Use these tools to plug security holes in your network

Mar 5, 2002
Steven Warren MCSE, MCDBA, Net+

With the increasing demands of today's network security, more and more network professionals are looking for ways to quickly locate and fix holes in their security matrix. Network security is not just about implementing a firewall and then leaving it alone. You should be auditing, reviewing logs, running scans, and developing good security policies that will keep your network protected. This article will show you some tools that can help you manage network security in a Windows network.

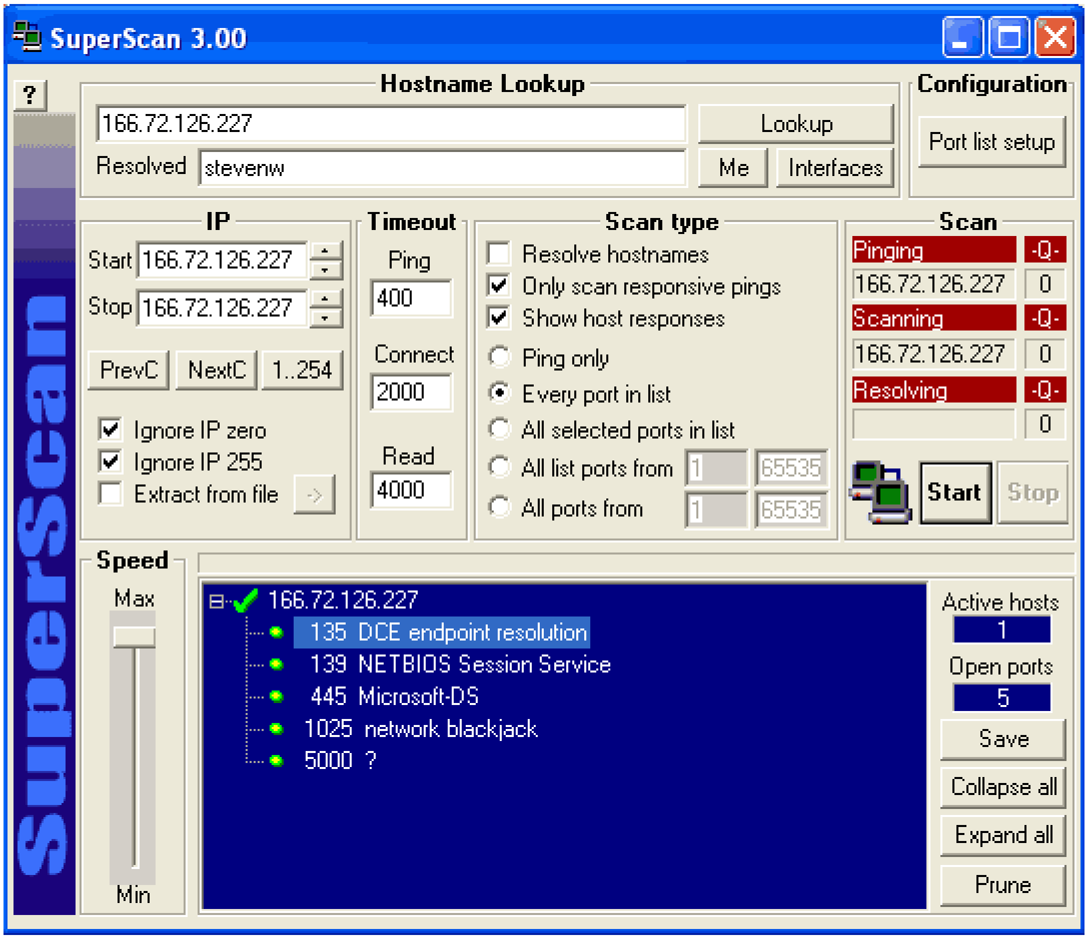
Port scanners

A port scanner will probe your system for open TCP and UDP ports. This is a good tool to help you determine what ports you may or may not need to keep open on your firewall and routers. It will also help you determine whether you have any active Trojans (placed by hackers) on your system that are listening on open ports. Here are two port scanners that will help you identify open ports on your systems.

