

CYB 310 5-1 Lab Worksheet

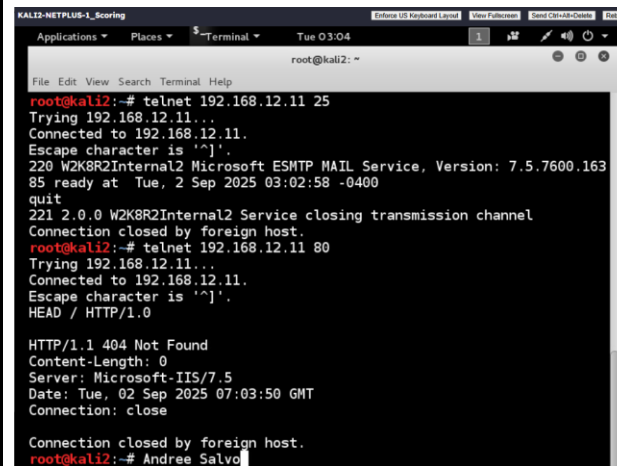
Andree Salvo
 Southern New Hampshire University
 CYB 310-13007
 5-1 Lab Worksheet
 Instructor: Raschid Muller
 9/2/2025

Lab: Closing Ports and Unnecessary Services

Prompt

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.

Response



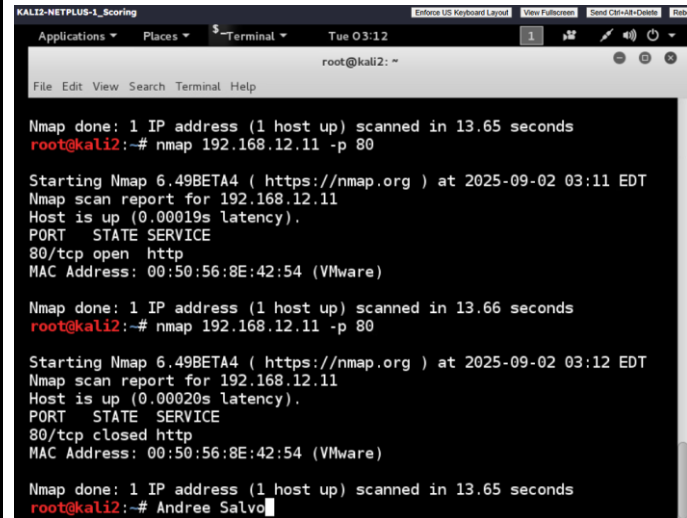
```

KAL12-NETPLUS-1_Scoring
Applications Places $ Terminal Tue 03:04
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# telnet 192.168.12.11 25
Trying 192.168.12.11...
Connected to 192.168.12.11.
Escape character is '^]'.
220 W2K8R2Internal2 Microsoft ESMTMP MAIL Service, Version: 7.5.7600.163
85 ready at Tue, 2 Sep 2025 03:02:58 -0400
quit
221 2.0.0 W2K8R2Internal2 Service closing transmission channel
Connection closed by foreign host.
root@kali2:~# telnet 192.168.12.11 80
Trying 192.168.12.11...
Connected to 192.168.12.11.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 404 Not Found
Content-Length: 0
Server: Microsoft-IIS/7.5
Date: Tue, 02 Sep 2025 07:03:50 GMT
Connection: close

Connection closed by foreign host.
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_Scoring 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>