SCANLOGD

Section: System Administration (8)
Updated: 8 May 2002
Index

NAME

scanlogd - detects and logs TCP port scans

SYNOPSIS

scanlogd

DESCRIPTION

scanlogd detects port scans and writes one line per scan via the **syslog**(3) mechanism. If a source address sends multiple packets to different ports in a short time, the event will be logged. The format of the messages is:

saddr[:**sport**] to **daddr** [and others,] ports **port**[, **port**...], ..., **flags**[, TOS **TOS**][, TTL **TTL**] **@HH:MM:SS**

The fields in square brackets are optional; **sport**, **TOS**, and **TTL** will only be displayed if they were constant during the scan.

The **flags** field represents TCP control bits seen in packets coming to the system from the address of the scan. It is a combination of eight characters, with each corresponding to one of the six defined and two reserved TCP control bits (see RFC 793). Control bits that were always set are encoded with an uppercase letter, and a lowercase letter is used if the bit was always clear. A question mark is used to indicate bits that changed from packet to packet.

INTERFACES

In order to do its job, **scanlogd** needs a way to obtain raw IP packets that either come to the system **scanlogd** is running on, or travel across a network segment that is directly connected to the system. Current versions of **scanlogd** can be built with support for one of several packet capture interfaces.

As of version 2.0, **scanlogd** is aware of the **raw socket** interface on Linux, **libnids**, and **libpcap**.

The use of **libpcap** alone is discouraged. If you're on a system other than Linux and/or want to monitor the

traffic of an entire network at once, you should be using **libnids** in order to handle fragmented IP packets.

COMPILE-TIME DEFAULTS

At least 7 different privileged or 21 non-privileged ports, or a weighted combination of those, have to be accessed with no longer than 3 seconds between the accesses to be treated as a scan. If more than 5 scans are detected within 20 seconds, that event will be logged and logging will be stopped temporarily.

Logging is done with a facility of **daemon** and a priority level **alert**.

scanlogd should be started as root since it needs access to a packet capture interface. By default, it switches to running as user **scanlogd** after the packet capture interface is initialized.

EXIT STATUS

If the daemon couldn't start up successfully, it will exit with a status of 1.

USAGE

You're expected to create a dummy user for **scanlogd** to run as. Make sure you allocate unique UID and GID to the user.

In most cases, **scanlogd** should be started from a rc.d script on system startup.

In /etc/syslog.conf you may use something like:

daemon.alert /var/log/alert

SECURITY NOTES

As the name indicates, **scanlogd** only logs port scans. **It does not prevent them.** You will only receive summarized information in the system's log.

Obviously, the source address of port scans can be spoofed. **Don't take any action against the source of attacks unless other evidence is available.** Sometimes IP addresses are shared between many people; this is the case for ISP shell servers, dynamic dialup pools, and corporate networks behind NAT (masquerading).

BUGS

Due to the nature of port scans, both false positives (detecting a scan when there isn't one) and false negatives (not detecting a scan when there's one) are possible. In particular, false positives occur when many small files are transferred rapidly with passive mode FTP.

AUTHORS

Solar Designer **<solar at openwall.com>**
Steffen Dettmer **<steffen at dett.de>** wrote the initial version of this manual page.

SEE ALSO

syslog(3), **syslog.conf**(5), **libnids**(3), **pcap**(3)
scanlogd home page: http://www.openwall.com/scanlogd/
Phrack Magazine, issue 53, article 13

Index

This document was created by man2html, using the scanlogd manual page, and required some editing.