SuperScan

SuperScan is a free download that allows you to check a range of ports or to scan a range of IP addresses. It comes with a slick and easy to use GUI, as shown in **Figure A**.

Figure A



166.72.126.227
Resolved stevenw

Start 166.72.126.227
Stop 166.72.126.227

☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Ping 400
Connect 2000
Read 4000

☐ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
● Every port in list
○ All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

Pinging -Q-
166.72.126.227 0
Scanning -Q-
166.72.126.227 0
Resolving -Q-
0

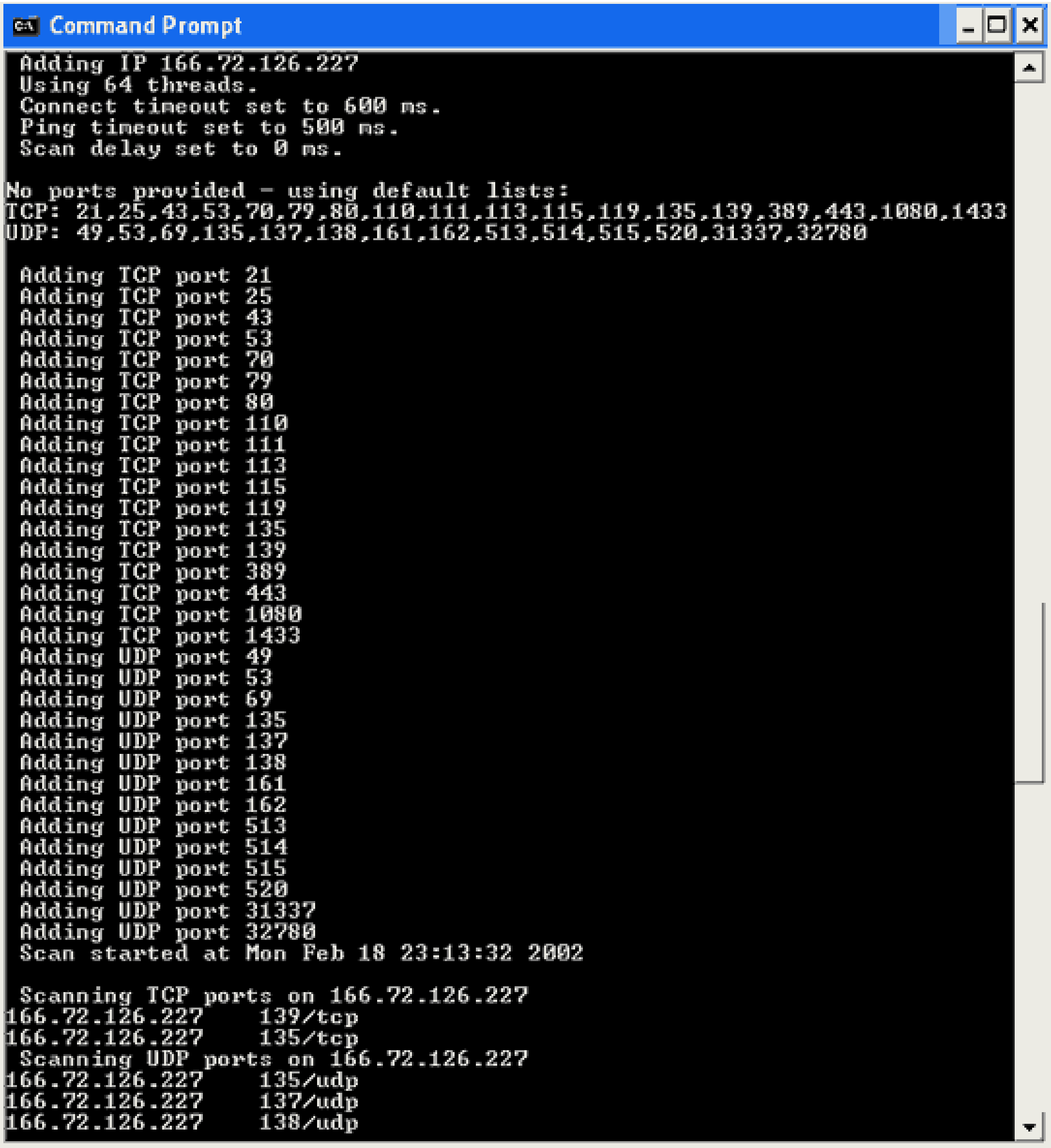
```
⊟ ✓ 166.72.126.227
     ● 135  DCE endpoint resolution
     ● 139  NETBIOS Session Service
     ● 445  Microsoft-DS
     ● 1025  network blackjack
     ● 5000  ?
```

