**Capt Alamri, 2Lt Hayden, 2Lt Mireles**

**Lab 2 – Scanning**

**Dr. Mullins**

**1/16/2019**

**Network Mapping**:

1. What is the IP address and host name of your machine? What is the IP address and host name of your partner’s machine?

* My IP address is

1. Using ping, determine if your partner’s workstation is up. Is your partner’s workstation up?
2. Using tracert, determine the number of hops between your two machines. How many hops are there between the two computers?
3. Perform a network sweep using arp-scan to identify potential targets/IPs quickly. What type of packet is the tool sending? Provide a Wireshark screenshot showing some of the captured packets. How many IPs did the tool discover? Did the tool scan sequentially? What are does the third column represent, and how is that information learned? [You are not required to show all devices found in the screenshot. You may just include a screenshot of the command used along with the first five machines found followed by a screenshot displaying the summary provided by the command (i.e., XXX packets received by… YYY responded).]

**Nmap**

1. Blackhat: Start Wireshark and perform a SYN scan using nmap or zenmap. Use aggressive timing and turn on verbose output. You may add other options as needed to provide the following information about the target. Using just 2 the nmap results, answer the following questions; in other words, you cannot ask your partner for the name of his/her machine.
   1. What nmap command did you use? Describe all options used and how they affect the scan.
   2. Which ports are open? Provide a screenshot.
   3. What services are being offered? Spell out all acronyms.
   4. What is the MAC address?
   5. What is the operating system?
   6. What is the hostname of the target (e.g., LISXP33LG)?
   7. Look at the Wireshark data. During the scans, what type of packets did your workstation send to the target (i.e., which flags are set in the packets)?
   8. Select a port listed as open by nmap. How did the target respond for the open port? How did the Blackhat computer respond to the target’s response? Provide a screenshot of your filtered results. Useful filter: **tcp.port == <port #>**
   9. Select a port listed as closed by nmap. How did the target respond for the closed port? Provide a screenshot of your filtered results.
   10. Were the ports scanned sequentially?
2. Now try nmap’s decoy feature.  
   Blackhat: Start Wireshark and run a SYN scan against ports 1-500 with decoy addresses of **2.2.2.2, 3.3.3.3, <<your real IP>>, 4.4.4.4**. Note there is no space between those addresses, just a comma. Also set your source port number to 999.
   1. Provide a screenshot of the Wireshark screen demonstrating the decoy and real IP addresses along with the 999 port number.
   2. Describe how the use of decoys is different than nmap’s idle scanning.
   3. Inspect the Wireshark output of your decoy scan. Describe when and how many decoys are sent per real packet.
3. Scan the IP addresses 10.1.0.1 through 10.1.0.20 looking just for FTP, SSH, or web servers. In the interest of time, I suggest running a simple SYN scan using aggressive timing without OS or version detection. Provide a screenshot showing the topology map generated by nmap. Ensure the text is readable. You may want to uncheck the hostname option in the controls panel to remove the clutter; displaying just IP addresses is fine.

**Shares**

Both team members perform the following, but only provide answers from one member. Provide a screenshot of your results.

Using a command shell, answer the following:

1. List all (including hidden) shares offered on your local machine.