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 15.199.95.91 15.199.94 203.0.113.32 161.35.96.20
```

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

```
There was one server alive {ip: 161.35.96.20} all of the other ones were
unreachable. This indicates that there is a vulnerability present.
```

3. List of IPs responding to echo requests:

```
IP: 161.35.96.20
```

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

```
OSI Layer 3: this layer is responsible for transmitting data between
networks (ie. routing and data transfer)
```

5. Mitigation recommendations (if needed):

```
Turning on a firewall rule to prevent any echo request from reaching 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:

```
Layer 4 or “Transport”
```

    b. Explain how you determined which layer:

```
SSH is a network protocol that operates on level 4; SSH is used for
providing secure connectivity via encryption.
```

3. Mitigation suggestions (if needed):

```
None; SSH already provides secure communication.
```

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 DNS is not set up correctly and was modified by an unauthorized server.
The DNS of rollingstone.com was modified to 192.0.66.114 from unauthorized
server 8.8.8.8#53
```

2. Command used to query Domain Name System records:

```
nslookup 98.137.246.8
```

3. Domain name findings:

```
Non-authoritative answer:
Name: rollingstone.com
Address: 192.0.66.114
```

4. Explain what OSI layer DNS runs on:

```
Layer 7
```

5. Mitigation suggestions (if needed):

```
Firewalls to prevent unauthorized access to DNS servers; this will prevent
attckers from being able to access and modify DNS records.
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
secretlogs.pcapng
```

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

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

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

```
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: the application layer where data transmits between web server and
client
```

b. Layer used for ARP:

```
Layer 2: Used to map MAC addresses to IP; operates on data link in the OS
```

5. Mitigation suggestions (if needed):

```
Utilizing https instaed of just http and use MAC filtering
```

Source:
https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/#:~:text=HTTPS%20is%20HTTP%20with%20encryption,far%20more%20secure%20than%20HTTP.

https://umn.bootcampcontent.com/University-of-Minnesota-Boot-Camp/UofM-VIRT-CYBER-PT-09-2022-U-LOLC/-/blob/main/11-Network-Security/1/StudentGuide.md