



CYB 310 5-1 Lab Worksheet

Andree Salvo

Southern New Hampshire University

CYB 310-13007

5-1 Lab Worksheet

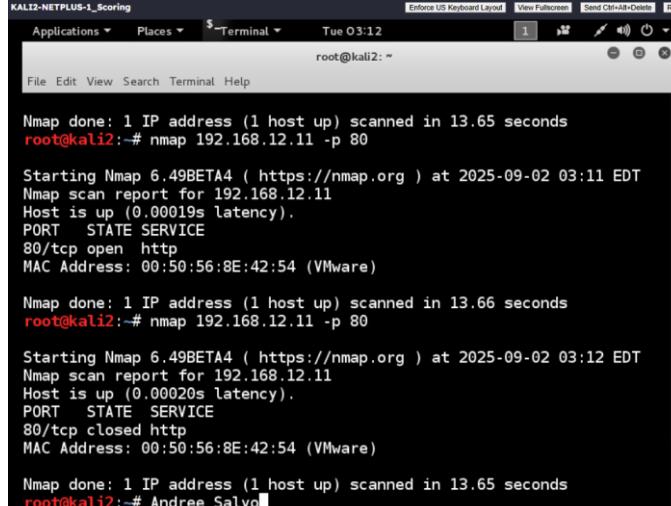
Instructor: Raschid Muller

9/2/2025

Lab: Closing Ports and Unnecessary Services

Prompt	Response
<p>In the lab section, "Connecting to the Open Ports and Services Using Telnet and FTP," Step 13, complete the steps, type your name after the command prompt, and take a screenshot of the output.</p>	A screenshot of a Kali Linux terminal window titled 'KALI2-NETPLUS-1_Scoring'. The window shows a root shell on a Kali Linux system. The user has run the command 'telnet 192.168.12.11 25' and connected to a Microsoft ESMTP MAIL Service. They then ran 'quit' to close the connection. Next, they ran 'telnet 192.168.12.11 80' and connected to an IIS service, receiving an HTTP/1.1 404 Not Found response. Finally, they ran 'quit' again. The terminal ends with the command 'root@kali2:~# Andree Salvo'.

Lab: Closing Ports and Unnecessary Services

Prompt	Response
<p>In the lab section, "Closing Unnecessary Ports and Services," Step 26, type your name after the command prompt and take a screenshot of the output of the scan of port 80 (www) on the Windows machine after closing HTTP services.</p>	 <pre> KALI2-NETPLUS-1_Scorer Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete Rebo Applications Places \$ Terminal Tue 03:12 root@kali2: ~ File Edit View Search Terminal Help Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds root@kali2:~# nmap 192.168.12.11 -p 80 Starting Nmap 6.49BETA4 (https://nmap.org) at 2025-09-02 03:11 EDT Nmap scan report for 192.168.12.11 Host is up (0.00019s latency). PORT STATE SERVICE 80/tcp open http MAC Address: 00:50:56:8E:42:54 (VMware) Nmap done: 1 IP address (1 host up) scanned in 13.66 seconds root@kali2:~# nmap 192.168.12.11 -p 80 Starting Nmap 6.49BETA4 (https://nmap.org) at 2025-09-02 03:12 EDT Nmap scan report for 192.168.12.11 Host is up (0.00020s latency). PORT STATE SERVICE 80/tcp closed http MAC Address: 00:50:56:8E:42:54 (VMware) Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds root@kali2:~# Andree Salvo </pre>
<p>Closing unwanted ports and communication mediums is essential to network hardening. Why is this essential and how does it help with network defense?</p>	<p>When it comes to closing unused ports and communication paths, it helps reduce the attack surface, making it much harder for a threat actor to exploit a vulnerability or even infiltrate the network.</p>
<p>Using an adversarial mindset, how can you test to make sure only needed ports are open? What tools would you use?</p>	<p>When I'm using an adversarial mindset, the first thing I would do is to test any open ports by scanning the network with tools like Nmap or Wireshark to confirm that only necessary ports are accessible.</p>