| Cybersecurity |
| --- |
| Module 8 Challenge Submission File |

## 

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

Make a copy of this document to work in, and then 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 -ga 15.199.95.91/28  fping -ga 15.199.94.91/28  fping -ga 11.199.158.91/28  fping -ga 161.35.96.20/32  fping -ga 11.199.141.91/28 |
| --- |

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

| Most IPs were unreachable, except for 161.35.96.20. |
| --- |

1. List of IPs responding to echo requests:

| 161.35.96.20 |
| --- |

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

| My findings were on layer 3 of the OSI Model |
| --- |

1. Mitigation recommendations (if needed):

| I would recommend disabling ping responses on 161.35.96 |
| --- |

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

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

| Port 22 is open |
| --- |

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

| The scans run on layer 4 of the OSI layer model. The transport layer |
| --- |

* 1. Explain how you determined which layer:

| Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation and desegmentation, and error control. |
| --- |

1. Mitigation suggestions (if needed):

| One way to mitigate this vulnerability is to filter ssh connections with a  firewall, and to use a custom port for ssh connections. Should also mitigate  ssh brute force attacks by limiting login attempts and adding a blocklist to  the firewall. |
| --- |

### 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:

| /etc/hosts on the Hollywood office computer was appended with:98.137.246.8  rollingstone.com, leading the computer to use an unreachable address for  rollingstone.com |
| --- |

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 runs on Layer 7, the application layer. When user applications request  that domain names be converted to IP addresses, DNS performs this in the  application layer to send communications down to the lower layers. |
| --- |

1. Mitigation suggestions (if needed):

| Closely monitor edits to /etc/hosts file, periodically compare system DNS  queries to authoritative DNS server queries, to ensure there is no DNS  spoofing. Can also disable local name resolution via the hosts file. |
| --- |

### Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

| secretlogs.pcapng |
| --- |

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

| 00:0c:29:0f:71:a3 is the hacker’s MAC address. He spoofed his mac address to  00:0c:29:1d:b3:b1, which is evidenced by the duplicate mac addresses of the  IP 192.168.47.200. |
| --- |

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

| HTTP packets revealed the hacker was accessing a forum website, examining  the HTTP POST packet revealed his message. Form item: "3<textarea>" = "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 Milliion  Dollars I will provide you the user and password!" |
| --- |

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

| HTTP is the protocol for website data, which are end-user applications, thus  it is in Layer 7. |
| --- |

* 1. Layer used for ARP:

| Address resolution protocol links MAC addresses and IP addresses, so it  works on two layers, Layer 2, datalink, where the mac address lives, and  Layer 3, network, where IP addresses live. |
| --- |

1. Mitigation suggestions (if needed):

| Use a static ARP table. Filter connections from duplicate MAC addresses in  order to prevent spoofing attacks in the future. |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.