*This column focuses on secure computing, providing tools and tips for those in the information security trenches. Each issue, we'll evaluate new technologies (primarily in the open source space) and discuss ways to integrate them into your organization.*

*We want to hear from you. Got a great utility or "magic" script that's saved you hours of tedious keyboard pounding? Something new we haven't heard about? Let us know at ciocorner@sandstorm.net.*

# Security Scanners
## Network-Based vs. Host-Based

Running a secure IT infrastructure implies long hours spent securing host PCs. After spending those long hours, how do you know you're secure? You can pay for consultants to run scans against your organization, or you can use several of the readily available tools. Enter the (in)security scanners.

These applications have been around for a long time, going back to tools like SATAN (Security Administration Tool for Analyzing Networks). The rationale is that you can make your systems more secure by breaking into them. Whether or not these sorts of tools are used for "good" or "evil" is not really at issue. The tools exist, and might well be used against you. Why not just use them against yourself to see if you're vulnerable?

### NETWORK-BASED SECURITY SCANNERS

These tools are run over a network against a target machine. The basic idea is to find out as much information about that machine as possible. This includes things like what OS the machine is running, what TCP/UDP ports are open, and what software is listening on those ports.

Nmap is the de facto king of port scanners. It's arguably the most well known scanner to date (it had a brief screen appearance in "The Matrix: Reloaded") – and for a good reason. It's great at what it does.

This scanner will give you the network-based view of what's running on a given host. So a quick "version detection" scan will output something like the box below:

| PORT | STATE | SERVICE | VERSION |
|---|---|---|---|
| 21/tcp | open | ftp | LukemFTPD 1.2 beta 1 (Mac OS X uses lukemftpd derivative) |
| 22/tcp | open | ssh | OpenSSH 3.4p1 (protocol 2.0) |
| 25/tcp | open | smtp | Sendmail 8.12.6/8.12.6 |
| 53/tcp | open | domain | ISC Bind 9.2.1 |
| 80/tcp | open | http | Apache httpd 1.3.29 ((Unix) AxKit/1.61 mod_perl/1.29 DAV/1.0.3 PHP/4.2.3) |
| 111/tcp | open | rpcbind | 2 (rpc #100000) |
| 139/tcp | open | netbios-ssn | Samba smbd (workgroup: EX) |
| 443/tcp | open | ssl/http | Apache httpd 1.3.27 (Ben-SSL/1.48 (Unix)) |
| 587/tcp | open | smtp | Sendmail 8.12.6/8.12.6 |
| 1021/tcp | open | status | 1 (rpc #100024) |
| 1022/tcp | open | nlockmgr | 1-4 (rpc #100021) |
| 1023/tcp | open | mountd | 1-3 (rpc #100005) |
| 2049/tcp | open | nfs? | |
| 2401/tcp | open | cvspserver | cvs pserver |
| 3306/tcp | open | mysql | MySQL 3.23.55-log |
| 8081/tcp | open | http | Apache httpd 1.3.29 ((Unix) AxKit/1.61 mod_perl/1.29 DAV/1.0.3 PHP/4.2.3) |

Device type: general purpose
Running: FreeBSD 4.X
OS details: FreeBSD 4.6.2-RELEASE - 4.8-RELEASE
Uptime 167.927 days (since Wed Dec 3 12:35:43 2003)

Here we can see all the TCP ports that are open, as well as Nmap's best guess as to what's listening on those open ports. It also uses TCP/IP fingerprinting to detect what operating system is running the host in question (there are slight subtleties in the varying implementations of TCP/IP that can be used to distinguish one from another).

It's generally a good idea to do these scans on a regular interval. A compromised system may be modified to hide listening ports from local administrative tools – but such a port may be detected from an external scan. As in the example scan, it gives an administrator the opportunity to do a quick sanity check against the services running on his machines.

Nessus is another network-based security scanner. This application actually incorporates Nmap in its security scan, but goes several steps further in that it launches "attacks" against the target to determine vulnerability against known exploits. It uses client/server architecture, so that several clients can launch scans from a single server. This can be beneficial when developing a traffic filtering policy. The server uses plug-ins, which define the attack pattern for a given exploit. Plug-ins can be marked as "dangerous," meaning they may cause the host to misbehave. Nessus generates excellent reports in a variety of formats.

### HOST-BASED SECURITY SCANNERS

These scanners run on the target machine. They check the host for insecure file permissions, vulnerable software, user

management issues, and so on. The problem with the development of host-based scanners is that the very nature of system development is highly specialized and constantly changing. In order to do a thorough scan of a host, the scanner must know about the intricacies of the user's operating system (the specific version of the system including patch level), the hardware platform, and the installed software. This is a huge undertaking.

An example of a host-based scanner is Tiger. This program was originally developed to scan Unix systems at Texas A&M. Although development fizzled around 1994, the project has been resurrected, and the code substantially improved.

Tiger runs a series of checks against the host, and generates a report file. It does not require root privileges, though certain checks will fail (or will be less accurate) if executed as a non-privileged user. The checks are generally thorough, but may require some tweaking – depending on the target operating system. Tiger will check for a myriad of local security problems, including device permissions, SUID files, the existence of unusual dot-files and so on.

These types of scans should be incorporated into a baseline security model. The reason is simple: Nmap won't tell you that /var/log/wtmp is world writable, but Tiger will:

```
# Checking for existence of log files...
–FAIL– [logf004f] Log file /var/log/wtmp
permission should be 644
–FAIL– [logf004f] Log file /var/run/utmp
permission should be 644
```

## BOTH HAVE A PLACE IN TODAY'S IT SECURITY TOOLKIT

Network-based scanners are generally more mature and they are in wide use by both security professionals and the script kiddy next door. Setting up a dedicated Nessus scanner for use by your InfoSec team is an excellent way to get started scanning. Any unused PC that's lying around could quickly be put to good use as a scanner. Scanning from both inside and outside your firewall will yield valuable results.

Host-based scanners will take more effort to research the correct tool for the job, and then will involve a configuration effort to get up and running. We've just scraped the surface of the available scanners. Rest assured that the hackers know these tools inside out, and use them on a daily basis.

Send us email with your favorite scanner at ciocorner@sandstorm.net and maybe we will feature it in a forthcoming column. Scan just finished – time to start another. CDM

## REFERENCES:

http://www.insecure.org/nmap/
http://www.nessus.org/
http://savannah.nongnu.org/projects/tiger
http://www.sandstorm.net/security/scanners

**Walker Whitehouse** *is CIO and* **Mike Yamamoto** *is a Network Systems Engineer at Sandstorm Enterprises, which develops aggressive software products for network monitoring, network forensics analysis, and security auditing including telephone scanning, penetration testing, and vulnerability assessment.*