Active hosts 1
Open ports 5

FScan

FScan is a command-line port scanner (**Figure B**) that allows you to scan ports and redirect the results to a text file of your choice. In addition to scanning TCP ports, you can scan UDP ports. This tool can scan over 200 ports per second. To download FScan, click here and then click Scanner, FScan, and Download Now.

Figure B



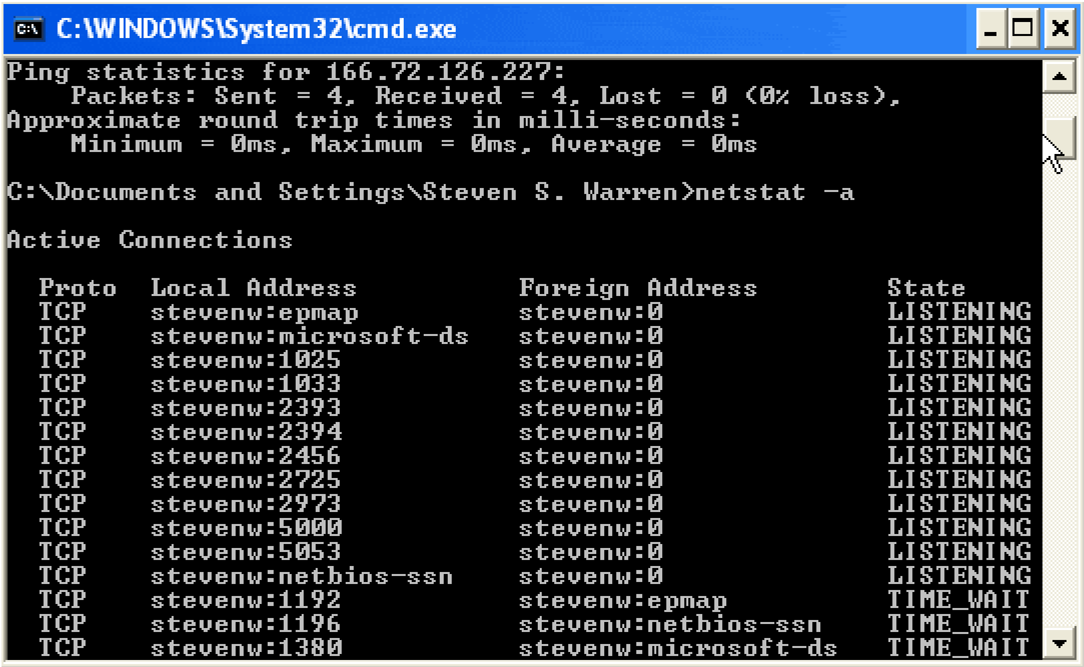
```
 Adding IP 166.72.126.227
 Using 64 threads.
 Connect timeout set to 600 ms.
 Ping timeout set to 500 ms.
 Scan delay set to 0 ms.

No ports provided - using default lists:
TCP: 21,25,43,53,70,79,80,110,111,113,115,119,135,139,389,443,1080,1433
UDP: 49,53,69,135,137,138,161,162,513,514,515,520,31337,32780

 Adding TCP port 21
 Adding TCP port 25
 Adding TCP port 43
 Adding TCP port 53
 Adding TCP port 70
 Adding TCP port 79
 Adding TCP port 80
 Adding TCP port 110
 Adding TCP port 111
 Adding TCP port 113
 Adding TCP port 115
 Adding TCP port 119
 Adding TCP port 135
 Adding TCP port 139
 Adding TCP port 389
 Adding TCP port 443
 Adding TCP port 1080
 Adding TCP port 1433
 Adding UDP port 49
 Adding UDP port 53
 Adding UDP port 69
 Adding UDP port 135
 Adding UDP port 137
 Adding UDP port 138
 Adding UDP port 161
 Adding UDP port 162
 Adding UDP port 513
 Adding UDP port 514
 Adding UDP port 515
 Adding UDP port 520
 Adding UDP port 31337
 Adding UDP port 32780
 Scan started at Mon Feb 18 23:13:32 2002

 Scanning TCP ports on 166.72.126.227
166.72.126.227    139/tcp
166.72.126.227    135/tcp
 Scanning UDP ports on 166.72.126.227
166.72.126.227    135/udp
166.72.126.227    137/udp
166.72.126.227    138/udp
```

