

## **MAKING USE OF FREE SECURITY TOOLS TO IMPROVE NETWORK SECURITY**

*This article appeared in the March/April 2000 issue of Internet Security Magazine*

By Eric Maiwald

### **Introduction**

Scanning networks and systems for vulnerabilities has become a necessary part of information security programs. A number of commercial vulnerability scanners are now on the market and most perform the task very well. Unfortunately, not all security budgets allow for the purchase of commercial tools. How can limited budget security departments efficiently identify vulnerabilities?

The answer is free scanning tools. A number of free tools exist (and the number is increasing all the time). In this paper, we examine four of the most useful tools for identifying vulnerabilities and mapping networks and discuss how they can be used to increase the security of your network.

### **Tools**

The four tools that we will examine are queso, nmap, saint, and nessus. All four are available free of charge (download sites can be found at the end of this paper) and are easy to install and use. All four tools also run only on Unix (Nessus does have a Windows client but still requires a Unix for the server piece).

### **Queso**

Queso is a tool that identifies the operating system of a target system. It does this by sending seven packets, one normal SYN packet and six with unexpected combinations of TCP flags, to the target. The operating system is identified by how the target responds to the packets. The packet characteristics that are examined include the sequence number, the ack number, the window, and the flags.

To use queso, issue the following command:

```
queso [options] host[/bits] [:port]
```

Host can be the name of a host or the host's IP address. The number of bits identifies the number of bits of the IP address that are significant. In order to target an entire class C address space, you would use 24 bits for example.

There are several options available for queso. The most useful options are `^d` and `^p` (a complete list of options can be found by typing queso with no options or targets identified. The `^d` option turns on debug mode and provides a list of the packets from the target. The `^p` options allows the user to specify the target port. The default port is 80 (http).

Queso can be used to scan large numbers of IP addresses for responding systems and to provide the identification of the operating system. Run queso against common ports (139 for Windows NT and 95/98 systems, 80, 25, 23, and 21 for Unix systems). It will be more accurate if you run several ports against your entire IP address range. That way you will likely pick up most of your systems.

By piping the queso output into a file, you can compare your results over time and identify new systems on your network. You can also identify how many systems are responding to mail and web traffic.

## Nmap

Nmap is a port scanning tools with a number of features that make it a useful security tool. The primary purpose of the tool is to identify systems that are up and the port to which they listen. The command syntax for nmap is:

```
Nmap [scan type] [options] <host or net #| ΣΣ host or net #N>
```

As you can see from the syntax, nmap will take any number of host names or IP addresses as command line arguments. You can also specify networks by specifying the number of significant bits in the address. For example:

```
192.168.1.0/24
```

This specification tells nmap to scan all the hosts in the 192.168.1.x subnet.

Nmap has the capability to perform normal port scans by attempting to connect to each port as well as stealth scans that are more difficult to detect. Nmap also has the capability to perform operating system identification in a manner similar to that of queso.

To perform a normal scan of your network while identifying all open TCP ports, you would issue the command:

```
Nmap -sT -O 192.168.1.0/24
```

This line tells nmap to perform a normal TCP connect scan (-sT) and perform operating system identification (-O) against the entire 192.168.1.x subnet. The output will come to the screen. This scan will search for all open TCP ports from 1-1024 plus those defined in /etc/services. Additional port ranges can be specified by using the -p option.

The results of such a scan look like this:

Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)  
Interesting ports on localhost (127.0.0.1):

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
25	open	tcp	smtp
515	open	tcp	printer
6000	open	tcp	X11

TCP Sequence Prediction: Class=random positive increments  
Difficulty=4960811 (Good luck!)

Remote operating system guess: Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

If we pipe the results to a file, we can use this file to identify hosts that respond on certain ports. By using the -m option, we can have nmap send the results to a file in a delimited format. This format can be used to load the information into a database or a spreadsheet.

## Saint

Saint is a tool developed by World Wide Digital Security. It is a follow-on to the original SATAN tool and uses the same type of web based user interface. Saint requires a web browser to run.

Saint can be configured to scan a single host or an entire subnet. Scans can be light, medium, or heavy. Saint does not allow you to change the checks used with the light, medium or heavy scans, however.

Once the scan is complete, Saint provides a web-based report on the target system. Reports can be sorted by vulnerability, by host, or by operating system. This report includes the name and address of the targets and the network services that are running on the system (see figure 1). If vulnerabilities exist, they are shown in red. Hyperlinks are provided for more information on the vulnerabilities.

## Nessus

The Nessus Project is attempting to build a world-class vulnerability scanning tool that can be made available free of charge. The members of the project are working on several versions of the tool including a Unix version, a Windows NT version and a Java version. All of the versions work from a client/server model. In other words, there is a server component that actually performs the scans and a client component that allows for target selection and scan configuration. The two components do not need to reside on the same system and access to the Nessus server can be limited to certain user Ids.

Nessus will perform port scans as well as vulnerability scans against the target system. Vulnerabilities to be tested are chosen by the user (see figure 2). Once the scan is complete, Nessus provides a graphical report to the user (see figure 3). The report can be saved as a text file and used to develop vulnerability reports.

## Putting it All Together

Now that we have these tools and we can do a basis scan with them, how can they help improve the security of your organization? The use of any of these

tools can help to identify systems on your network. These tools can also be used to identify what ports and what vulnerabilities exist on your network. By performing regular scans, providing the results to system administrators, and comparing the results of consecutive scans, you will be able to identify new systems on your network, systems that are offering services that they should not be, and systems that may be vulnerable to attack.

Regular scanning is the key to all of this. If you are going to use these free tools, make sure that you develop a procedure so that your networks are scanned on a monthly basis. Take the results to the system administrators and show them how the systems can be vulnerable to attack. Then scan to determine if the vulnerabilities have been corrected.

### **Where to Find the Tools**

Queso: <http://www.apostols.org>  
Nmap: <http://www.insecure.org>  
Saint: <http://www.wwdsi.com>  
Nessus: <http://www.nessus.org>

