Global Information Assurance Certification Paper

Using Fport on Windows NT to Map Applications to Open Ports

by Teena J. Henson

Overview

To develop defense-in-depth computer security, an understanding of various vulnerabilities must be realized before a protection strategy is developed. One element to minimize vulnerabilities is to develop computer security policies, and these policies must be in practice. In addition, risk assessments should be performed, and the highest risk-factor vulnerabilities must be eliminated promptly. A commonly accepted computer security policy usually starts with a firewall being established at the company's Internet connection. A next step could be host scanning or network intrusion detection systems within the organization. Also for consideration is "backdoor" access to the network via modem connections from other networks. Policies should extend to routine backups for critical data. Additional protection can be installed with host-based intrusion detection systems to protect against the "insider threat" or access through the firewall. However, to establish an effective host-based intrusion detection system, knowledge of the services and applications that open ports on the system is a necessity.

The Question

An interesting question was posed by Chris Brenton in his "Poor Man's NT Auditing" presentation portion of the coursework for the SANS GSEC Certification. Mr. Brenton asked "The $64,000 question is, can you identify each of the processes running on your machine that have opened each of the listed listening ports?"

The Goal

Identify all open ports on a Windows NT 4.0 Workstation utilizing tools and knowledge provided in the SANS GSEC coursework or obtained from the internet.

Methods Used to Achieve the Goal

1) Issue a netstat-a command at a MS-DOS command prompt to reveal the open ports on your system. This list may be surprising. There are many applications

and services that open ports, and the goal is to find what these are and why they are opening these specific ports.

"Netstat –a" provides the protocol, the local address (your system) and port, the foreign address (the system you connected to) and the state of the connection. This data can be redirected into a file by issuing the netstat –a > filename command at the command prompt for comparison purposes.

2) To manually identify what services or applications are opening ports, start by shutting down some services. Go to "start", "control panel", "services" and "stop" a service that appears to map to an application. e.g., Norton Antivirus Client. Once the service is stopped, issue the "netstat –a" command again. If this service was opening a port or ports, the output of the netstat command will show less open ports. This method of course, is very time intensive and still doesn't produce the actual executable that is opening the port.

3) Another test for open ports is to close any applications that load upon startup of the system. There are many applications that open ports. Some applications, like Nukenabber, open ports to "listen" on them for hacker activity.

Through many stop and start of services, closing of applications, shutdowns and restarts of your system, a small amount of information may be derived using this method. But it is still very difficult to identify the specific application opening the port with the standard utilities provided with the system.

Fport

Fport is a free tool provided by Foundstone, which will identify the specific applications that open ports on your system. According to Foundstone's web page, Foundstone is "…. a versatile all-star team of computer security professionals. Each of our experts brings something special to the company, creating a collection of security knowledge and experience unmatched in the industry." Foundstone provides free tools for security staff to use to better secure their systems. They also provide consulting services and training for security professionals.

Fport is a fairly new tool developed by Foundstone. It is available at: http://www.foundstone.com/rdlabs/tools.php?category=Forensic and is easy to install. Download the file, unzip the package and run fport from a MS-DOS prompt window. Output can be redirected to a file (fport > filename) and imported into Microsoft Excel for sorting purposes. The table below is an example of the output.

135	TCP	C:\WINNT\system32\RpcSs.exe
1025	TCP	C:\WINNT\system32\RpcSs.exe
1028	TCP	C:\WINNT\system32\RpcSs.exe
135	UDP	C:\WINNT\system32\RpcSs.exe
1084	TCP	C:\Program Files\Netscape\Communicator\Program\netscape.exe
1085	TCP	C:\Program Files\Netscape\Communicator\Program\netscape.exe
1086	TCP	C:\Program Files\Netscape\Communicator\Program\netscape.exe
1087	TCP	C:\Program Files\Netscape\Communicator\Program\netscape.exe
13	TCP	C:\WINNT\System32\tardisnt.exe
37	TCP	C:\WINNT\System32\tardisnt.exe
13	UDP	C:\WINNT\System32\tardisnt.exe
37	UDP	C:\WINNT\System32\tardisnt.exe
123	UDP	C:\WINNT\System32\tardisnt.exe
1029	TCP	C:\WINNT\system32\MSTask.exe
1030	TCP	C:\WINNT\system32\MSTask.exe
38037	UDP	C:\WINNT\System32\MsgSys.EXE
53	TCP	C:\Program Files\NukeNabber\nukenabber.exe
129	TCP	C:\Program Files\NukeNabber\nukenabber.exe
137	TCP	C:\Program Files\NukeNabber\nukenabber.exe
138	TCP	C:\Program Files\NukeNabber\nukenabber.exe
139	TCP	C:\Program Files\NukeNabber\nukenabber.exe
1027	TCP	C:\Program Files\NukeNabber\nukenabber.exe
1032	TCP	C:\Program Files\NukeNabber\nukenabber.exe
1080	TCP	C:\Program Files\NukeNabber\nukenabber.exe
5000	TCP	C:\Program Files\NukeNabber\nukenabber.exe
5001	TCP	C:\Program Files\NukeNabber\nukenabber.exe
19	UDP	C:\Program Files\NukeNabber\nukenabber.exe
1041	UDP	C:\Program Files\NukeNabber\nukenabber.exe

Analyzing the Ports

Following is an analysis of the ports open on the system being reviewed.

