CT1406 Network Security Lab
Lab7

Port Number	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384-32,767	UDP	RTP-based Voice and Video

Learning Objectives:

After completing this lab, you will be able to

- Use Nmap to scan a network for hosts that are up.
- Use Nmap to enumerate the ports and services available on a host.
- Identify the qualities of the Nmap ping sweep signature.
- Explain the different methods Nmap uses to enumerate the ports normally and stealthily.
- Determine and interpret service information from banners obtained via Telnet.

Lab 7: Using Nmap in Windows

Materials and Setup

You will need the following:

- Windows 7
- Windows 2008 Server

In addition you will need

- Wireshark https://www.wireshark.org/download.html
- Nmap https://nmap.org/download.html
  (Both installed in Windows 7)

Lab Steps at a Glance

Step 1: Start the Windows 2008 Server and Windows 7 machines. Only log on to the 7, machine.
Step 2: Start Wireshark.
Step 3: Use Nmap to scan the network.
Step 4: Analyze the output from Wireshark.
Step 5: Use Nmap to scan open TCP ports.
Step 6: Use Wireshark to analyze the scan.

CT1406 Network Security Lab
Lab7

Step 7: Use Nmap to do a stealth scan on the computer.
Step 8: Use Wireshark to analyze the scan.
Step 9: Log off from the Windows 7 PC and windows server 2008.

Lab Steps

Step 1: Start the Windows 2008 Server and Windows 7 machines. Only log on to the Windows 7 machine.

Step 2: Start Wireshark.
You are going to launch Wireshark to capture Nmap-generated network traffic and analyze how it discovers active hosts.
1. On the Windows 7 desktop, double-click Wireshark.
2. On the Wireshark, double click on Local Area Connection adapter to start the live capture.

Step 3: Use Nmap to scan the network.
1. Choose Start | Run.
2. In the Open field, type **cmd** and click OK.
3. At the command line, type **nmap –sP 10.170.26.*** and press enter, as shown in Figure 4-1.
The –sP option tells Nmap to perform a ping scan. The * at the end of the address means to scan for every host address on the 10.170.26 network. The scan should take about 20 to 30 seconds.

- **a.** Observe the output.
- **b.** How many hosts did Nmap find?
- **c.** What is the IP address of the host?
- **d.** How long did the scan take?

Step 4: Analyze the output from Wireshark.
1. Click on the Wireshark Capture screen and click Stop. See Figure 4-2.
2. Identify the qualities of the ping sweep signature.

- **a.** Observe the output.
- **b.** Why are there so many ARP broadcasts?
- **c.** What can you tell about the timing between broadcasts?

