Cyber Operations

Unit 06 – Advanced Scanning

# Lab 04 Nmap

You will need your Kali VM or a desktop that can run the tools shown below (nmap). You will also need a Metasploitable virtual machine to scan. Be extremely careful in running these scans, it is your responsibility to remain passive and to only access systems you are authorized to do so.

### **Save the output**

For each of the nmap commands below, you will need to save the output using the -oA flag, with a filename that includes your first initial, last name, and the scan type.

### **Host Discovery**

Use the proper nmap switch to determine which IP / hosts are alive on your network. Take a screenshot of the output.

### **Full Port Scan**

After locating the Metasploitable target in the previous step, conduct a full scan of all the ports on the target system and take a screenshot of the output. Be sure to include TCP and UDP results.

### **TCP Connect Scan**

Using the proper nmap command, launch a TCP Connect scan against the target. This scan also needs to determine the operating system and the detailed service version information for each of the ports open on the system. Take a screenshot of the output.

### **Violate the TCP Protocol**

Run an NMAP scan that violates the TCP protocol. Take a screenshot of the output. Examples of scans that violate the TCP protocol include FIN, Xmas tree, Null, Ack, etc.

### **Choose your own port scanner**

Run a different port scanner against the Metasploitable machine and take a screenshot of the output. This will give you an opportunity to take a look at and evaluate other tools and utilities.

## What to submit

Create a PDF document containing the screenshots required in the lab. The document should include your name and only the screenshots requested.