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 -s 15.199.95.91 15.199.94.91 11.199.158.91 161.35.96.20 11.199.141.91
```

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

```
161.35.96.20 is alive and the other 4 are unreachable
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

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

```
Network Layer
```

5. Mitigation recommendations (if needed):

```
The corporation doesn't want any ip addresses to be reachable so we would
have to block that ip using the firewall
```

Phase 2: *“Some SYN for Nothin`”*

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

```
Port 22 is open
```

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

```
Transport Layer
```

    b. Explain how you determined which layer:

```
Port 22 is the transport layer on the TCP model
```

3. Mitigation suggestions (if needed):

```
I don’t think there is any mitigation needed
```

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:

```
I believe the wrong ip address is associated with the website
```

2. Command used to query Domain Name System records:

```
nslookup www.rollingstones.com
```

3. Domain name findings:

```
The Ip address for rollingstones.com is 18.190.122.157
The other address is 2607:f8b0:4009:818::2004
```

4. Explain what OSI layer DNS runs on:

```
Application layer
```

5. Mitigation suggestions (if needed):

```
Change the ip route to run off of the 161.35.96.20 address
```

Phase 4: *"ShARP Dressed Man"*

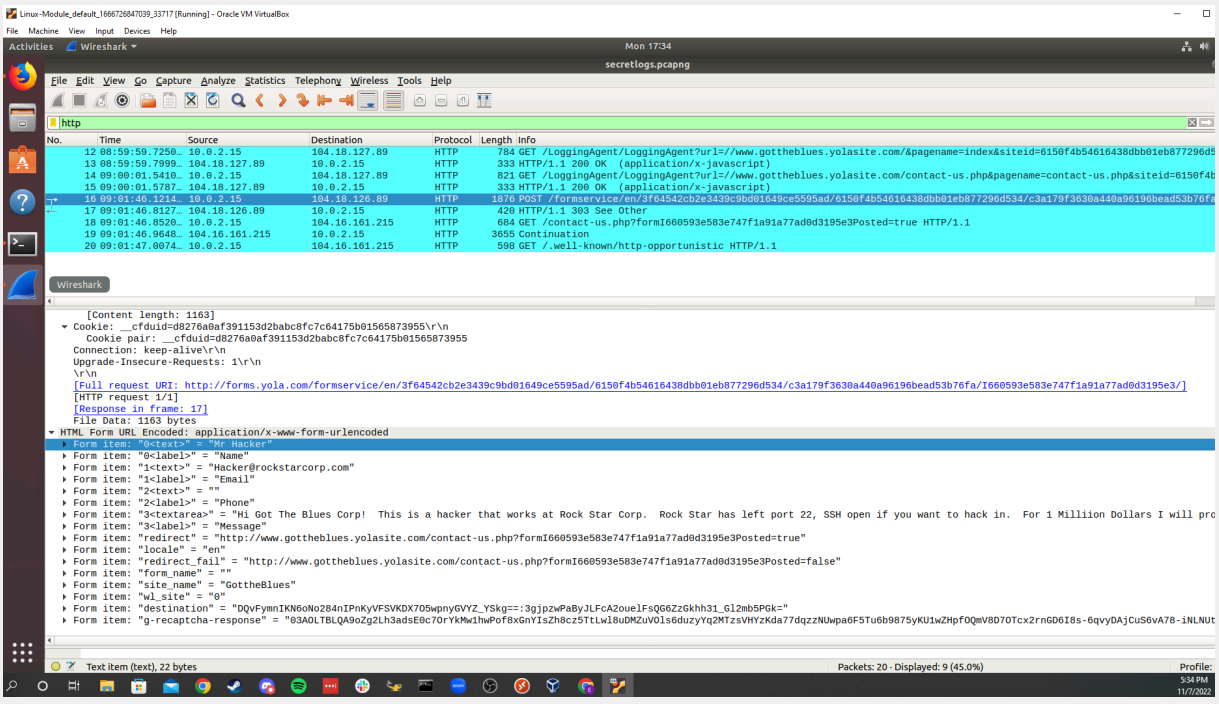
1. Name of file containing packets:

```
secretlogs.pcapng
```

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

```
There is a duplicate ip address for 192.168.47.200
```

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



4. Explain the OSI layers for HTTP and ARP.
    a. Layer used for HTTP:

```
Application layer
```

    b. Layer used for ARP:

```
Data Link layer
```

5. Mitigation suggestions (if needed):

```
Change the ip address so they won’t be duplicated
```