

Some Simple Free Network Scanners for Checking the Security of a Network

Robin Snyder

Savannah State University
126 Jordan, P. O. Box 20359
Savannah, GA 31404
(912) 356-2716
snyderr@savstate.edu
<http://www.RobinSnyder.com>

Abstract

The home/work/school network connected to the Internet has become ubiquitous. At the same time, security concerns have increased dramatically in recent years. This paper (and talk) will discuss (and present) some ways in which several freely available security scanners can be used to find weaknesses in a network, as well as to better understand how networks and security work hand-in-hand. Much of the material to be presented was recently used in an information security course.

Background

The ubiquitous computer is a machine that performs computations and, for convenience, stores data (i.e., that can be interpreted as information). In order to share resources, computers are connected together as parts of networks. Information is an important resource on a network, but only one of many possible resources that can be shared. But sharing usually needs to be limited, which is the purpose of security.

The ultimate in sharing is the Internet, a global communication network that is based on the TCP/IP suite of communication protocols. TCP (Transmission Control Protocol) runs on top of IP (Internet Protocol). Packets of data are sent between computers.

The typical tiered information systems model of a web-based system consists of the following layers.

- The presentation layer consists of the web browser using HTML that is formatted and displayed to the user.
- The business logic layer consists of a web server with some form of server-side processing, such as ASP (Active Server Pages), PHP (Personal Home Page) (or the recursive definition of PHP Hypertext Preprocessor), JSP (Java Server Pages), etc.
- The data access layer consists of a database management system such as SQL Server, Oracle, etc., sometimes with a connection to a mainframe database.

Every computer on the Internet needs a unique IP address. A computer can have more than one IP address (e.g., network IP, wireless IP, modem IP, etc.), but no IP address on the Internet should be used by more than one computer at any one time.

Each computer has 65,536 possible TCP/IP ports. Some of the most common are the following.

- TELNET on port 23 (remote login)
- HTTP on port 80 (web pages)
- SMTP on port 25 (outgoing email)
- FTP on port 21 (file transfer)
- HTTPS on port 443 (secure web pages)

Server software on a computer constantly monitors these ports (usually via an interrupt mechanism) to see if there is a client computer who wants to use the services of the server computer.

The Internet has become so popular that local networks, even if not connected to the Internet, are configured as small Internets, called Intranets. Thus, an intranet is an Internet-like TCP/IP network set up within a business or home that is often protected from the outside by security features like firewalls and routers.

Since the number of IP addresses is limited, various schemes have been developed to reuse IP addresses. DHCP (Dynamic Host Control Protocol) is often used to reuse IP addresses. NAT (Network Address Translation) is often used in conjunction with Intranets (i.e., a local Internet) and DHCP, to both isolate Intranets from Internets and reuse IP addresses.

The standard IP intranet addresses are as follows.

- 10.x.x.x (class A)
- 172.16.x.x (class B)
- 192.168.1.x (class C)

Firewalls

For home users connected to the Internet via high-speed Cable Modem or DSL (Digital Subscriber Line) phone access, security can be a problem as computers left on are always connected to the Internet, even when no one is using them who might otherwise notice if something unusually is happening, such as a hacker attack.

The common solution is that, between the presentation layer and the business logic layer, a firewall is placed that only allows certain TCP/IP messages to pass through the firewall. The Internet is outside the firewall while the local intranet (or just the one computer) is inside the firewall. Of course, there are more sophisticated configurations where more than one firewall is used, but that is beyond the scope of this discussion.

Typically, a hardware firewall protects well against outside threats such as network scanners outside the firewall while a software firewall protects against (new) programs running on the computer from getting out, or accepting outside requests, without permission.

A free, for individual noncommercial use, firewall software program that the author uses is ZoneAlarm available at <http://www.zonelabs.com>. You might have to look around for the free

version as most sites do not make it easy to find the free version; they hope you will go for the upgrade. Windows XP, SP2 (Service Pack 2), includes a built-in firewall. Such software will not only help protect your computer, it will make you more aware of what a firewall program does and how it does it. From Internet research, it appears that you should definitely not use both firewalls at the same time, and as of Spring 2005, the ZoneAlarm firewall was the better choice. Be aware that the XP firewall is turned on by default, so you will want to turn it off if you install another firewall.

Installation of a Cable/DSL router, such as one from LinkSys, at <http://www.linksys.com>, NetGear, at <http://www.netgear.com>, etc., typically provides NAT to isolate the internal home intranet from direct unsolicited access from the Internet. Most newer routers feature a hardware firewall, as well as other security features. However, if you connect the Internet from the intranet, the connected site can communicate back to the site that initiated the communication. Most companies and academic institutions use NAT to isolate the intranet from the Internet. In most cases, direct access to SQL Server is only allowed from within the firewall (i.e., on the intranet). Thus, users outside the firewall cannot directly access SQL Server. Instead, the firewall allows traffic on the `http:` port (port 80) and the `https:` port (port 443) to pass through the firewall in both directions. Often, some other ports (e.g., email) may also allow messages to pass.

