        stream_user
        stream_file
        arp_spoof
        back_orifice
        imap
        netflow
        normalizer
        pop
        sip
        ssh
        ssl
        telnet
        cip
        dnp3
        iec104
        mms
        modbus
        opcua
        s7commplus
        dce_smb
        dce_tcp
        dce_udp
        dce_http_proxy
        dce_http_server
        gtp_inspect
        port_scan
        smtp
        ftp_server
        ftp_client
        ftp_data
        http_inspect
        http2_inspect
        file_policy
        js_norm
        appid
        wizard
        ips
        binder
        references
        classifications
        file_id
        rpc_decode
        dns
        stream_tcp
        trace
Finished /usr/local/snort/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
--------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0     219       0     219    /usr/local/snort/etc/snort/snort.lua
--------------------------------------------------
```

```
rule counts
       total rules loaded: 219
               text rules: 219
            option chains: 219
            chain headers: 1
--------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      219     219
                    total:      219     219
--------------------------------------------------
fast pattern groups
                to_server: 1
                to_client: 1
--------------------------------------------------
search engine (ac_bnfa)
                instances: 2
                 patterns: 438
            pattern chars: 2602
               num states: 1832
         num match states: 392
             memory scale: KB
             total memory: 71.2812
           pattern memory: 19.6484
        match list memory: 28.4375
        transition memory: 22.9453
appid: MaxRss diff: 3084
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to passive.

Snort successfully validated the configuration (with 0 warnings).
o")~   Snort exiting
```

### 2.3 - Utilisation de snort

Pour lancer Snort 3 en tant qu'outil de détection d'instrusion, utilisez la commande suivante :

```
root@debian12:~# snort -c /usr/local/snort/etc/snort/snort.lua -i ens18 -A alert_fast -s 65535 -k none &
[2] 28057

root@debian12:~# --------------------------------------------------
o")~   Snort++ 3.10.0.0
--------------------------------------------------
Loading /usr/local/snort/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        active
        alerts
        daq
        decode
        host_cache
        host_tracker
        hosts
        packets
        process
        search_engine
        so_proxy
        stream
        stream_ip
        stream_icmp
        stream_tcp
        stream_udp
        stream_user
        stream_file
        arp_spoof
        back_orifice
        dns
        imap
        netflow
        normalizer
        pop
        rpc_decode
        sip
        ssh
        ssl
        telnet
        cip
        dnp3
        iec104
        modbus
        opcua
        s7commplus
        dce_smb
        dce_tcp
        dce_udp
        dce_http_proxy
        dce_http_server
        gtp_inspect
        smtp
        ftp_server
        ftp_client
        ftp_data
        http_inspect
        http2_inspect
        file_policy
        appid
        wizard
        binder
        ips
        classifications
        js_norm
        file_id
        port_scan
        mms
        output
        references
        network
        trace
Finished /usr/local/snort/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
--------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0     219       0     219    /usr/local/snort/etc/snort/snort.lua
--------------------------------------------------
rule counts
       total rules loaded: 219
               text rules: 219
            option chains: 219
            chain headers: 1
--------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      219     219
                    total:      219     219
--------------------------------------------------
fast pattern groups
                to_server: 1
                to_client: 1
--------------------------------------------------
search engine (ac_bnfa)
                instances: 2
```

```
                 patterns: 438
            pattern chars: 2602
               num states: 1832
         num match states: 392
             memory scale: KB
             total memory: 71.2812
           pattern memory: 19.6484
        match list memory: 28.4375
        transition memory: 22.9453
appid: MaxRss diff: 3408
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
Retry queue interval is: 200 ms
++ [0] ens18
[Entrée]

root@debian12:~# ps aux | grep 28057
root       28057  1.9  0.3 188032 56952 pts/3    Sl   15:52   0:03 snort -c /usr/local/snort/etc/snort/snort.lua
-i ens18 -A alert_fast -s 65535 -k none
root       28065  0.0  0.0   6340  2056 pts/3    S+   15:54   0:00 grep 28057
```

Tuez le processus de Snort 3 :

```
root@debian12:~# kill 28057
root@debian12:~# ** caught term signal
== stopping
-- [0] ens18
--------------------------------------------------
Packet Statistics
--------------------------------------------------
daq
                 received: 1070
                 analyzed: 1067
                    allow: 1067
                 rx_bytes: 201558
--------------------------------------------------
codec
                    total: 1067         (100.000%)
                      arp: 12           (  1.125%)
                      eth: 1067         (100.000%)
                    icmp4: 1            (  0.094%)
                 icmp4_ip: 1            (  0.094%)
                    icmp6: 1            (  0.094%)
                     ipv4: 1054         ( 98.782%)
                     ipv6: 1            (  0.094%)
                      tcp: 1052         ( 98.594%)
                      udp: 1            (  0.094%)
--------------------------------------------------
Module Statistics
--------------------------------------------------
ac_full
                 searches: 2
                    bytes: 184
--------------------------------------------------
appid
                  packets: 1055
        processed_packets: 1048
          ignored_packets: 7
           total_sessions: 5
       service_cache_adds: 1
             bytes_in_use: 168
             items_in_use: 1
--------------------------------------------------
arp_spoof
                  packets: 12
--------------------------------------------------
```