RpcSs.exe – The Remote Procedure Call Server Service. A remote procedure call is described in "Microsoft Windows NT 4.0 Security, Audit, and Control" as "RPCs allow commands to be sent from one system to execute programs on another system." An interesting additional bit of information provided was "RPC's security implications include a denial of service attack against the RPC port of TCP/IP. RPC operates on port 135 and a telnet to this port in a Windows NT system that is not patched to Service Pack 3 could be susceptible to this." So this is one of the important reasons to apply the latest service pack.

Netscape.exe – The web browser. Through testing, it was determined that Netscape opens ports within a range – usually anywhere from 1055 – 1300 or more depending on the number of web pages open. Also, by using netstat –a, an identification of the destination system is available, which could aid in the analysis of a system that has been suspected of going to an inappropriate web site which has been disallowed by a company's computer use policy. Here is an example of netstats' output regarding destination systems:

TCP	janedoepc:1130	img3.yahoo.com:80	LAST_ACK
TCP	janedoepc:1166	server1.sans.org:80	LAST_ACK
TCP	janedoepc:1205	server1.sans.org:80	LAST_ACK
TCP	janedoepc:1207	server1.sans.org:80	LAST_ACK
TCP	janedoepc:1208	server1.sans.org:80	LAST_ACK
TCP	janedoepc:1209	server1.sans.org:80	LAST_ACK
TCP	janedoepc:1293	www.foundstone.com:80	LAST_ACK
TCP	janedoepc:1312	www.foundstone.com:80	CLOSE_WAIT
TCP	janedoepc:1313	www.foundstone.com:80	CLOSE_WAIT

Tardisnt.exe – Information was available on this product from the developer's website http://www.kaska.demon.co.uk/. "Tardis is a shareware utility for Windows that makes sure your PC's clock tells the right time." Tardis uses ports identified in RFCs 868, 867 and 2030. RFC 868 specifies the standard for the Time protocol, which uses TCP and UDP port 37. RFC 867, the Daytime protocol, uses TCP and UDP port 13. RFC 2030, the SNTP protocol uses the same port specified in RFC 1305, the Network Time Protocol (NTP). That port is UDP port 123. So the tardisnt application's behaviour was normal.

MSTask.exe – This is the Task Scheduler program. This is the UNIX cron equivalent. Unless the system administrator has established jobs to be run at a later time using the "at" command, this service can be disabled in the services control panel. This service runs on TCP ports 1029 and 1030.

MsgSys.exe – This program opened port 38037 when the Norton Antivirus Client was started as a service. In checking the properties of this file, it was actually created by Intel. A thorough search of Intel's web page regarding this file revealed nothing. A search of the disk drive showed that this file was indeed installed during the installation of Norton Antivirus software.

Nukenabber.exe – This is a freeware product distributed by Dynamic Solutions International (DSI). Following is DSI's description of the software from the web page:

> NukeNabber sets itself up to listen on TCP and UDP ports commonly attacked over the Internet. A total of 50 ports can be monitored simultaneously. ICMP dest_unreach attacks are now logged. It is designed to give you the information you need in order to trace an attacker including a method of finding an attacker's nickname on IRC (mIRC, VIRC and PIRCH clients are supported).

The output from fport regarding Nukenabber will change based on the configuration of Nukenabber. As noted above, Nukenabber can monitor up to 50 ports simultaneously, so this list could become very large. This specific configuration has Nukenabber "watching" ports TCP53, TCP129, TCP137, TCP138, TCP139, TCP1027, TCP1032, TCP1080, TCP5000, TCP5001, UDP19, and UDP1041.

Upon conclusion of analysis of the ports, it was determined that all open ports were valid excluding TCP ports 1029 and 1030. These were the ports opened by the Task Scheduler, which was not needed. This service was reconfigured to a manual startup in the services control panel so the ports would not be opened unnecessarily.

Summary

Fport used with netstat –a and Microsoft Excel can help you answer another question asked by Mr. Brenton, "How well do you know your system?" By routinely using this tool, a system administrator can become familiar with the applications that open ports, and what ports those applications open. A snapshot of the system can be taken with all of the applications running that are typical. This can be used for comparison purposes after installation of a service or software so any newly opened ports can be identified.

Also, information derived from fport may also be used in conjunction with a "tripwire" type of application. Identify the executables that open ports and set up tripwire to monitor these applications. If a hacker was able to plant a Trojan version of one of these applications to open a port that would appear "normal", based on your snapshot of the system tripwire would send notification that the actual executable had changed. You would know something had gone wrong with the application and that you should shut it down.

The use of fport allows you to answer both questions posed by Mr. Brenton. It took some searching to find it, but should be considered a must for any Windows NT system administrator's toolkit.

In conclusion, expanded studies in the computer security area underscore and elevate the importance of continued education in this area. Ensuring that no system has vulnerabilities is only one aspect of securing a system. Remaining aware of current hacker exploits is necessary to provide enhanced computer security protection. Staying current on tools that aid in the securing of a system is invaluable to the oftentimes-overworked system administrator.

References

SANS GSEC Certification Course Materials; Chris Brenton's "Poor Man's NT Auditing".

Jumes, Cooper, Chamoun, and Feinman. Microsoft Windows NT 4.0, Security, Audit, and Control. Redmond: Microsoft Press, 1999. 77

Puppet's Place Web Page; http://www.dynamsol.com/puppet/nukenabber.html

Foundstone; http://www.foundstone.com

Microsoft Corporation; http://www.microsoft.com

HC Mingham-Smith Ltd.; http://www.kaska.demon.co.uk/.

Symantec Corporation; http://www.symantec.com

Intel Corporation; http://www.intel.com