TCP/IP tools in Windows

When administering security, you need to have a good grasp of the basic TCP/IP tools. The following are command-line TCP/IP tools that are built in to Windows NT/2000:

- **Netstat**—Windows administrators should be very familiar with this tool. It can quickly tell you what TCP and UDP ports are in use on a system. From the command line, simply type *netstat –a* for a list of open and listening ports, such as the one shown in **Figure C**.

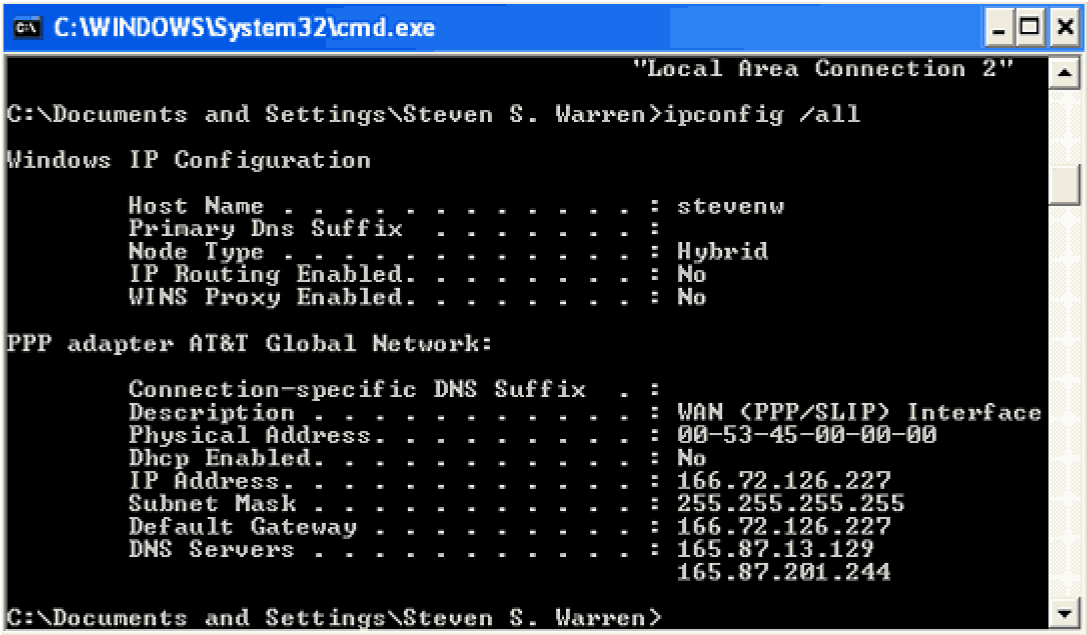
Figure C



```
Ping statistics for 166.72.126.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Steven S. Warren>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    stevenw:epmap          stevenw:0              LISTENING
  TCP    stevenw:microsoft-ds   stevenw:0              LISTENING
  TCP    stevenw:1025           stevenw:0              LISTENING
  TCP    stevenw:1033           stevenw:0              LISTENING
  TCP    stevenw:2393           stevenw:0              LISTENING
  TCP    stevenw:2394           stevenw:0              LISTENING
  TCP    stevenw:2456           stevenw:0              LISTENING
  TCP    stevenw:2725           stevenw:0              LISTENING
  TCP    stevenw:2973           stevenw:0              LISTENING
  TCP    stevenw:5000           stevenw:0              LISTENING
  TCP    stevenw:5053           stevenw:0              LISTENING
  TCP    stevenw:netbios-ssn    stevenw:0              LISTENING
  TCP    stevenw:1192           stevenw:epmap          TIME_WAIT
  TCP    stevenw:1196           stevenw:netbios-ssn    TIME_WAIT
  TCP    stevenw:1380           stevenw:microsoft-ds   TIME_WAIT
```

