scanlogd - a port scan detection tool

scanlogd is a TCP port scan detection tool, originally designed to illustrate various attacks an IDS developer has to deal with, for a Phrack Magazine article. Thus, unlike some of the other port scan detection tools out there, scanlogd is designed to be totally safe to use.

This release of scanlogd can be built with support for one of several packet capture interfaces. In addition to the raw socket interface on Linux (which does not require any libraries), scanlogd is now aware of 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.

Please read the scanlogd(8) manual page and the original Phrack Magazine article.

Download:

- scanlogd 2.2.7 and its signature
- "Designing and Attacking Port Scan Detection Tools", the Phrack Magazine article

These files, as well as the third-party libraries listed below, are also available from the Openwall file archive. The source code of scanlogd may be browsed via CVSweb.

Follow this link for information on verifying the signatures.

Related third-party raw IP networking libraries:

- libpcap - local copy of libpcap 1.0.0 (512 KB) and its signature
- libnet - required for libnids
  local copy of libnet 1.1.3 release candidate (1129 KB)
  local copy of libnet 1.0.2a (137 KB) - much smaller, but also works with libnids and scanlogd
- libnids - local copy of libnids 1.24 (148 KB) and its signature

Slightly older versions of these libraries are known to work with scanlogd, too.

Commercial support for scanlogd is available, please check out our services. We may help you configure, compile, and install both scanlogd itself and any or all of the third-party raw IP networking libraries.

Contributed resources:

- scanlogd 2.2 pre-compiled for Win32 (195 KB), by Michael Davis

scanlogd is part of Owl, Debian GNU/Linux, Gentoo Linux, OpenSUSE, distributions by ALT Linux team, and OpenWrt. There's an OpenBSD port of scanlogd in the OpenBSD ports collection and a FreeBSD port in the FreeBSD ports collection.

scanlogd is a registered project with Open Hub.

Looking for a good port scanner to test your installation of scanlogd? Use Nmap.

Quick Comment: Send