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
fping -g 11.199.141.91/28
```

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

```
All ip ranges are down besides 161.35.96.20/32. 161.35.96.20/32 is alive.
```

3. List of IPs responding to echo requests:

```
161.35.96.20/32
```

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

```
Layer 3
```

5. Mitigation recommendations (if needed):

```
Close all ports
```

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:

```
Layer 4
```

    b. Explain how you determined which layer:

The **Transport layer** is responsible for actually transmitting data across the network.

It puts data onto the network,
and assigns source and destination ports

3. Mitigation suggestions (if needed):

```
Close port 22
```

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 /etc/hosts file has rollingstone.com set up to go to the wrong ip
address. 98.137.246.8 is associated with unknown.yahoo.com
```

2. Command used to query Domain Name System records:

```
nslookup 98.137.246.8
```

3. Domain name findings:

```
8.246.137.98.in-addr.arpa     name = unknown.yahoo.com.
98.137.246.8 is associated with unknown.yahoo.com
```

4. Explain what OSI layer DNS runs on:

```
Layer 7: used to communicate across an IP network.
```

5. Mitigation suggestions (if needed):

```
Change the host file to route traffic back to the correct web service. Close
port 22 to prevent further security breaches.
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
packetcaptureinfo.txt
```

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

```
Sender MAC address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
```

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

```
The hacker sent an email to Got The Blue Corp which read: "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!"
```

4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

```
Layer 7
```

b. Layer used for ARP:

```
Layer 2
```

5. Mitigation suggestions (if needed):

```
Perform regular inspections.
```