

CYB 310 Module Five Lab Worksheet

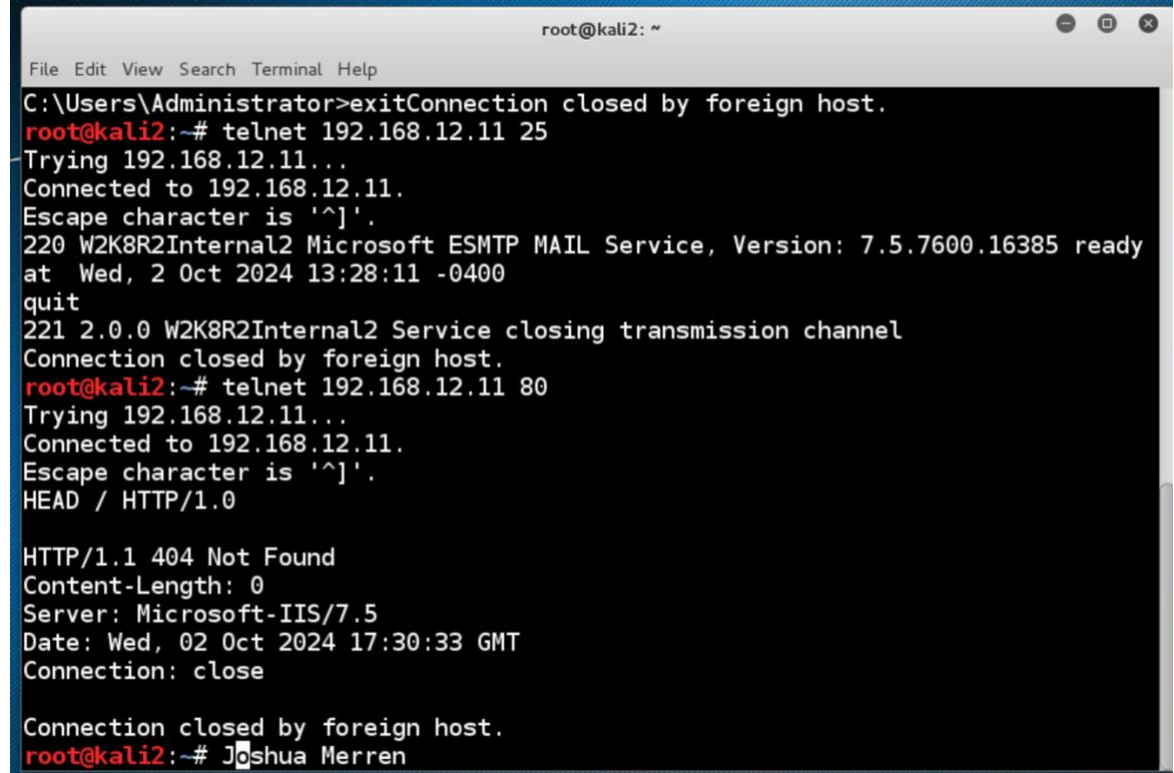
Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

