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 -a
```

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

```
2 IP's are alive and 3 are unreachable
161.35.96.20 - alive
192.0.2.0 - alive
15.199.95.91 - unreachable
15.199.94.91 - unreachable
203.0.113.32 - unreachable
```

3. List of IPs responding to echo requests:

```
161.35.96.20   192.0.2.0
```

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

```
Layer 3 and layer 4. Layer 3 the network layer is responsible for IP
addressing, routing, and forwarding of packets between networks which showed
```

```
the 2 IP addresses that were alive and the other 3 that were inactive. Layer 4 the transport layer is responsible for establishing connections and managing the flow of data between hosts which showed that the 2 IP addresses that were alive indicated that the connection was successfully established and the data was flowing between the hosts.
```

5. Mitigation recommendations (if needed):

```
Setup a firewall to block requests and replies
```

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: transport
```

    b. Explain how you determined which layer:

```
I determined the layer bc it has to scan the IP addresses and scanning through them tells me which ports are open.
```

3. Mitigation suggestions (if needed):

```
Use port knocking. Use a firewall. Change default ports and close unused ports.
```

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 rollingstone.com in the hosts file is not the actual IP address to get to that website.
```

2. Command used to query Domain Name System records:

```
nslookup 98.137.246.8
```

3. Domain name findings:

```
unknown.yahoo.com
```

4. Explain what OSI layer DNS runs on:

```
Application layer 7
```

5. Mitigation suggestions (if needed):

```
Update the correct IP address for rollingstone.com in the hosts file and set permission on who can read or write in the file.
```

Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

```
packetcaptureinfo.txt
```

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

```
IP address 192.168.47.200 has a duplicate and the hacker’s MAC address is 00:0c:29:1d:b3:b1
```

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

```
A message for CloudFlare.inc (IP address: 104.18.126.89)  saying “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!”
```

4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

```
Layer 7 Application: this is used to exchange information between web
servers and clients over the internet
```

    b. Layer used for ARP:

```
Layer 2 Data Link Layer: this allows network devices to communicate with
each other on the same local network
```

5. Mitigation suggestions (if needed):

```
Implement access controls and authentication mechanisms. Implement ARP
spoofing prevention measures.
```