Cybersecurity

Networking Challenge Submission File

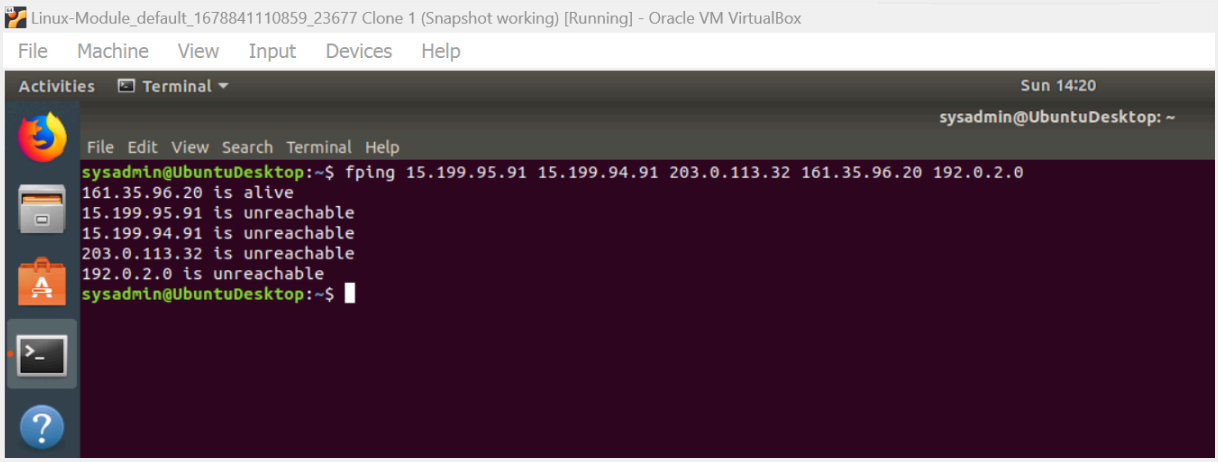
Networking Fundamentals: Rocking your Network

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:

```
fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
```

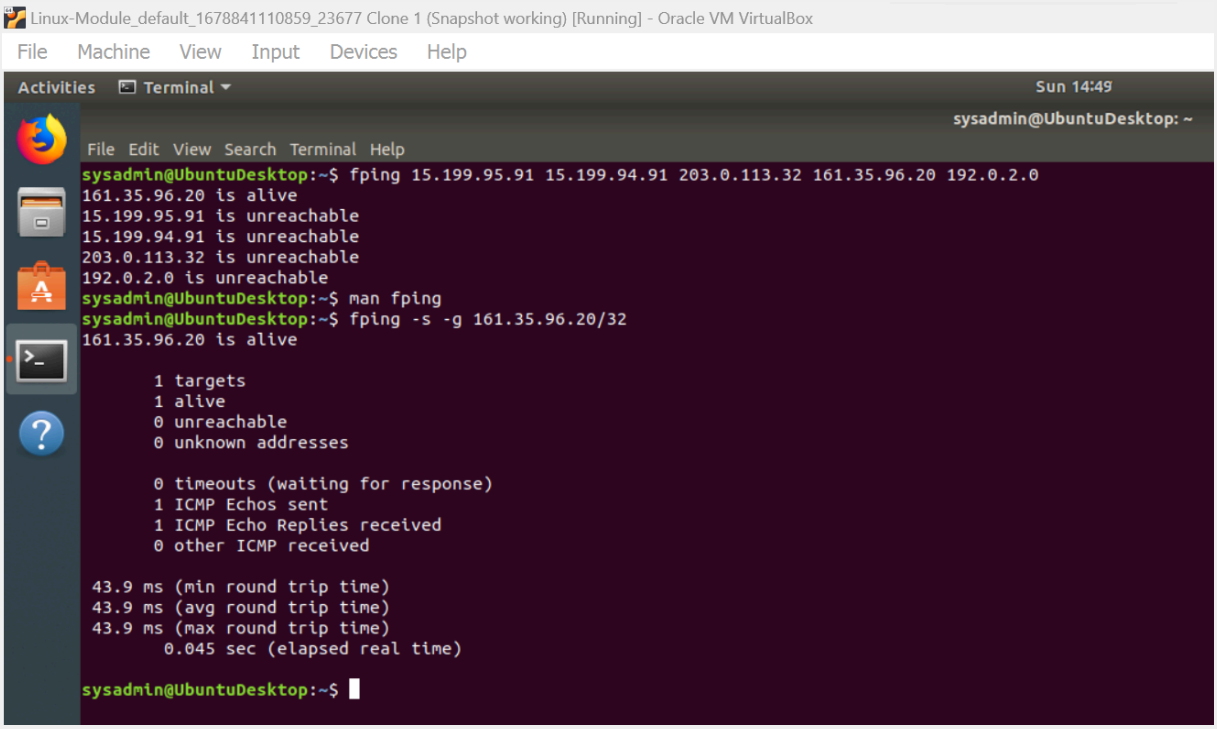


2. Summarize the results of the `ping` command(s):

```
The results of the fping command show us that only the IP 161.35.96.20 is reachable.
```

