Portsentry

Introduction

portsentry est un programme de détection et de blocage de "scan de ports" (généralement programme qui scanne votre machine à le recherche de ports ouverts, en général dans le but de préparer une attaque).

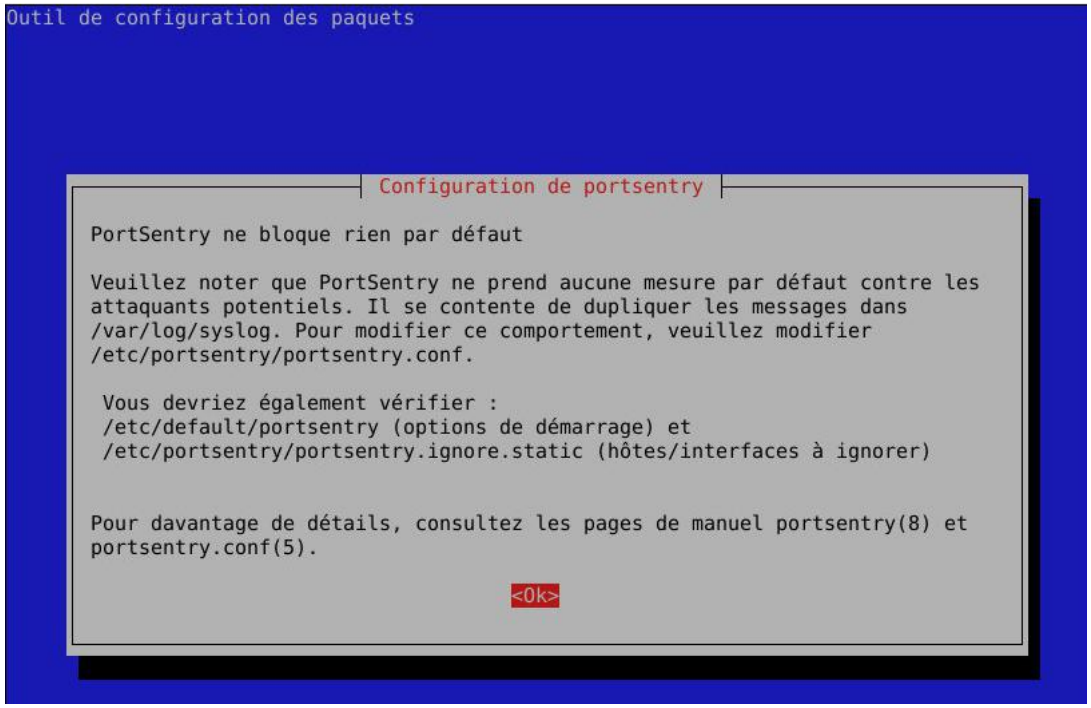
Installation

```
# apt-get update
# apt-get upgrade
# apt-get install portsentry
```

Main page
Le Forum
Téléversements multiples
Actualités
Recent changes
Arborescence des catégories
Random page
Help

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Browse properties

Print/export
Create a book
Download as PDF
Printable version



Configuration

Tel qu'il est installé, portsentry ne fera rien pour vous... il va falloir le configurer pour que la détection, et le blocage soit effectif!

```
# nano /etc/portsentry/portsentry.conf
```

Choisissez ici le niveau de surveillance. Laissez l'option par défaut, elle couvre un nombre de ports raisonnables. Ne choisissez que des ports inutilisés, jusqu'à 64.

