Lab 3: Scanning and nmap

Preliminaries

Refer to Lecture slides in Week 3.

Tasks

Turn on all three VMs. Log into your Kali VM, and start a terminal. Then, complete the following tasks. Note that you should always run nmap on Kali, and add ‘sudo’ before ‘nmap’.

Write your answers for all questions to your lab report.

1. Nmap host discovery.
   - 1.1 Use 'ip a' command to determine the block of IP addresses used by the virtual local network where you run Kali. Write your answer into the lab report. Your answer should be in the form of <subnet address>/<#mask-bits>, e.g., 192.168.221.0/24.
   - 1.2 Use nmap with appropriate options to discover which hosts are alive on this local network without scanning ports on these hosts.
     - a) What is your command line used?
     - b) Include the list of discovered active hosts into your lab report.

     Hint: consider the '-sn' option and how to specify a range of IP addresses from our slides.
   - 1.3 Find out the IP addresses of the gateway, the Kali VM, the Win7 VM and the Metasploitable2 VM as you did in Lab 1.
     - a) Write each machine and its IP address into your lab report.
     - b) Check whether these IP addresses appear in the active hosts list above. Simply answer yes or no in your lab report.
   - 1.4 Start Wireshark to capture all traffic on the network. Then, run the command line for task 1.2 again. Observe the Wireshark capture. Based on the observation, explain in your report how nmap discovers active hosts in a local network.

2. Nmap port scanning.
   - 2.1 Use nmap to detect whether the top 200 TCP ports on the Win7 VM are open. Write your command line and the scan results into your lab report.
   - 2.2 Start Wireshark to capture all traffic on the network. Then, use nmap with proper arguments to only detect whether the TCP port 80 on the Metasploitable2 VM is open (Hint: see how to specify ports in our slides).
     - a) Write your command line into the lab report.
     - b) Observe the Wireshark capture. Based on the observation, explain in your report how nmap determines whether a port is open or not.

3. Nmap service detection.
   3.1 Use nmap with proper arguments to detect services possibly provided by the top 200 TCP ports on the Win7 VM.
      a) Write your command line and the scan results into your lab report.
      b) Compare the output with the one from Task 2.1. What are the differences?

   3.2 Use nmap with proper arguments to detect services possibly provided by the top 50 TCP ports on Metasploitable2 VM and skip host discovery as you already know that it is running. Write your command line and the scan results into your lab report.

   3.3 Use nmap with proper arguments to detect service on UDP port 53 on the gateway. (Hint: see service detection part in our slides). Write your command line and the scan results into your lab report.

4. Nmap OS detection.
   4.1 Use nmap with proper arguments to detect OS on the Metasploitable2 VM.
      a) Write your command line into your lab report.
      b) What OS does nmap thinks the Metasploitable2 VM is running?
      c) If it is Linux, what is the kernel version number believed by nmap?

   4.2 Use nmap with proper arguments to detect OS on the Win7 VM.
      a) Write your command line into your lab report.
      b) What OS does nmap thinks the Win7 VM is running?
      c) If it is Win7, can nmap be sure that it is Win7 SP1?

   4.3 Use nmap with proper arguments to detect OS on the gateway (which is your virtual NAT box).
      a) Write your command line into your lab report.
      b) What OS does nmap think the gateway device is running?

5. Nmap output formats.
   5.1 Make sure you are currently in the directory of "/home/kali".
      a) Create a new directory under it called "outputs" using command "mkdir". If you are unsure how to use "mkdir", do "man mkdir".
      b) Execute "cd outputs". Then, Execute "pwd". What's the result of this command?

   5.2 Use nmap with proper arguments to detect whether the TCP ports in the range of 8001-8010 on Metasploitable2 VM are open, and output in all three formats of Normal, XML, and Greppable to files. The output file names without the suffix part should use "ports8001-8010". Write your command line for achieving the above into your lab report.

   5.3 Execute ‘ls’ command. What are the full file names of the three output files from Task 5.2?

   5.4 Use a text editor of your choice to examine the contents of the XML output file, which is convenient for exporting nmap output to other programs. An XML file typically includes a hierarchy of tags. For example, you'll notice that the <scaninfo> tag is nested directly inside the <nmaprun> tag in XML output file. Similarly, which tag is the <port> tag nested inside directly?

6. An exercise on ‘grep’. Use the Firefox from Kali VM to visit the vUWS site of this unit. Download the Lab3-Supplement-treasure.zip accompanying this lab and save it in the “Downloads” directory under “/home/kali”.
   6.1 Decompress this file using the ‘unzip’ command. Write your command line into the lab report. (If you are unsure how to use ‘unzip’, do a ‘man unzip’.)
   6.2 After decompressing, you should see a directory called “treasure”. Under this directory, you see many further directories and files. Only one of these files contains a line with the following string “Secret:OpenSeseme”. Use ‘grep’ to find out which file it is. (Suppose you are now under the directory “/home/kali/Downloads/treasure”). Write your command line and result into the lab report, and attach a screenshot as proof.
   Hint: Study a good tutorial on 'grep', and focus on the ‘-r’ option.

Last but very important: First shutdown and then power off all your three VMs. Our school's cloud is under heavy load, as you can see your VMs may not respond to you quickly. Therefore, if you are not using them, you should have them shutdown and power off.