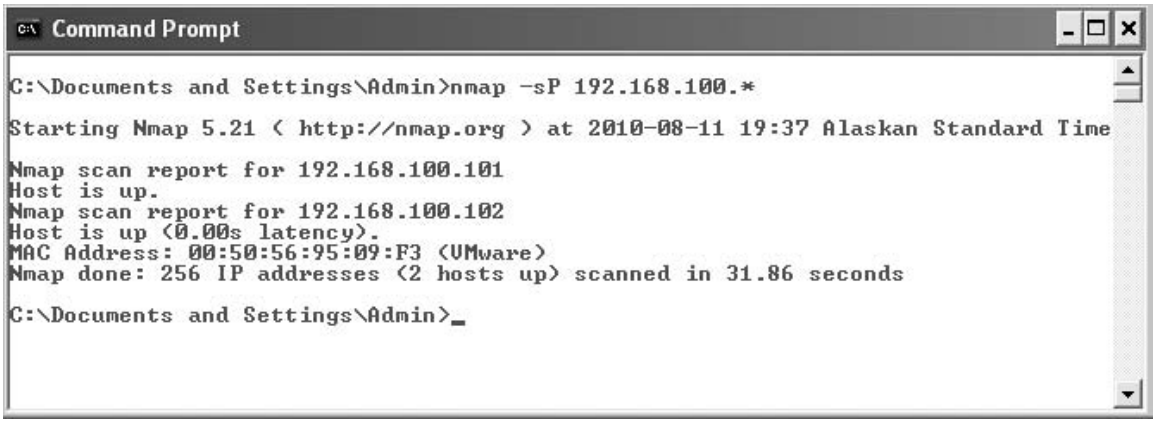

Figure 4-1 Using Nmap to perform a scan of the network

CT1406 Network Security Lab
Lab7

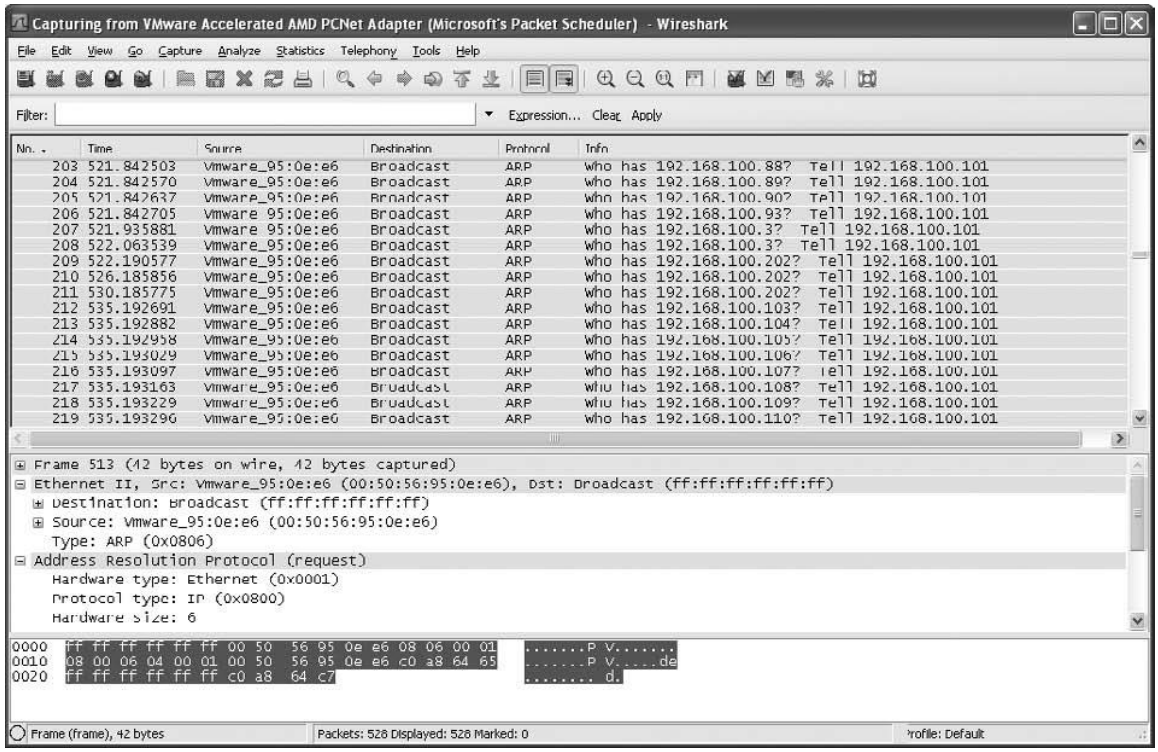

Figure 4-2 Traffic generated by Nmap scan

d. What do you notice about the source addresses?
e. What do you notice about the broadcast addresses?

3. On the Wireshark menu, choose Capture | Start, click Continue without Saving.

Step 5: Use Nmap to scan open TCP ports.

1. At the command line, type **nmap –sT 10.170.26.161** and press enter.

The –sT option tells Nmap to perform a TCP port scan. This is a full connection scan. The scan should take about eight to ten minutes.

a. Observe the output.
b. How many ports did it find?
c. How long did the scan take?

Step 6: Use Wireshark to analyze the scan.

1. Click on the Wireshark Capture screen and click Stop.

a. Observe the output.
b. How many packets did Wireshark capture?

Look at the signature of the scan. Notice that there are many SYN packets sent from 10.170.26.101 (the computer doing the scanning) and many RST/ACK packets being sent back. RST/ACK is the response for a request to connect to a port that is not open.

CT1406 Network Security Lab
Lab7

Look at what happens when an open port is discovered. If you look at the output from the Nmap scan, you know that port 80, the HTTP service port, is open. To find those particular packets out of the thousands of packets captured, you will need to filter out the unwanted traffic.

2. In the Filter box, type **tcp.port==80** and press enter. (Note: There should be no spaces between any of the characters typed in the Filter box.)

Look at the last four packets captured. Note the SYN, SYN/ACK, and ACK packets. A three-way handshake was completed so that the port could be established as open. This is okay, but it is very noisy and can show up in the server logs. The last of the four packets is an RST sent by the scanning computer.

3. Click Clear to the right of the Filter box.

4. On the Wireshark menu, choose Capture | Start

5. In the Save Capture File Before Starting a New Capture? Dialog box, click Continue without Saving.

Step 7: Use Nmap to do a stealth scan on the computer.

1. At the command line, type **nmap –sS 10.170.26.161** and press enter.

The **–**sS option tells Nmap to perform a TCP SYN stealth port scan. Since this type of scan requires Nmap to behave on the network in an atypical manner, you must have administrative rights. The scan should take about one second.

a. Observe the output.

b. How many ports did it find? Compare this to the number of ports found with a TCP scan.

c. How long did the scan take? Compare this to the amount of time it took with the TCP scan.

Step 8: Use Wireshark to analyze the scan.

1. Click on the Wireshark Capture screen and click Stop.

a. Observe the output.

b. How many total packets were captured? How does this compare to the previous capture?

2. In the Filter box, type **tcp.port==80** and press enter. (Note: There should be no spaces between the characters.)

Look at the last three packets. Note that this time the three-way handshake is not completed. The SYN packet is sent and the SYN/ACK is returned, but instead of sending back an ACK, the scanning computer sends an RST. This will allow the scanning computer to establish that the port is in fact opened, but is less likely to be registered in the logs.

3. Close Wireshark and do not save the results.