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



```

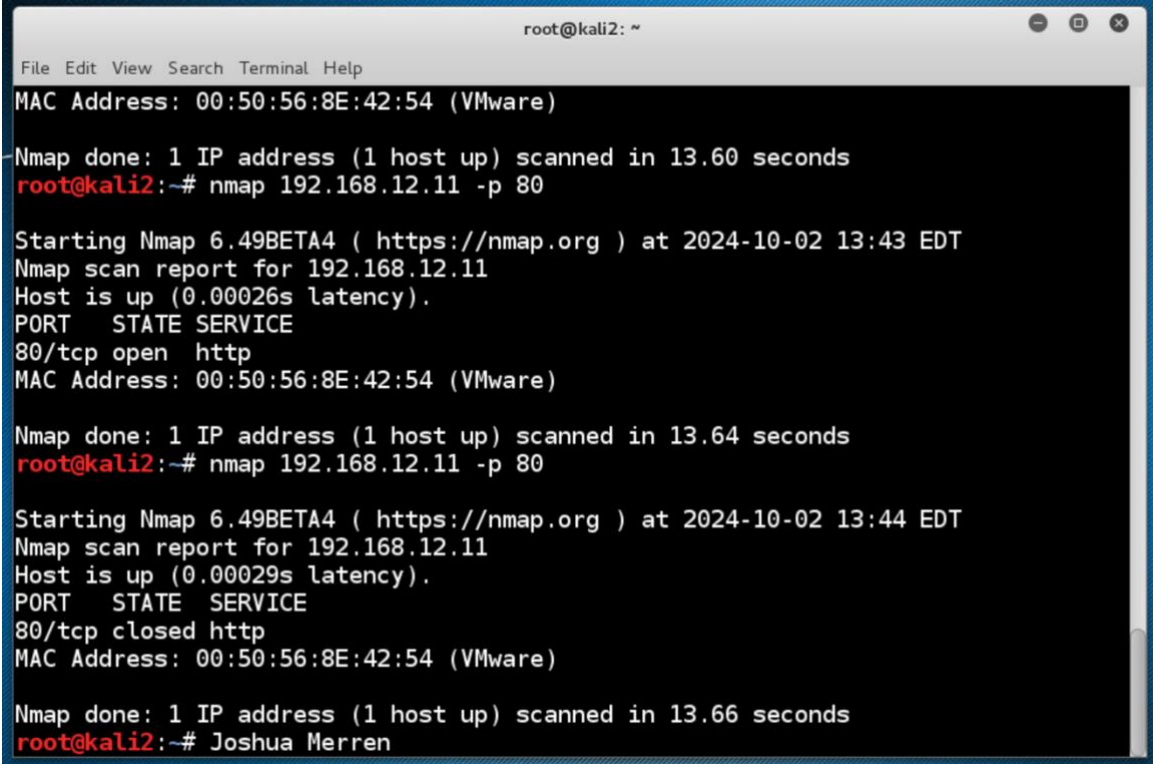
root@kali2: ~
File Edit View Search Terminal Help
C:\Users\Administrator>exitConnection closed by foreign host.
root@kali2:~# telnet 192.168.12.11 25
Trying 192.168.12.11...
Connected to 192.168.12.11.
Escape character is '^]'.
220 W2K8R2Internal2 Microsoft ESMTPL MAIL Service, Version: 7.5.7600.16385 ready
at Wed, 2 Oct 2024 13:28:11 -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: Wed, 02 Oct 2024 17:30:33 GMT
Connection: close

Connection closed by foreign host.
root@kali2:~# Joshua Merren

```

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> root@kali2: ~ File Edit View Search Terminal Help MAC Address: 00:50:56:8E:42:54 (VMware) Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds root@kali2:~# nmap 192.168.12.11 -p 80 Starting Nmap 6.49BETA4 (https://nmap.org) at 2024-10-02 13:43 EDT Nmap scan report for 192.168.12.11 Host is up (0.00026s 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 13.64 seconds root@kali2:~# nmap 192.168.12.11 -p 80 Starting Nmap 6.49BETA4 (https://nmap.org) at 2024-10-02 13:44 EDT Nmap scan report for 192.168.12.11 Host is up (0.00029s 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 13.66 seconds root@kali2:~# Joshua Merren </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>Closing unwanted ports and turning off unnecessary services are critical steps in strengthening network security, often called network hardening. This practice is essential because open ports and active services can serve as entry points for attackers. Attackers could exploit each open port to gain unauthorized access or disrupt services through DDoS attacks. By minimizing the number of open ports and running services, we effectively reduce the system's attack surface, making it harder for attackers to find vulnerable points. This can also simplify the management of security measures, as there are fewer components to monitor and secure, enhancing overall defense against external threats.</p>

Lab: Closing Ports and Unnecessary Services

Prompt	Response
Using an adversarial mindset, how can you test to make sure only needed ports are open? What tools would you use?	Adopting an adversarial mindset to ensure that only necessary ports are open involves regularly assessing the network as if one were an attacker. You can use tools such as Nmap or Wireshark for this purpose. Nmap allows you to perform port scanning to discover open ports and services on network devices. It can identify what services are running on those ports and whether any ports are unnecessarily open. On the other hand, Wireshark helps analyze packets, allowing you to monitor data flow through the network and ensure that no sensitive information transmits through insecure protocols or ports. By continuously monitoring and testing the network with these tools, we can identify and rectify vulnerabilities or misconfigurations early to maintain robust network security.