| Cybersecurity |
| --- |
| Networking Challenge Submission File |

## 

## **Networking Fundamentals: Rocking your Network**

Make a copy of this document to work in. For each phase, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

### Phase **1:** *“I’d like to Teach the World to ping”*

1. Command(s) used to run ping against the IP ranges:

| ping than the IP address for example ping 12.205.151.91 |
| --- |

1. Summarize the results of the ping command(s):

| ping 12.205.151.91 (Request timed out)  ping 15.199.151.91 (Request timed out)  ping 15.199.158.91 (Request timed out)  ping 15.199.141.91 (Request timed out)  ping 15.199.131.91 (Request timed out)  ping 15.199.121.91 (Request timed out)  ping 15.199.111.91 (Request timed out)  ping 15.199.100.91 (Request timed out)  ping 15.199.99.91 (Request timed out)  ping 15.199.98.91 (Request timed out)  ping 15.199.97.91 (Request timed out)  ping 15.199.96.91 (Request timed out)  ping 15.199.95.91 (Request timed out)  ping 15.199.94.91 (Request timed out)  Ping 203.0.113.32 (Request timed out)  Ping 161.35.96.20 (Reply from 161.35.96.20: bytes=32 time=216ms TTL=49  Reply from 161.35.96.20: bytes=32 time=212ms TTL=49  Reply from 161.35.96.20: bytes=32 time=214ms TTL=49  Reply from 161.35.96.20: bytes=32 time=214ms TTL=49)  Ping 192.0.2.0 (Request timed out)  Ping 192.0.2.16 (Request timed out)  Ping 198.51.100.0 (Request timed out)  Ping 198.51.100.16 (Request timed out)  Ping 198.51.100.32 (Request timed out)  Ping 203.0.113.0 (Request timed out)  Ping 203.0.113.16 (Request timed out) |
| --- |

1. List of IPs responding to echo requests:

| Ping 161.35.96.20 (Reply from 161.35.96.20: bytes=32 time=216ms TTL=49  Reply from 161.35.96.20: bytes=32 time=212ms TTL=49  Reply from 161.35.96.20: bytes=32 time=214ms TTL=49  Reply from 161.35.96.20: bytes=32 time=214ms TTL=49)  IP 161.35.96.20 is still functioning and alive |
| --- |

1. Explain which OSI layer(s) your findings involve:

| Ping operates at the Network Layer (Layer 3) of the OSI model as it generates ICMP Echo Request messages to assess the reachability of a network host |
| --- |

1. Mitigation recommendations (if needed):

| To protect network devices from ICMP Echo Requests risks, the CISO can configure devices to block or limit ping requests, making them less visible and reducing attacks from hackers |
| --- |

### Phase **2:** *“Some SYN for Nothin’”*

1. Which ports are open on the RockStar Corp server?

| Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-30 05:41 UTC  Nmap scan report for 161.35.96.20  The host is up (0.22s latency).  Not shown: 999 closed ports  PORT STATE SERVICE  22/tcp open ssh  Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds  The port open is 22 |
| --- |

1. Which OSI layer do SYN scans run on?
   1. OSI layer:

| SYN scans run on the transport layer 4 |
| --- |

* 1. Explain how you determined which layer:

| SYN scans are used to reveal the status of open ports by employing TCP SYN packets. When executing a SYN scan, the analysis of network traffic becomes a valuable tool. The use of SYN, ACK, FIN, and RST acronyms in response packets allows for a comprehensive assessment of host-to-host communication. Each of these acronyms provides distinct information, signaling whether the traffic is open, acknowledged, rejected, or closed. This nuanced analysis facilitates a thorough understanding of the accessibility and security status of networked machines. |
| --- |

1. Mitigation suggestions (if needed):

| To mitigate against SYN attacks use things like a firewall to limit the number of SYN packets you receive at once and also load balancing so if a hacker tries to send too many packets at once causing your machine to crash you can have a load balancer that it distributes across multiple machines instead of one. |
| --- |

### Phase **3:** *“I Feel a DNS Change Comin’ On”*

1. Summarize your findings about why access to rollingstone.com is not working as expected from the RockStar Corp Hollywood office:

| The reason Why they cannot access their account is due to someone deleted the home directory for Jimi Hendrix |
| --- |

1. Command used to query Domain Name System records:

| Nslookup 98.137.246.8 |
| --- |

1. Domain name findings:

| unknown.yahoo.com |
| --- |

1. Explain what OSI layer DNS runs on:

| Layer 7 |
| --- |

1. Mitigation suggestions (if needed):

| Disable port 22 |
| --- |

### Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

| packetcaptureinfo.txt |
| --- |

1. ARP findings identifying the hacker’s MAC address:

| The hacker's MAC address is 1d:b3:b1 |
| --- |

1. HTTP findings, including the message from the hacker:



1. Explain the OSI layers for HTTP and ARP.
   1. Layer used for HTTP:

| HTTP Overview  • Application-layer protocol in OSI model for web communication.  • Operates over TCP for fetching and displaying web content.  • Governs interaction between web clients and servers.  • Enables retrieval and presentation of multimedia content  Layer 7 |
| --- |

* 1. Layer used for ARP:

| Address Resolution Protocol (ARP) Functions  • Functions at the Data Link layer on local area networks.  • Mapping IP addresses to MAC addresses.  • Enables proper data link layer communication.  • Exchanges ARP request and reply messages for updated IP and MAC address mapping.  Layer 2 |
| --- |

1. Mitigation suggestions (if needed):

| Ensure the security of your information by regularly checking for open ports to prevent unauthorized access by potential hackers. |
| --- |

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.