Most hardware firewall routers provide an option to email security logs on a regular basis. Typically, logs are sent on each event, once a day, etc., as specified by the administrator. Here is a (typical) log from a NetGear firewall router. Notice that every few minutes there is a probe from some other computer.

```
Begin of Log -----
Sat, 09/27/2003 07:37:30 - TCP connection dropped -
  Source:81.52.249.113, 443, WAN -
  Destination:199.222.138.2, 3057,
  LAN - 'Suspicious TCP Data'
Sat, 09/27/2003 07:42:01 - TCP connection dropped -
  Source:161.114.19.93, 80, WAN -
  Destination:199.222.138.2, 3062,
  LAN - 'Suspicious TCP Data'
Sat, 09/27/2003 07:47:36 - TCP connection dropped -
  Source:207.68.178.238, 80, WAN -
  Destination:199.222.138.2, 17336,
  LAN - 'Possible Port Scan'
Sat, 09/27/2003 07:50:22 - TCP connection dropped -
  Source:199.77.203.33, 80, WAN -
  Destination:199.222.138.2, 17280,
  LAN - 'Possible Port Scan'
Sat, 09/27/2003 08:11:44 - UDP packet dropped -
  Source:165.166.15.70, 53, WAN -
  Destination:199.222.138.2, 60485,
  LAN - 'Suspicious UDP Data'
End of Log -----
```

Here are some of the IP source locations (some redundant ones were removed from the listing). The location of the computer/firewall was Rock Hill, SC.

- 81.52.249.113: Amsterdam, Netherlands
- 161.114.19.93: Palo Alto, CA (Hewlett-Packard)

- 207.68.178.238: Redmond, WA (Microsoft)
- 199.77.203.33: Broomfield, CO (Level 3 Communications)
- 165.166.15.70: Fort Mill, SC (Info Avenue Internet Services)

Some of these requests might be reasonable, from companies tracking computers, but other requests are probably from users running scanning software to look for certain things. A convenient place to find the (probable) location of an IP address can often be found from a web site such as <http://www.networksolutions.com> [as of Fri, Apr 29, 2005].

Network access

"Security is a process, not a product." [3, p. 84]. Security involves the human factor and is only as strong as the weakest link. A common example is the use of password protected resources. The strongest cryptography will not help if a user compromises their password.

So, who has access to your network? And, how would you know? From the above discussion, there are several ways an attacker can gain access to a network.

- An attacker can attack from outside the network (i.e., outside the firewall).
- An attacker can attack from inside the network (i.e., inside the firewall).

An attacker can use any publicly available Internet WHOIS utility to find out information about a given IP address. But what can the attacker see at that IP address? A firewall lets one monitor what comes into and out of the network.

An IDS (Intrusion Detection Service) can help determine when a computer has been accessed. The following are possible errors in the context of an intrusion detection system.

- A type I error is that an alarm is sounded, but there is no intrusion.
- A type II error is that no alarm is sounded, but there is an intrusion.

To determine what can be seen from a given point on the network, to help determine how well an IDS is working, and to learn more about your network in general, a port scanner can be used.

Port scanners

A port scanner scans a range of IP addresses in an attempt to gather information about the IP addresses in that range. Keep in mind that hackers use port scanners from outside the network. Most firewalls and IDS's can either minimize or prohibit this problem. This is often done with NAT filtering, closing ports, etc.

However, many security problems come from within the network. This means that uncooperating users on the network might be scanning the network. Or, it means that cooperating users on the network might have inadvertently downloaded and/or installed malicious software (e.g., from the Internet) that might scan the network and report back the results to a site outside of the network. Remember that it is usually easier to move information from within the firewall to outside of the

firewall (and network) than it is to get information (e.g., code) from outside of the firewall to inside the firewall. Unless, of course, uncooperating or cooperating users assist in the process.

A port scanner will attempt to contact computers at various IP addresses. These IP addresses can be specified or selected at random. For each IP address selected, the ports to check can be specified or selected at random.

A common process called footprinting or fingerprinting is used to determine which server software might be running on a computer at a given IP address. Most server software uses standard ports. For example, SQL Server, by default, uses port 1433. Each server uses a pre-determined protocol at each port. For publicly available server software, this protocol is known. Port scanners will check such known ports in an attempt to what server software is running at which ports.

Once server software is identified running at a given port, the version and type of that software is determined. Once the version and type of that software is determined, an attempt can be made to exploit the known bugs for that server software.