3. List of IPs responding to echo requests:

```
fping -s -g 161.35.96.20/32
This command shows that this IP
```



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

```
The OSI layer in the findings involve the Network layer.
```

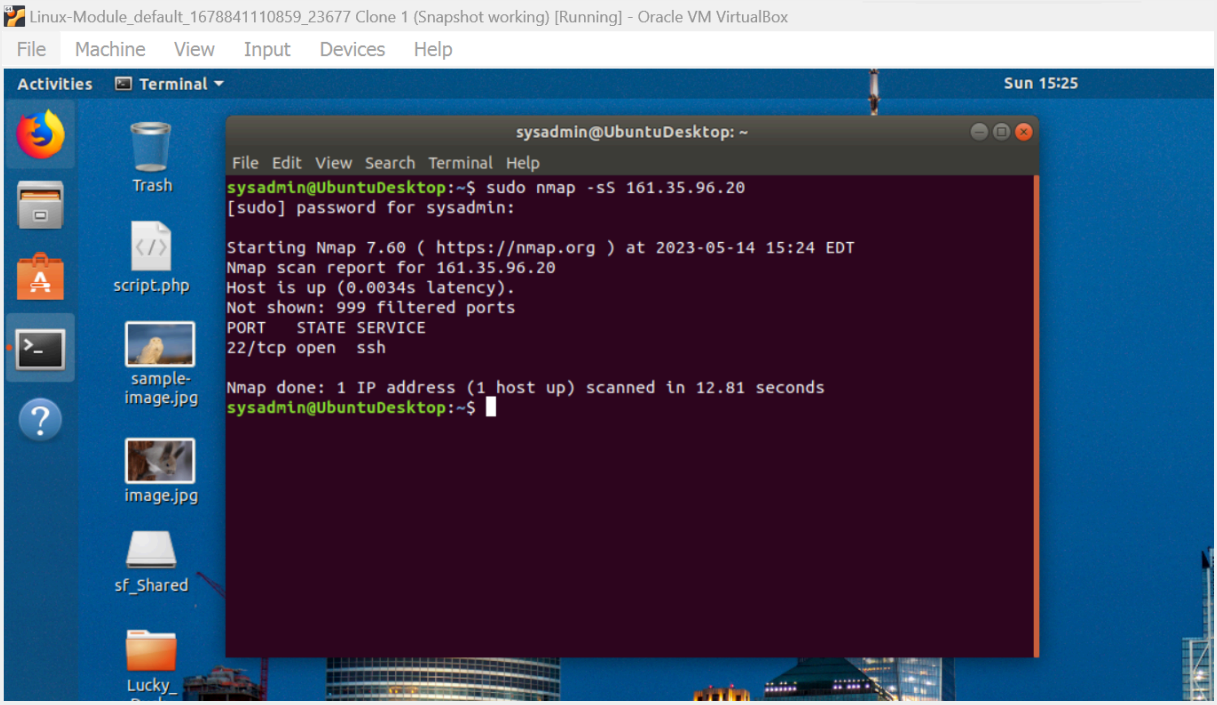
5. Mitigation recommendations (if needed):

```
Using the fping command we were able to see that the IP 161.35.96.20 is
alive and is accepting pings. Rockstar Corp did not want any of their IP
address to respond to requests and sice this IP is it could lead to a
vulnerability as it could allow for unauthorized access. We need to make
adjustmnets to make sure that all servers are alive but show as unreachable
and also make sure that our ports are closed as we don not want to be a
victim of a DoS attack.
```

Phase 2: *“Some SYN for Nothin’”*

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

After running the nmap command, we are able to see that port 22 is open



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

The OSI layer the SYN scans run on are the Transport layer.

    b. Explain how you determined which layer:

In class we discussed TCP and the three way handshake that is needed to esablish a connection. The port that is opne is 22 and its involves TCP to establish a connection for the SSH.

