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 161.35.96.32/20
fping -g 11.199.141.91/28
```

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

```
161.35.96.20/32 was the only server that sent back pings.
```

3. List of IPs responding to echo requests:

```
161.35.96.32/20
```

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

```
The Network Layer 3 would be involved in this.
```

5. Mitigation recommendations (if needed):

```
Restrict the ICMP Echo requests to their servers including 161.35.96.20
```

Phase 2: *“Some SYN for Nothin`”*

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

```
According to the nmap scan the ssh port 22 is open on the 161.35.96.20
Hollywood Application Server.
```

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

```
They run on Layer 4 the transport layer.
```

    b. Explain how you determined which layer:

```
Layer 4 is the transport layer which allows for end to end communication
over a network.
```

3. Mitigation suggestions (if needed):

```
Implement filtering for SSH traffic into their servers to prevent
unauthorized 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:

```
While checking the /etc/hosts file there was an ip address rerouting traffic
to an unknown site on 98.137.246.8.
```

2. Command used to query Domain Name System records:

```
Nslookup 98.137.246.8
```

3. Domain name findings:

```
The results of the nslookup were as follows:
8.246.137.98.in-addr.arpa     name = unknown.yahoo.com.
The ip address was rerouting to an unknown yahoo server.
```

4. Explain what OSI layer DNS runs on:

```
DNS runs on the Application Layer 7. Layer 7 is shared by many protocols to
communicate across an IP network.
```

5. Mitigation suggestions (if needed):

```
Change all default username/passwords and reset them across all servers. The
Write access on the Host file should only be given to certain employees.
```

Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

```
packetcaptureinfo.txt
```

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

```
There was ARP poisoning, the hacker submitted a malicious server to the ARP
cache to steal traffic. 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 as follows:
“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 is used by HTTP to communicate across an IP network.
```

b. Layer used for ARP:

```
Layer 2 the Data Link layer is used to transfer traffic within a local
network.
```

5. Mitigation suggestions (if needed):

```
Create static ARP entries or invest in Networking solutions that can stop
and identify spoofed ARP requests.
```