Cyber Operations

Unit 07 Vulnerability Scanning

# Lab05 – Port Scanning and Nessus

You will need your Kali VM or a desktop that can run the tools shown below (nmap, Microsoft Baseline Security Analyzer, Nessus, and OpenVAS). 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.

### **Advanced Port Scanning with Nmap**

On your Kali machine, start a Wireshark packet capture. While the capture is running, start a port scan with the following parameters:

* Scan type: Syn Scan
* Timing: T4
* Source Port:443
* Range: 192.168.1.0/24 (Or your internal network range)

Once that scan finishes, stop your Wireshark capture. Finding multiple packets coming from your host to the destination with a source port of 443 and the target destination port of whatever nmap was checking. Take a screenshot that shows that your scans were coming from port 443 in Wireshark.

### **MBSA**

Install the MBSA tool from Microsoft on a Windows host. Perform a scan against your local machine that you installed MBSA on. Take a screenshot of the finalized results.

### **Nessus**

Register for and install Nessus home on your Kali VM. Configure a custom scan policy based off the Basic Network Scan policy that Nessus comes with. The scan policy should contain your name. When creating the scan, upload your fping.txt file from the previous labs so that all hosts are scanned in the network (excluding Kali), or manually type in the hosts. Launch the scan with Nessus and take a screenshot of the hosts summary once the scan completes.

### **OpenVAS**

Startup OpenVAS in your Kali machine and create a new scan containing your name + Target (firstLast Target). The hosts of this scan should include your entire testing network. Change the Alive Test to **ICMP, TCP-ACK Service & ARP Ping**. Once you have that scan target defined, create a new scan task with your name + Scan. Set the target of this scan to the target we created in the previous step, change the Scan config to **Full and fast ultimate**, and set the order of the targets to be **random**. Run the scan and allow it to complete, then, click on the report and download a PDF copy of it. Open up that PDF and take a screenshot of the Results Overview section.

## 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.