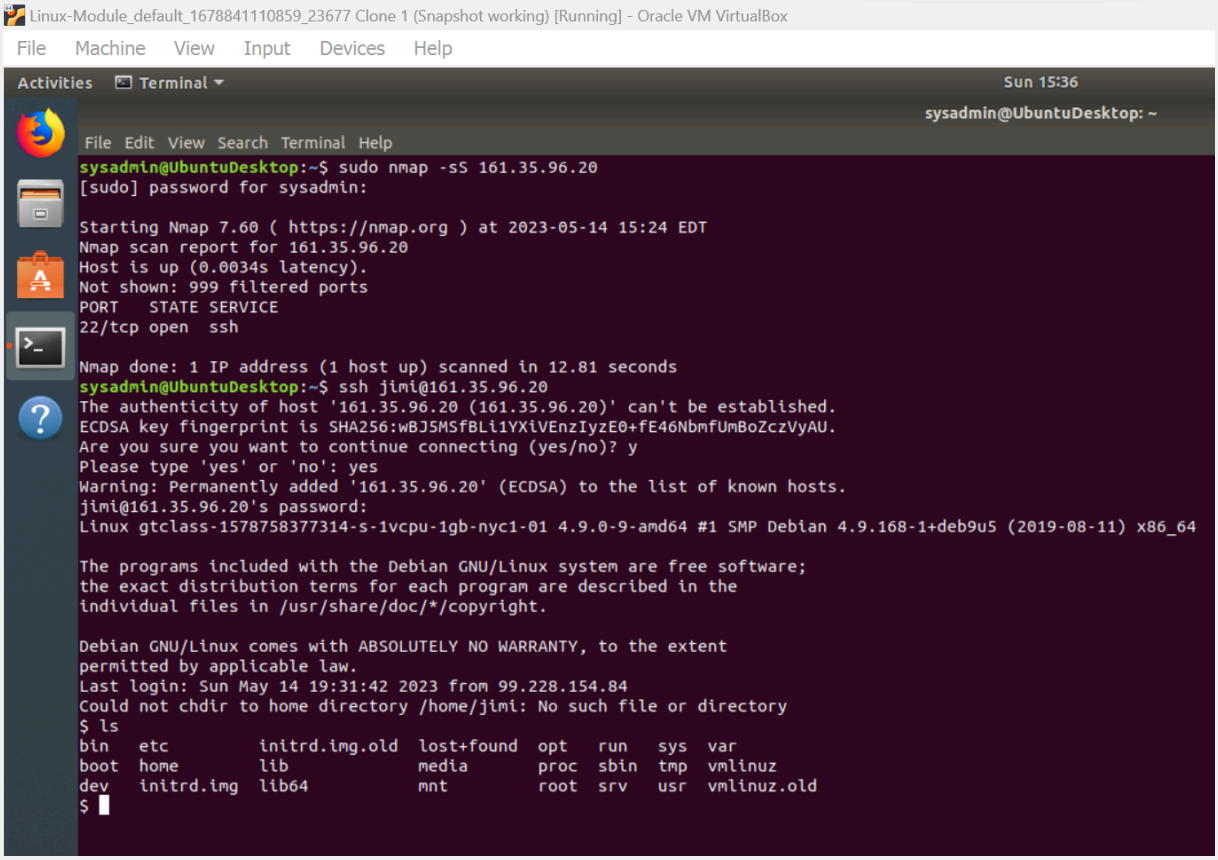
3. Mitigation suggestions (if needed):

