| Cybersecurity |
| --- |
| Module 8 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 fping against the IP ranges:

| fping -g -r 1 15.199.95.91/28  fping -g -r 1 15.199.94.91/28  fping -g -r 1 203.0.113.32/28  fping -g -r 1 161.35.96.20/32  fping -g -r 1 192.0.2.0/28 |
| --- |

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

| All IP addresses with subnets of 28 were unreachable through fping, while the one IP address with a subnet of 32 was reachable. |
| --- |

1. List of IPs responding to echo requests:

| 161.35.96.20 |
| --- |

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

| Layer 7, the Application Layer |
| --- |

1. Mitigation recommendations (if needed):

| IP 161.35.96.20 is a vulnerability since Rockstar Corp does not want to show a response to any request, recommend restricting the echo commands for IP 161.35.96.20 |
| --- |

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

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

| Port 22 |
| --- |

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

| Layer 4, the Transport Layer |
| --- |

* 1. Explain how you determined which layer:

| SYN scans are a type of TCP scan that involves sending a SYN packet to a target IP and port number, and then waiting for a response. |
| --- |

1. Mitigation suggestions (if needed):

| Reconfigure the firewall to block traffic to port 22 to mitigate this vulnerability. |
| --- |

### 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:

| An unknown person utilized the vulnerability on the Application server through port 22 to spoof the DNS of rollingstone.com to direct traffic to another website. |
| --- |

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:

| DNS uses layer 7, the Application Layer. |
| --- |

1. Mitigation suggestions (if needed):

| Utilizing the firewall after the open port issue is fixed. Implement DNSSEC. Monitor DNS traffic more frequently. Ensure no other users have sudo access to modifying the /etc/hosts file. |
| --- |

### Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

| packetcaptureinfo.txt |
| --- |

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

| Hacker used ARP spoofing to direct traffic to 192.168.47.200 intended for “the good host” at 00:0c:29:0f:71:a3 to the hackers physical address of 00:0c:29:1d:b3:b1. |
| --- |

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

| The hacker appears to be an employee at Rockstar Corp. They sent a message to Gottheblues via their contact us page at [www.gottheblues.yolasite.com/contact-us.php](http://www.gottheblues.yolasite.com/contact-us.php), advising that they have left port 22 open and will provide login credentials for $1 million.  “Hi Got The Blues Corp! This is a hacker that works at Rock Star Corp. Rock Star has left port 22, SSH open if you want to hack in. For 1 Million Dollars I will provide you the user and password!” |
| --- |

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

| Layer 7, the Application Layer |
| --- |

* 1. Layer used for ARP:

| ARP works between Layers 2 (Data-Link) and 3 (Network) |
| --- |

1. Mitigation suggestions (if needed):

| Set up static ARP entries, permanent IP-to-MAC mapping in the local ARP cache. |
| --- |

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