- **Ipconfig**—This utility displays the TCP/IP configuration of your computer. Type *ipconfig /all*, as shown in **Figure D**, to display the TCP/IP configuration.

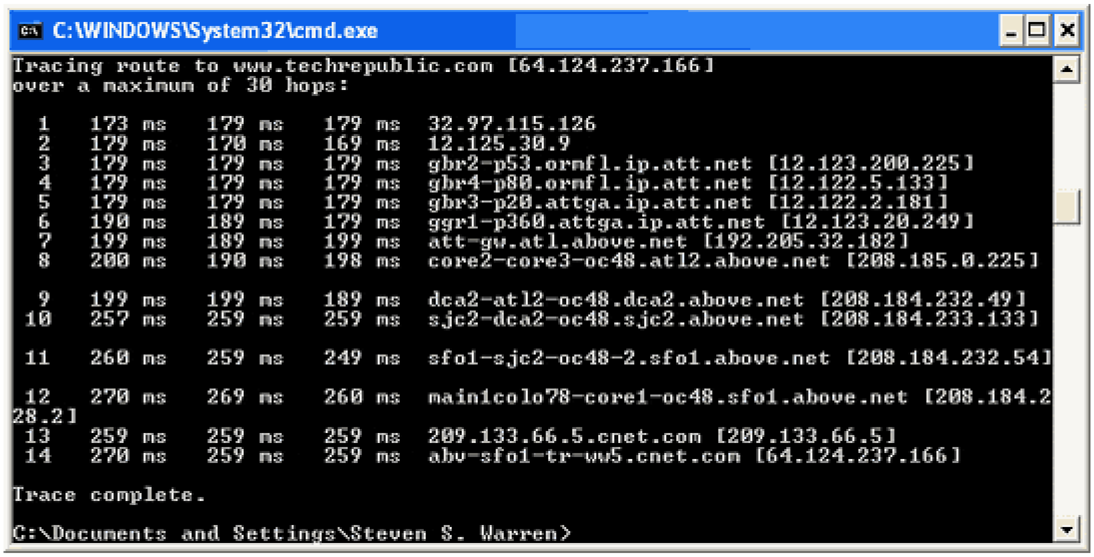
Figure D



```
                                         "Local Area Connection 2"

C:\Documents and Settings\Steven S. Warren>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : stevenw
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

PPP adapter AT&T Global Network:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Physical Address. . . . . . . . . : 00-53-45-00-00-00
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 166.72.126.227
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 166.72.126.227
        DNS Servers . . . . . . . . . . . : 165.87.13.129
                                            165.87.201.244

C:\Documents and Settings\Steven S. Warren>
```

- **Ping**—Everyone should be familiar with the Ping command. It allows you to test network connectivity between a host system and another system using the IP address, NetBIOS name, or host name. The syntax is simply *ping [hostname, IP address, or NetBIOS name]*.
- **Tracert**—This utility goes a step further than Ping by allowing you to trace the hops between one system and a destination system (**Figure E**). It is helpful in determining where your connection is failing along the way to its destination. You invoke this tool using *tracert [domain name, hostname, IP address, or NetBIOS name]*.

