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 -g 15.199.95.91/28
fping -g 15.199.94.91/28
fping -g 11.199.158.91/28
fping -g 161.35.96.20/32
```

2. Summarize the results of the `fping` command(s):

```
<ip address> is unreachable
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

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

```
Network/Layer 3
```

5. Mitigation recommendations (if needed):

```
Restrict the ability to ping the servers
```

Phase 2: *“Some SYN for Nothin`”*

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

```
Port 22
```

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

```
Transport Layer/Layer 4
```

    b. Explain how you determined which layer:

```
Layer 4 is to search to find the integrity of the connection
```

3. Mitigation suggestions (if needed):

```
Better maintenance and monitoring of who has access
```

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 IP address for rolling stone had a different IP Address associated in
the NS records. It redirected me to an unknown yahoo domain because that is
the IP address associated with the rolling stone host file.
```

2. Command used to query Domain Name System records:

```
nslookup
```

3. Domain name findings:

```
Unknownyahoo.com domain name
```

4. Explain what OSI layer DNS runs on:

```
Application Layer/Layer 7
```

5. Mitigation suggestions (if needed):

```
Making sure the host file has the most up to date IP Addresses
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
packetcaptureinfo.txt
```

2. ARP findings identifying the hacker's MAC address:

```
In Packet 5, Wireshark called out duplicate Mac address responding to IP
address 192.168.47.200
```

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

```
"Hi, I got the Blues Corp! This is a hacker that works at Rock Stars Corp."
```

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

```
Layer 7/Application Layer
```

    b. Layer used for ARP:

```
Layer 2/ Data Link Layer
```

5. Mitigation suggestions (if needed):

```
You can run a firewall that specifically looks for Mac spoofing
```