On occasion, a trap will be set for hackers. The trap is called a honey pot. A honey pot will attempt to look like server software that is operating on a given port on a given machine at a given IP address, but in reality sets off a silent alarm when a hacker (or port scanner) attempts to access it. The legal implications can be compared to setting a trap for an intruder in that the intruder may claim liability for injury if the trap injures the intruder. Such legal implications are beyond the scope of the current discussion.

Some free port scanners are now discussed. As a minimum, the discussion should show how easy it is to acquire and use port scanners, for friends and foes alike. Remember that such port scanning functionality can be built into hacker software that is downloaded and run, with or without the users' knowledge.

WinPcap, at <http://winpcap.polito.it/> [as of Thu, Oct 14, 2004], is a free packet capture architecture for Windows. It is required for many of the free scanners to run properly. It appears to have been intentionally broke by Microsoft in the SP2 upgrade to Windows XP, but a work-around has since been done.

Raw Logic Software

Raw Logic Software has several products in the network security area. One of these products is NetBrute, which is free. The NetBrute scanner includes NetBrute, PortScan, and WebBrute. The download and installation is straightforward. Once installed and started, the easiest way to start using NetBrute is to use the "**NetBrute**" tab.

NetBrute allows you to scan a single computer or multiple IP addresses for available Windows File & Print Sharing resources. This is probably one of the most dangerous and easily exploitable security holes. It is common for your novice users to have their printers or their entire hard drive shared without being aware of it. This utility will help you to

find these resources, so you can secure them with a firewall or by informing your users how to properly configure their shares with tighter security.

<http://www.rawlogic.com/products.html> [as of Sun, Sep 05, 2004]

Here is how to start using this part of NetBrute.

- Select "**Get IP**" to get the IP of the computer NetBrute is being run from.
- Select the up arrow to set the "**Range**" parameters to this computer.
- Select "**Scan**" to scan this computer.

By default, the NetBrute port scan will be done on port 139 which is the netbios-ssn port, which is used for Windows file and print sharing. The results might appear as follows (check the box for "**Report View**" to get the text for the report).

```
192.168.0.201
E$:Default share
D$:Default share
D:
XPM:
F$:Default share
E:
ADMIN$:Remote Admin
C$:Default share
```

Note the intranet IP address. Note also the use of naming shares with the suffix of the dollar sign "\$". This makes it harder to see those shares from the network (i.e., you, or the software, would have to guess the name of the share which may not be easy). Of course, they can be easily seen when running NetBrute from the computer on which they reside.

To extend the search, modify the upper and lower IP "**Range**" settings and select "**Scan**". For example, the above instructions would set the upper and lower settings to 201. To expand the settings set the lower setting to 1 and the upper setting to 254 (note that 0, all zeros, and 255, all ones, are reserved and can be included or excluded from the scan).

The larger the search area, the longer the search will take. Unless the scan is randomized both in time and space, the scan should be easily detected by most IDS's. More sophisticated scanners (i.e., those used by hackers) would be more versatile in their scanning.

To scan ports in general (i.e., more than just port 139), select the "**PortScan**" tab.

PortScan allows you to scan a single computer or multiple IP addresses for available Internet services. This will allow you to identify which TCP ports need to be blocked by your firewall, if you wish to secure them. Or it will allow you to identify unused services that are running, so they can be stopped <http://www.rawlogic.com/products.html> [as of Sun, Sep 05, 2004]

The same methods can be used, but additional ports can be scanned. An interesting exercise is to run PortScan on your own computer and then identify every port being used and what is being done on that port. For example, the following ports were identified when scanning self-scanning.

```
192.168.0.201
192.168.0.201 #7
192.168.0.201 #9
192.168.0.201 #80
192.168.0.201 #1032
192.168.0.201 #2107
192.168.0.201 #2869
```

Port 80 is the web port. Port 7 is the echo port. Port 9 is the discard port. A web search did not reveal the true purpose some of the other ports. An Internet search for "**tcp ports**" revealed the following at <http://www.iana.org/assignments/port-numbers> [as of Fri, Mar 18, 2005].

Abbreviation	Port	Information
echo	7	Echo
discard	9	Discard
http	80	Word Wide Web HTTP
iad3	1032	BBN
bintec-admin	2107	BinTec Admin
icslap	2869	ICSLAP

If you are running a web server on a computer where users can create and maintain web sites, the WebBrute part of NetBrute will attempt to guess user passwords. This option can put a load on the web server, but can be useful in certain circumstances (i.e., those listed above).

Nmap and NWinMap

Nmap, for "**Network Mapper**", from <http://www.insecure.org/nmap/> [as of Wed, Sep 08, 2004], is a free open source utility for network exploration and/or security auditing. There is a wealth of useful information at this web site.

Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL.
<http://www.insecure.org/nmap/> [as of Wed, Sep 08, 2004]

Nmap runs primarily only under UNIX systems such as Linux. A port of Nmap for Windows is called NMap (command line) and NMapWin (GUI).