Si vous choisissez le mode atcp et audp dans /etc/defaults/portsentry, inutile de préciser les ports; Portsentry va vérifier les ports utilisés et automatiquement "lier" les ports disponibles. C'est l'options la plus efficace ("a" signifie avancé). Avec cette options, portsentry établit une liste des ports d'écoute, TCP et UDP, et bloque l'hôte se connectant sur ces ports, sauf s'il est présent dans le fichier portsentry.ignore.

```
#######################
# Port Configurations #
#######################
# Un-comment these if you are really anal:
#TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,4000,4001,5742,6000,6001,6667,12345,12346,20034,27665,30303

#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,32770,32771,32772,32773,32774,31337,54321"
#
# Use these if you just want to be aware:
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,32773,32774,40421,49724,54320"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321"
#
# Use these for just bare-bones
```

```
#TCP_PORTS="1,11,15,110,111,143,540,635,1080,1524,2000,12345,12346,20034,32771,32772,32773,32774,49724,54320"
#UDP_PORTS="1,7,9,69,161,162,513,640,700,32770,32771,32772,32773,32774,31337,54321"
...
```

Laissez ici les options par défaut, ou ajoutez des ports que vous ne souhaitez pas surveiller:

```
##########################################
# Advanced Stealth Scan Detection Options #
##########################################
...
ADVANCED_PORTS_TCP="1024"
ADVANCED_PORTS_UDP="1024"
...
# Default TCP ident and NetBIOS service
ADVANCED_EXCLUDE_TCP="113,139"
# Default UDP route (RIP), NetBIOS, bootp broadcasts.
ADVANCED_EXCLUDE_UDP="520,138,137,67"
...
```

Emplacement des fichiers de configuration, laissez les choix par défaut.

```
#####################
# Configuration Files#
#####################
#
# Hosts to ignore
IGNORE_FILE="/etc/portsentry/portsentry.ignore"
# Hosts that have been denied (running history)
HISTORY_FILE="/var/lib/portsentry/portsentry.history"
# Hosts that have been denied this session only (temporary until next restart)
BLOCKED_FILE="/var/lib/portsentry/portsentry.blocked"
```

Par défaut BLOCK est à 0. Laissez comme ça pour vos essais, inutile de vous bloquer vous-même... Mettez à un pour mettre "en production".

```
##################
# Ignore Options #
##################
...
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"
...
```

```
###################
# Dropping Routes:#
###################
```

```
...
# Newer versions of Linux support the reject flag now. This
# is cleaner than the above option.
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
```

```
###############
# TCP Wrappers#
###############
...
KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"
```

Attention, dans le fichiers de configuration par défaut, l'option --log-level est fixée à DEBUG (majuscule), option qui ne fonctionne pas avec rsyslog. Ecrivez donc 'debug' en minuscules.

```
###################
# External Command#
###################
...
KILL_RUN_CMD="/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: '"
```

Inutile de faire de la provocation, laissez commenté:

```
######################
# Port Banner Section#
######################
...
#PORT_BANNER="** UNAUTHORIZED ACCESS PROHIBITED *** YOUR CONNECTION ATTEMPT HAS BEEN LOGGED. GO AWAY."
```

Préférez le mode atcp et audp (a pour advanced) c'est le plus efficace:

```
# nano /etc/default/portsentry
```

```
# /etc/default/portsentry
#
# This file is read by /etc/init.d/portsentry. See the portsentry.8
# manpage for details.
#
# The options in this file refer to commandline arguments (all in lowercase)
# of portsentry. Use only one tcp and udp mode at a time.
#
TCP_MODE="atcp"
UDP_MODE="audp"
```

```
# service portsentry restart
Stopping anti portscan daemon: portsentry.
Starting anti portscan daemon: portsentry in atcp & audp mode.
```

Autorisez les scans légitimes

Vous avez la possibilité de laisser certaines IP faire des scans de ports dans le fichier nano /etc/portsentry/portsentry.ignore.static

Pensez à mettre dans ce fichier les machines de votre réseau qui ont la permission de faire des scans... Puis de relancer portsentry:

```
# service portsentry restart
```

