**CPS3498 Computers Security**

**Lab 4: Port Scanning and System Vulnerability**

**Description:**

Scanning a network to discover what computer systems are attached and operating is a useful task for both a system administrator and an intruder. The information gained from a network scan assists in the determination of the actual layout. Once the devices and their open ports have been identified, a vulnerability scanner can be used, with its database of vulnerabilities, to test if the system has any of them. These vulnerabilities are further researched online.

Nmap is a popular scanning utility. It is a powerful tool that can quickly and easily gather information about a network’s hosts, including their availability, their IP addresses, and their names. Nmap can also identify the operating system that is running on the host by using stack fingerprinting, based on the fact that different operating systems implement TCP/IP in slightly different ways.

Some vulnerabilities are known to public and can be researched on the Internet. There are web sites that list not only vulnerabilities, but also exploits, the methods with which those vulnerabilities can be exploited. One such source of information is the Common Vulnerabilities and Exposures (CVE) database. The CVE database is maintained by MITRE Corporation.

This lab uses tools Nmap to scan a network for enumerating the ports and services available on a host. Then you will research on system vulnerabilities of Microsoft Windows.

**Procedure:**

**Lab 4.1 IP Address and Port Scanning, Service Identity Determination**

1. Long on to a Windows PC with the administrator account, or an account that has administrator privilege.
2. Go to <http://nmap.org/download.html>. Download Nmap and install it on your computer. This should install both Nmap and Zenmap GUI applications. If you use other Operating System, such as Mac OS, you may need to compile the binary code by following the instructions listed on the web page to install Nmap.
3. Start Wireshark. Start capturing data by clicking on “Interface List” on the startup screen. In the Capture Interface dialog box, click on Start to start capturing data.
4. Start command prompt. At the command prompt, type **ipconfig** to find the IP address (Ref. Lab1 for details) assigned to your computer and your default gateway.
5. Start Nmap and you should see Zenmap GUI appears. As shown in Figure4-1, there are 5 sections on the Zenmap’s scan output screen.
   1. Nmap Output: Located on the left, this section displays a summary of scan report.
   2. Ports/Hosts: Located in the left middle, this section displays the ports and services on the hosts.
   3. Topology: Located in the middle, this section shows the network topology.
   4. Host Details: Located in the right middle, this section shows host status and addresses.
   5. Scans: Located on the right, this section displays a list of all commands that have been executed.

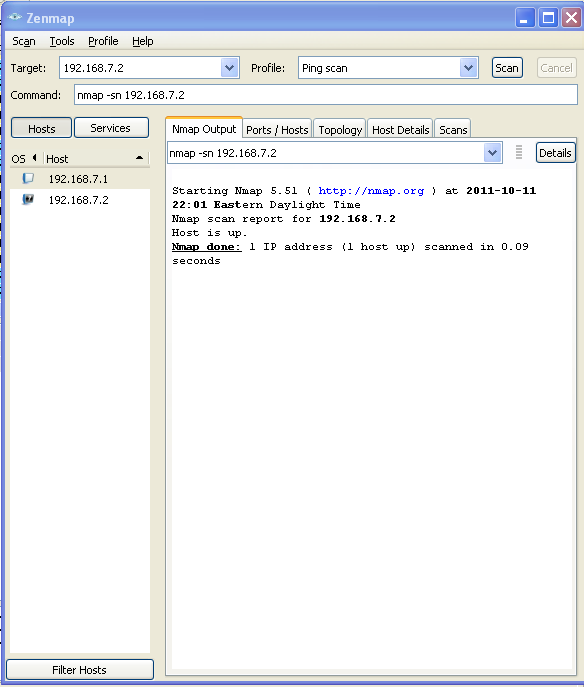


Figure 4-1

1. On the Zenmap, Enter your [IPv4 address] into Target field and select “ping scan” from profile. The command line should look like “nmap –sn 192.168.7.2” in Figure 4-1. Observe the outputs by clicking on each host. Observe the output on Wireshark, too.
2. On the Zenmap, replace the last octet of the IP address in the target to \* (e.g., 192.168.7.1 to 192.168.7.\*). The \* at the last octet of the address means to scan every host address on the 192.168.7 network. This scan could take a few seconds. Observe the output from both WIreshark and Zenmap.
   1. How many hosts did Nmap find?
   2. What are the IP addresses of the hosts?
   3. How long did the scan take?
3. Click on the Wireshark Capture screen and click Stop. Identify the qualities of the ping sweep signature by observing the output
   1. Why are there so many ARP broadcasts?
   2. What can you tell about the timing between broadcasts?
   3. What do you notice about the source addresses?
   4. What do you notice about the broadcast addresses?
4. Click on the Wireshark Capture screen and click Start. Click on Continue without Saving. On Zenmap, At the Command line, type nmap –sT [IPv4 address of the gateway] and click on Scan. The –sT option tells Nmap to perform a TCP port scan. This is a full connection scan which may take a few minutes to scan all 65536 ports. Observe the output:
   1. How many ports did it find?
   2. How long did the scan take?
5. Click on the Wireshark Capture screen and click Stop. Observe the output. How many packets did Wireshark capture?