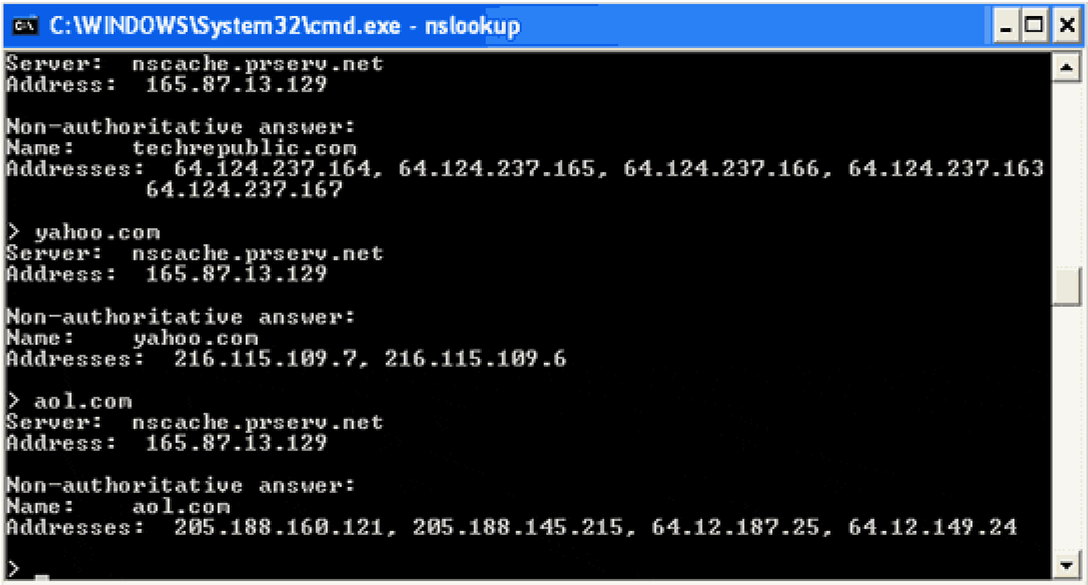
Figure E



```
Tracing route to www.techrepublic.com [64.124.237.166]
over a maximum of 30 hops:

  1   173 ms    179 ms    179 ms  32.97.115.126
  2   179 ms    170 ms    169 ms  12.125.30.9
  3   179 ms    179 ms    179 ms  gbr2-p53.ormfl.ip.att.net [12.123.200.225]
  4   179 ms    179 ms    179 ms  gbr4-p80.ormfl.ip.att.net [12.122.5.133]
  5   179 ms    179 ms    179 ms  gbr3-p20.attga.ip.att.net [12.122.2.181]
  6   190 ms    189 ms    179 ms  ggr1-p360.attga.ip.att.net [12.123.20.249]
  7   199 ms    189 ms    199 ms  att-gw.atl.above.net [192.205.32.182]
  8   200 ms    190 ms    198 ms  core2-core3-oc48.atl2.above.net [208.185.0.225]

  9   199 ms    199 ms    189 ms  dca2-atl2-oc48.dca2.above.net [208.184.232.49]
 10   257 ms    259 ms    259 ms  sjc2-dca2-oc48.sjc2.above.net [208.184.233.133]

 11   260 ms    259 ms    249 ms  sfo1-sjc2-oc48-2.sfo1.above.net [208.184.232.54]

 12   270 ms    269 ms    260 ms  main1colo78-core1-oc48.sfo1.above.net [208.184.2
28.2]
 13   259 ms    259 ms    259 ms  209.133.66.5.cnet.com [209.133.66.5]
 14   270 ms    259 ms    259 ms  abv-sfo1-tr-ww5.cnet.com [64.124.237.166]

Trace complete.

C:\Documents and Settings\Steven S. Warren>
```