Test

Tel qu'il est configuré par apt, portsentry ne sera pas efficace, pas même pour faire de la détection, un nmap depuis une autre machine vous le prouvera:

```
root@nas:~# nmap -v -PN -p 0-2000,60000 10.9.8.2
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2011-10-27 16:08 EAT NSE: Loaded 0 scripts for scanning. Initiating ARP Ping Scan at 16:08 Scanning 10.9.8.2 [1 port] Completed ARP Ping Scan at 16:08, 0.06s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 16:08 Completed Parallel DNS resolution of 1 host. at 16:08, 6.50s elapsed Initiating SYN Stealth Scan at 16:08 Scanning sidlol.zehome.org (10.9.8.2) [2002 ports] Discovered open port 111/tcp on 10.9.8.2 Discovered open port 80/tcp on 10.9.8.2 Discovered open port 22/tcp on 10.9.8.2 Discovered open port 143/tcp on 10.9.8.2 Discovered open port 119/tcp on 10.9.8.2 Discovered open port 635/tcp on 10.9.8.2 Discovered open port 15/tcp on 10.9.8.2 Discovered open port 1/tcp on 10.9.8.2 Discovered open port 79/tcp on 10.9.8.2 Discovered open port 1524/tcp on 10.9.8.2 Discovered open port 11/tcp on 10.9.8.2 Discovered open port 540/tcp on 10.9.8.2 Discovered open port 2000/tcp on 10.9.8.2 Discovered open port 1080/tcp on 10.9.8.2 Completed SYN Stealth Scan at 16:08, 0.12s elapsed (2002 total ports) Host sidlol.zehome.org (10.9.8.2) is up (0.000047s latency). Interesting ports on sidlol.zehome.org (10.9.8.2): Not shown: 1988 closed ports PORT STATE SERVICE 1/tcp open tcpmux 11/tcp open systat 15/tcp open netstat 22/tcp open ssh 79/tcp open finger 80/tcp open http 111/tcp open rpcbind 119/tcp open nntp 143/tcp open imap 540/tcp open uucp 635/tcp open unknown 1080/tcp open socks 1524/tcp open ingreslock 2000/tcp open callbook MAC Address: 00:15:E9:B5:69:26 (D-Link)
```

```
Read data files from: /usr/share/nmap Nmap done: 1 IP address (1 host up) scanned in 6.95 seconds
```

```
          Raw packets sent: 2003 (88.130KB) | Rcvd: 2011 (80.594KB)
```

Rien dans /var/log/syslog...

En remplaçant tcp et udp par atcp et audp dans /etc/default/portsentry, vous obtiendrez de meilleurs résultats...

```
Oct 27 16:11:33 sidlol portsentry[4077]: attackalert: TCP SYN/Normal scan from host: 10.9.8.6/10.9.8.6 to TCP port: 135 Oct 27 16:11:33 sidlol portsentry[4077]: attackalert: Ignoring TCP response per configuration file setting. Oct 27 16:11:33 sidlol portsentry[4077]: attackalert: TCP SYN/Normal scan from host: 10.9.8.6/10.9.8.6 to TCP port: 53 Oct 27 16:11:33 sidlol portsentry[4077]: attackalert: Host: 10.9.8.6/10.9.8.6 is already blocked Ignoring
```

En précisant à portsentry de bloquer les ip qui tentent des scans sur votre serveur, la protection sera bien réelle...

/etc/portsentry/portsentry.conf

```
...
BLOCK_UDP="1"
BLOCK_TCP="1"
```

Le résultat doit être immédiat:

```
# cat /etc/hosts.deny
...
ALL: 10.9.8.6 : DENY
```

```
# iptables -S
...
-A INPUT -s 10.9.8.6/32 -m limit --limit 3/min -j LOG --log-prefix "Portsentry: dropping: " --log-level 7
```

```
# route
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
10.9.8.6   -               255.255.255.255 !H    0      -        0 -
```

```
Le méchant scanner de port est définitivement bloqué...
```

Lol 27 octobre 2011 à 08:44 (CDT)

Category: Sécurité