CSC436 Lab 03

Take only the screenshots of your work as indicated below and save them to a single Word or PDF document.

All scans performed for this lab should be of the **10.10.30.0/24 subnet**

Nmap

1. For all of the commands below, you need to save the output (**-oA** in nmap) with a filename that is **first initial + last name_scanType** (e.g. **cwelu_syn**).

2. Use the proper nmap switch to determine which IP / hosts are alive on your network.

   HINT: be sure to scan the entire /24 network. This scan should **<u>only</u>** do host discovery, not a port scan as well. Provide a single screenshot showing your command and the output.

3. After locating the Metasploitable target in the previous step, conduct a full scan of all ports on the system (65,535). Provide a screenshot showing your command and output.

4. Utilize the appropriate nmap command to launch a TCP Connect scan. The scan needs to determine the operating system and the detailed service version information for each of the ports open on the target. Provide a screenshot showing your command and output.

5. Use nmap to run a scan that violates the TCP protocol. Provide a screenshot showing your command and output.

6. How could you find systems that do not respond to ICMP ping? Perform that scan or scans to find additional host(s).

7. If you feel you need to, complete any additional scans to learn what you need from the network.

8. Compile your findings into a brief report. What systems did you find? What do you know about those systems?