The sys admin's daily grind: PortSentry

Ten Years After

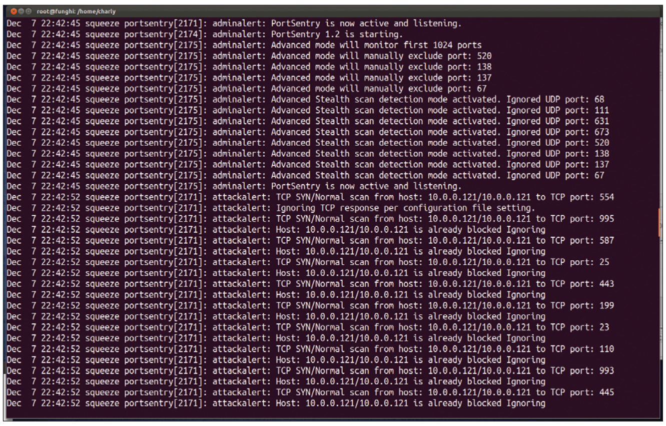
To celebrate 10 years of his column, Charly sets up a sensitive detector that measures the cosmic background radiation of the Internet. *By Charly Kühnast*

Scanning the ports on a machine belonging to someone else is not generally regarded as an attack. Of course, any serious attack will be preceded by a port scan. Administrators who take their security seriously always take a proactive approach to port scans, such as blocking the IP address that initiated the port scan for an extended period of time. The tool that lets you do this goes by the name of PortSentry [1] and is included in most distributions. The daemon identifies and logs port scans and runs commands after doing so.

The detection mode is set in `/etc/default/portsentry`:

```
TCP_MODE="tcp"
UDP_MODE="udp"
```

If you don't want PortSentry to monitor UDP ports, you can simply delete the second line. If you replace `tcp` and `udp` with `stcp` and `sudp`, the tool is more sensitive to stealth scans. If you enter `atcp` and `audp`, it binds all unused ports below 1024 and reports them back to the attacker as open; doing this means that the attacker knows just as much about your system after the scan as beforehand.



```
Dec  7 22:42:45 squeeze portsentry[2171]: adminalert: PortSentry is now active and listening.
Dec  7 22:42:45 squeeze portsentry[2174]: adminalert: PortSentry 1.2 is starting.
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced mode will monitor first 1024 ports
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced mode will manually exclude port: 520
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced mode will manually exclude port: 138
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced mode will manually exclude port: 137
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced mode will manually exclude port: 67
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 68
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 111
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 631
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 673
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 520
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 138
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 137
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: Advanced Stealth scan detection mode activated. Ignored UDP port: 67
Dec  7 22:42:45 squeeze portsentry[2175]: adminalert: PortSentry is now active and listening.
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 554
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Ignoring TCP response per configuration file setting.
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 995
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 587
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 25
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 443
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 199
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 23
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 110
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 993
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: TCP SYN/Normal scan from host: 10.0.0.121/10.0.0.121 to TCP port: 445
Dec  7 22:42:52 squeeze portsentry[2171]: attackalert: Host: 10.0.0.121/10.0.0.121 is already blocked Ignoring
```

Figure 1: PortSentry initializing and detecting port scans in line with its configuration.

The `/etc/portsentry/portsentry.conf` file gives you more scope for setting up the system. Here, you can define trigger ports that act as port scan detectors. The default selection is very useful; I would only change it if I were running a daemon on one of these ports.

It is more important to set the sensitivity with the `SCAN_TRIGGER` variable. The default of `0` means that PortSentry reacts immediately if a trigger port is addressed. Values of 1 or `2` reduce the sensitivity and thus avoid false positives. `ADVANCED_EXCLUDE_TCP=` does the same thing: Ports that are often addressed by external hosts, such as Ident (port 113) and NetBIOS (port 139), are excluded in `atcp` mode; similarly `ADVANCED_EXCLUDE_UDP=` excludes the UDP ports 67, 137, 138, and 520 (DHCP, NetBIOS, RIP) (Figure 1).

By default, PortSentry doesn't respond to scans but simply logs their existence. You can modify this behavior with the following:

```
BLOCK_UDP="0"
BLOCK_TCP="0"
```

A 1 here prevents IP addresses that have issued port scans in the past from opening connections by telling PortSentry to issue the

```
/sbin/route add -host $TARGET$ reject
```

command, which drops the connections and returns a refused message (Figure 1). The IP address that issued the port scan is also logged in `/var/lib/portsentry/portsentry.blocked` and stays there until you restart the daemon.

Securing Your Weapons

To prevent your own systems from falling foul of PortSentry's traps, you have the `/etc/portsentry/portsentry.ignore.static` file, which is where you define individual hosts or whole networks that will not be counterattacked. Incidentally, if you set `BLOCK_TCP` and `UDP` to `2`, PortSentry will run the command that you define as `KILL_RUN_CMD` – this could be something like issuing a text alert, but it could just as easily run the large-bore Metasploit weapon for vicious counterattacks. A word of caution: Pointing a double-barreled shotgun at somebody who knocks at your front door is generally regarded as unfriendly. ■■■

INFO

[1] PortSentry: *http://sourceforge.net/projects/sentrytools/*

AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.