NMap runs from the command line, which is useful for automation purposes. NMapWin runs using a GUI (Graphical User Interface), which is convenient for interactive use. Note that during Spring 2005, NMapWin was considered out-of-date from the updated NMap. After starting NMapWin, select "**Help**" to get more information on using NMapWin.

NMapWin allows the selection of options to NMap in a graphical way. When a **"Scan"** is done, the command line is displayed at the bottom left under **"CMD:"**. The output of the command is shown in the **"Output"** window.

If the `nmap` command is taking too long to complete, and you wish to stop before it is done, select **"Stop"**. Here are some examples. They are just examples, and will not necessarily work on your network. For example, you will have to adjust the IP range for your network.

I selected a scan of **"Host:"** IP 192.168.0.201. Under the **"Scan"** tab, I selected a **"Mode"** of **"List Scan"**. I selected **"Scan"**. Here is the command line under **"CMD:"**.

```
CMD: nmap -sL -PT -PI -O -T 3 192.168.0.201
```

Here is the output from the **"Output"** window.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host ACER2000 (192.168.0.201) not scanned
Nmap run completed -- 1 IP address (0 hosts up) scanned in 0 seconds
```

The output tells me that there is a computer at IP address 192.168.0.201 called ACER2000.

To copy the output to the clipboard as text, right-click on the **"Output"** area and select **"Select All"**, then right-click on the **"Output"** area and select **"Copy"**.

Selecting a **"Host:"** IP of 192.168.0.* resulted in the same information, but took 90 seconds. In the above output, I knew that the only other computer on the network was at 192.168.0.201, which took 2 seconds.

On the **"Win32"** tab, select **"List Interfaces"**. Here is the command line.

```
CMD: nmap --win_list_interfaces
```

Here is the output.

```
Available interfaces:
Name      Raw send  Raw receive  IP
loopback0 none      none         127.0.0.1
eth0      none      none         0.0.0.0
eth1      winpcap  winpcap     0.0.0.0
eth2      winpcap  winpcap     192.168.0.200
```

On the **"Scan"** tab, I selected **"SYN Stealth"**, **"Scan"**. Here is the command.

```
CMD: nmap -sS -PT -PI -O -T 3 192.168.0.201
```

Here is the output.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on ACER2000 (192.168.0.201):
(The 1584 ports scanned but not shown below are in state: closed)
Port      State      Service
```

```
21/tcp    open     ftp
25/tcp    open     smtp
80/tcp    open     http
119/tcp   open     nntp
135/tcp   open     loc-srv
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
563/tcp   open     snews
1025/tcp  open     NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1030/tcp  open     iadl
1033/tcp  open     netinfo
1433/tcp  open     ms-sql-s
3372/tcp  open     msdtc
6667/tcp  open     irc
6668/tcp  open     irc
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or
WinXP
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

Here is the "**Scan**" for "**FIN Stealth**". Here is the command.

```
CMD: nmap -sF -PT -PI -O -T 3 192.168.0.201
```

Here is the output.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1601 scanned ports on ACER2000 (192.168.0.201) are: closed
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
```

Here is the "**Scan**" for "**IP Scan**". Here is the command.

```
CMD: nmap -sO -PT -PI -O -T 3 192.168.0.201
```

Here is the output.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning: OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Interesting protocols on ACER2000 (192.168.0.201):
(The 250 protocols scanned but not shown below are in state: closed)
Protocol  State      Name
1         open      icmp
2         open      igmp
6         open      tcp
17        open      udp
47        open      gre
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 10 seconds
```

Languard

The Languard Network Scanner, at <http://www.gfi.com/languard/> [as of Tue, Sep 14, 2004], is another free scanner that can be used for network enumeration purposes.

Summary

This paper has discussed various security aspects of port scanners, and some freely available port scanners.

References

- [1] Klevinsky, T., Saliberte, S., & Gupta, A. (2002). Hack I.T.: security through penetration testing. Boston: Addison-Wesley.
- [2] Scambray, J., McClure, S., & Kurtz, G. (2001). Hacking exposed: network security secrets and solutions, 2nd ed. Berkeley, CA: Osborne/McGraw-Hill.
- [3] Schneier, B. (2000). Secrets & lies: digital security in a networked world. New York: John Wiley & Sons, Inc.
- [4] Snyder, R. (1994). Proactive approaches to information systems and computer security. Proceedings of the 27th Annual Conference of the Association of Small Computer Users in Education. Myrtle Beach, SC.
- [5] Snyder, R. (2001). Computer and information security considerations for installing and running Microsoft Internet Information Server and Microsoft SQL Server. Proceedings of the 34th Annual Conference of the Association of Small Computer Users in Education. Myrtle Beach, SC.
- [6] Whitman, M., & Shackleford, D. (2003) Hands-On Information Security Lab Manual. Thompson Publishing.