Cybersecurity

Networking 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 `ping` against the IP ranges:

```
ping 15.199.95.91
ping 15.199.94.91
ping 203.0.113.32
ping 161.35.96.20
ping 192.0.2.0
```

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

```
Hollywood Application Server 1 is the only one responding. All other servers
are not responding.
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

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

```
Layer 3: Network, as utilizing IP addresses falls on this Layer.
```

5. Mitigation recommendations (if needed):

```
Hollywood Application Server 1 is a vulnerability. It will be necessary to
investigate further.
```

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:

```
Network Layer 4: Transport
```

    b. Explain how you determined which layer:

```
SYN scans utilize Transport Connection Protocol (tcp) to determine which
ports are open.
```

3. Mitigation suggestions (if needed):

```
Determine if the server is accessible.
```

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:

```
On the /etc/hosts configuration file, the IP 98.137.246.8 was given the
hostname “rollingstone.com”. This causes the ping command to attempt to
connect to the IP address of that user instead of the actual website. In
this case, it was unable to connect.
```

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:

```
Layer 7: Application, as it helps determine how data is sent and received
between applications.
```

5. Mitigation suggestions (if needed):

```
Determine how to remove the IP address from the hostname.
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
/etc/packetcaptureinfo.txt
```

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

```
00:0c:29:1d:b3:b1
```

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

```
Name: MrHacker
Email: Hacker@rockstarcorp.com
Message: "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 5: Session
```

b. Layer used for ARP:

```
Layer 2: Data Link
```

5. Mitigation suggestions (if needed):

```
The MAC address and the user has been found and will need to be removed from the server.
```