Look at the signature of the scan and notice that there are many SYN packets sent from your [IPv4] address 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. The last four

1. 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 on the Wireshark, you will need to filter out the unwanted traffic. In the Filter box, type **tcp.port==80** and press Enter.

Look at the SYN, SYN/ACK, and ACK packets captured. A three-way handshake was completed so that the post could be established as open. The last packet is and RST sent by the scanning computer.

1. Click Clear to the right of the Filter box on the Wireshark. Click on the Wireshark Capture screen and click Start. Click on Continue without Saving.
2. On Zenmap, At the Command line, type nmap –sS [IPv4 address of the gateway] and click on Scan. The –sS option tells Nmap to perform a TCP SYN stealth port scan. You must have administrative rights to perform such scan. Observe the output.
   1. How many ports did it find? Compare this value to the one found with a TCP scan.
   2. How long did the scan take? Compare this value to the one found with a TCP scan.
3. Click on the Wireshark Capture screen and click Stop. Observe the output. How many packets did Wireshark capture?
4. In the Filter box, type **tcp.port==80** and press Enter. Notice the three-way handshake is not completed. The SYN packet is sent and the SYN/ACK is returned, but instead of sending ack an ACK, the scanning computer sends an RST.
5. On Zenmap, At the Command line, type nmap –O [IPv4 address of the gateway] and click on Scan. The –O option tells Nmap to perform a scan and guess what operating system is on the computer. Observe the output. Notice the OS details. What is the guess made by Nmap?

**Lab 4.2 Researching System Vulnerabilities**

1. Open a web browser and enter the URL [www.google.com/](http://www.google.com/). In the Google search box, type either **windows 2008 server r2 vulnerabilities** or **windows 2012 server vulnerabilities**.
   1. How many hits did your search result in?
   2. What were the domain names of the top five hits (such as Microsoft.com, Mitre.org etc)?
   3. Did your search turn up a specific vulnerability? If so, which one? What does this vulnerability allow an attacker to do?
2. The vulnerability reporting community uses a single identifier for each vulnerability to ensure commonality when working on the vulnerability. The single identifier is called a CVE (Common vulnerability and Exposures) Identifier. Enter [www.cve.mitre.org](http://www.cve.mitre.org) in the URL box.
3. On the web page, click on the Search NVD link on the left panel. In the Keyword Search box, type Microsoft Windows 2008 (2012) Server and click Search All. How many vulnerabilities did it return?
4. Take a specific vulnerability and search for the MS bulletin you discovered in the Google search.
5. Click the back button in your browser, enter **MS13-081** in the keyword search box, and click on search All. Click on the CVE-2013-3894 link at the top of the search results.
6. What is the Impact Subscore?
7. What is the Exploitability Subscore?
8. Read the information regarding the vulnerability.
9. Enter [www.metasploit.com/modules/](http://www.metasploit.com/modules/) into the URL box. Type the above CVE identifier or the MS Bulletin in the appropriate box and click Search Modules.
   1. Does an exploit for the vulnerability exist in the metasploit Framework?
   2. If so, what is the rank?
10. Microsoft provides a tool, Microsoft Baseline Security Analyzer (MBSA), to scan Windows system for security vulnerability. Enter http://www.microsoft.com/en-us/download/details.aspx?id=7558 into the URL box, download and install the tool. Record any vulnerability existing in your system?

**Notes and Suggestions:**

* Different computers may have different operating systems and hardware configurations. If you use your own computer for this lab, the above procedure may not be completely applicable. For example, you cannot follow the same procedure for MAC computer.
* Make sure that the computer is back to its original condition. Do not leave a computer in a non-functioning condition.

**Lab report:**

* Your report should include all information required to be noted in the procedure, any problems/issues you encountered during the lab and how did you resolve them.