- **Nslookup**—This utility allows you to gather valuable host, IP address, and domain information (**Figure F**). You can use this command by entering *nslookup [fully qualified domain name or IP address]* or by simply issuing the command *nslookup*, which will take you into interactive mode (with the > prompt). At that point, you can enter just the IP address or fully qualified domain name. Interactive mode is best to use when you're doing multiple lookups.

Figure F



```
Server:  nscache.prserv.net
Address:  165.87.13.129

Non-authoritative answer:
Name:    techrepublic.com
Addresses:  64.124.237.164, 64.124.237.165, 64.124.237.166, 64.124.237.163
          64.124.237.167

> yahoo.com
Server:  nscache.prserv.net
Address:  165.87.13.129

Non-authoritative answer:
Name:    yahoo.com
Addresses:  216.115.109.7, 216.115.109.6

> aol.com
Server:  nscache.prserv.net
Address:  165.87.13.129

Non-authoritative answer:
Name:    aol.com
Addresses:  205.188.160.121, 205.188.145.215, 64.12.187.25, 64.12.149.24

> _
```

In addition to the above command-line tools, the following tools may also be useful:

- **TcpView**—This utility is a free download that basically gives you the same information as Netstat but lets you view it graphically.
- **TDimon**—This utility gives you TCP and UDP activity in real time on the system that is being scanned (**Figure G**). You can download this tool here.

Figure G

Click to view image

- **Fport**—This little tool displays all TCP and UDP ports and maps them to their owning application. This tool can aid you in determining what ports to open or close on your firewall. You can download this tool by clicking here and then clicking Intrusion Detection, Fport, and Download Now.

Other tools

Network security scanner

After using some of the tools recommended above, you can add another level of protection to your network by downloading a security scanner. Scanners look for security holes and vulnerabilities and display the results. Two of my favorite security scanners include RealSecure Network Protection from Internet Security Systems and NetIQ Security Analyzer from WebTrends.

These products will cost you some money, but they can save a lot of the time it would take you to manually find the holes in your network. They also can often point out things you would probably miss otherwise. This especially includes some security best practices that are not technically flaws or vulnerabilities. Both of these products can act like an in-house security consultant.

Packet sniffer

A packet sniffer grabs packets off your network and allows you to analyze them at a basic level. Windows 2000 Server comes with a built-in sniffer called Network Monitor. You can install it from the Add/Remove Components applet in the Control Panel, if it is not already installed. After installation, you can use the analyzer to sniff packets on your network for any suspicious activity, such as DoS attacks and other hacker exploits.

Sam Spade

Another useful—and free—resource is the Sam Spade tool and Web site. This is probably one of the most robust and helpful sites on the Internet for gathering network information. You can either use the online version of Sam Spade or download a small Windows program that does the same things and more.

Sam Spade allows you to find out a ton of information about an IP address or FQDN. Let’s say, for example, that in one of my security logs I discovered an IP address that was repeatedly scanning my systems (most likely a hacker trying to find open ports and vulnerabilities). I could take this IP address and do a Whois query and/or a Dig query to find out more about where the attacker is coming from and try to take action against the person via his or her company or ISP.

Sam Spade includes a number of other useful tools. I recommend that you read the article "Sam Spade: The Swiss Army Knife of network analysis" and spend some time working with Sam Spade to get to know all of the features it offers.

Summary

Network security is obviously critical at this stage in the IT game. To be successful, you should have many tools at your disposal. The tools we've looked at here, combined with your security policy and firewall, will help you keep your network secure.

Visit us at www.TechRepublic.com