```
back_orifice
                  packets: 1
--------------------------------------------------
binder
              raw_packets: 19
                new_flows: 5
                 inspects: 24
--------------------------------------------------
detection
                 analyzed: 1067
--------------------------------------------------
port_scan
                  packets: 1055
                 trackers: 8
--------------------------------------------------
stream
                    flows: 5
             total_prunes: 3
idle_prunes_proto_timeout: 3
       udp_timeout_prunes: 1
      icmp_timeout_prunes: 2
--------------------------------------------------
stream_icmp
                 sessions: 2
                      max: 2
                  created: 2
                 released: 2
--------------------------------------------------
stream_tcp
                 sessions: 2
                      max: 2
                  created: 2
                 released: 2
                 timeouts: 1
             instantiated: 1
                   setups: 2
            data_trackers: 2
              segs_queued: 639
            segs_released: 639
                segs_used: 638
          rebuilt_packets: 144
            rebuilt_bytes: 131204
          client_cleanups: 1
          server_cleanups: 2
        partial_fallbacks: 2
                 max_segs: 199
                max_bytes: 9608
--------------------------------------------------
stream_udp
                 sessions: 1
                      max: 1
                  created: 1
                 released: 1
              total_bytes: 92
--------------------------------------------------
wizard
                tcp_scans: 292
               tcp_misses: 2
                udp_scans: 1
               udp_misses: 1
--------------------------------------------------
Appid Statistics
--------------------------------------------------
detected apps and services
              Application: Services   Clients    Users      Payloads   Misc       Referred
                  unknown: 2          0          0          0          0          0
--------------------------------------------------
Summary Statistics
```

```
--------------------------------------------------
process
                  signals: 1
--------------------------------------------------
timing
                  runtime: 00:10:13
                  seconds: 613.666561
                 pkts/sec: 2
o")~   Snort exiting

[2]+  Done                    snort -c /usr/local/snort/etc/snort/snort.lua -i ens18 -A alert_fast -s 65535 -k
none  (wd: /usr/local/snort/etc/snort)
(wd now: ~)
```

## 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 **Prévention** d'**I**ntrusion (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).

### 3.1 - Installation

Utilisez simplement APT pour installer portsentry :

```
root@debian12:~# apt install portsentry
```

### 3.2 - Configuration

Modifiez le fichier **/etc/portsentry/portsentry.conf** en mofifiant les lignes 135, 135 et 213 et en ajoutant la ligne **270** :

```
root@debian12:~# vi /etc/portsentry/portsentry.conf
```

```
...
   131 # 0 = Do not block UDP/TCP scans.
   132 # 1 = Block UDP/TCP scans.
   133 # 2 = Run external command only (KILL_RUN_CMD)
   134
   135 BLOCK_UDP="1"
   136 BLOCK_TCP="1"
...
   211 # iptables support for Linux with limit and LOG support. Logs only
   212 # a limited number of packets to avoid a denial of service attack.
   213 KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP && /sbin/iptables -I INPUT -s $TARGET$ -m limit --limit 3/minute --limit-burst 5 -j LOG --log-level DEBUG --log-prefix 'Portsentry: dropping: '"
...
    268 #KILL_RUN_CMD="/some/path/here/script $TARGET$ $PORT$ $MODE$"
    269 # for examples see /usr/share/doc/portsentry/examples/
    270 KILL_RUN_CMD="/bin/mail -s 'Portscan from $TARGET$ on port $PORT$' root@localhost < /dev/null"
...
```

### 3.3 - Utilisation

Redémarrez le service **portsentry** :

```
root@debian12:~# systemctl restart portsentry

root@debian12:~# systemctl status portsentry
● portsentry.service - LSB: # start and stop portsentry
     Loaded: loaded (/etc/init.d/portsentry; generated)
     Active: active (running) since Thu 2025-12-04 16:10:22 CET; 2s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 28347 ExecStart=/etc/init.d/portsentry start (code=exited, status=0/SUCCESS)
      Tasks: 2 (limit: 19123)
     Memory: 768.0K
        CPU: 84ms
     CGroup: /system.slice/portsentry.service
             ├─28360 /usr/sbin/portsentry -tcp
             └─28364 /usr/sbin/portsentry -udp

Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 34555
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 31335
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 32770
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 32771
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 32772
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 32773
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 32774
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 31337
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: Going into listen mode on UDP port: 54321
Dec 04 16:10:22 debian12 portsentry[28364]: adminalert: PortSentry is now active and listening.
```

Consultez les processus de Portsentry :

```
root@debian12:~# ps aux | grep portsentry
root       28360  0.0  0.0   2500   112 ?        Ss   16:10   0:00 /usr/sbin/portsentry -tcp
root       28364  0.0  0.0   2500   112 ?        Ss   16:10   0:00 /usr/sbin/portsentry -udp
root       28369  0.0  0.0   6340  2160 pts/3    S+   16:10   0:00 grep portsentry
```