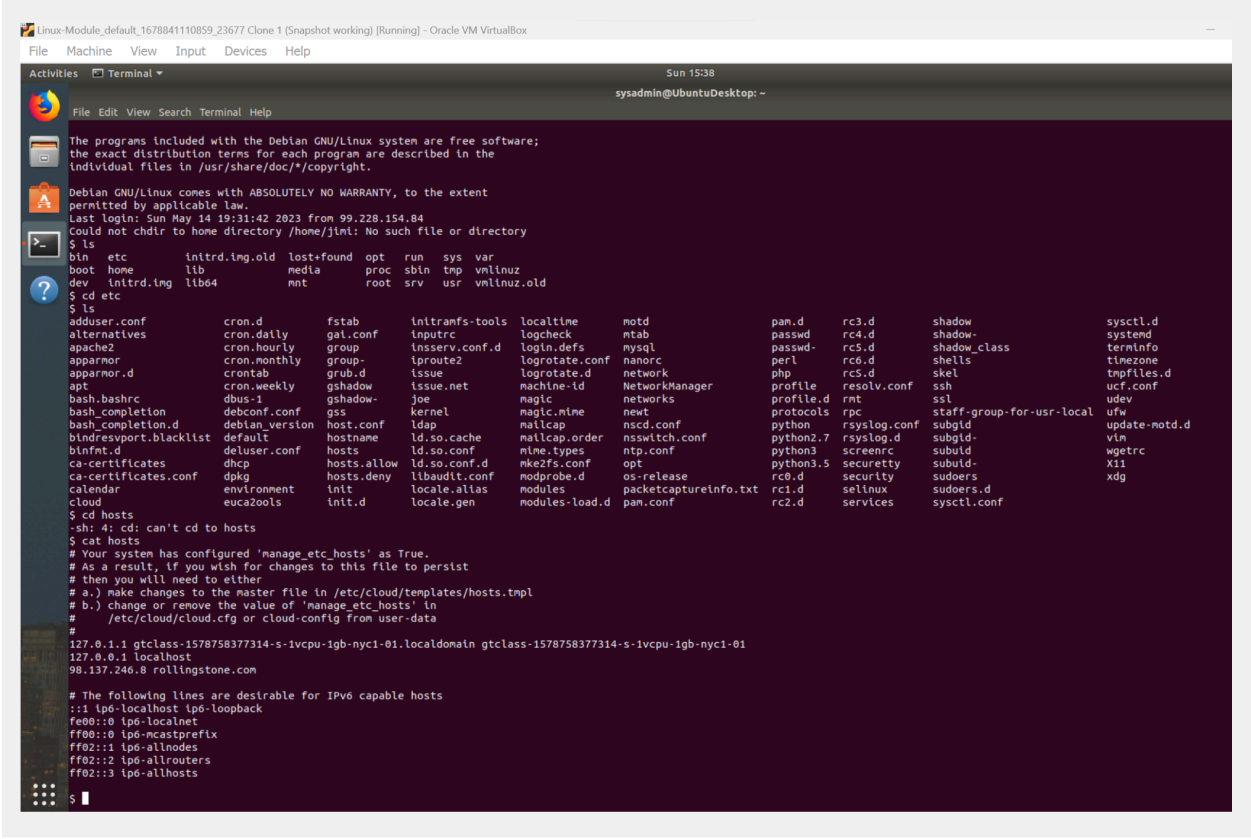
Port 22 needs to be shut down so no bad actor is able to SSH into the system.

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:

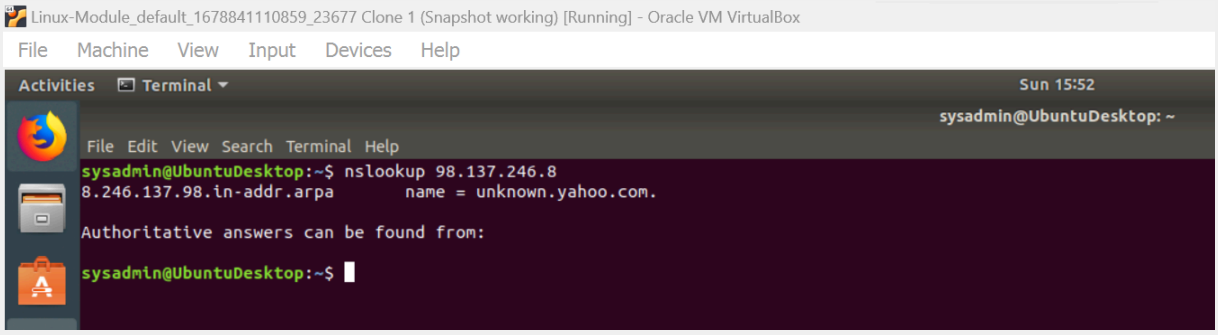
I was able to ssh into the system, which means a hacker would also be able to access the system and set up a backdoor and change the IP address.





2. Command used to query Domain Name System records:

```
nslookup 98.137.246.8
```



3. Domain name findings:

```
There seems to another domain found unknown.yahoo.com.
```

4. Explain what OSI layer DNS runs on:

The OSI layer that the DNS runs on is the application layer (layer 7).

5. Mitigation suggestions (if needed):

The IP address needs to be changed immediately to the original and port 22 should be closed ASAP so the hacker cannot get back in and change the IP address. As an extra level of caution a DNS filter should be added for security.

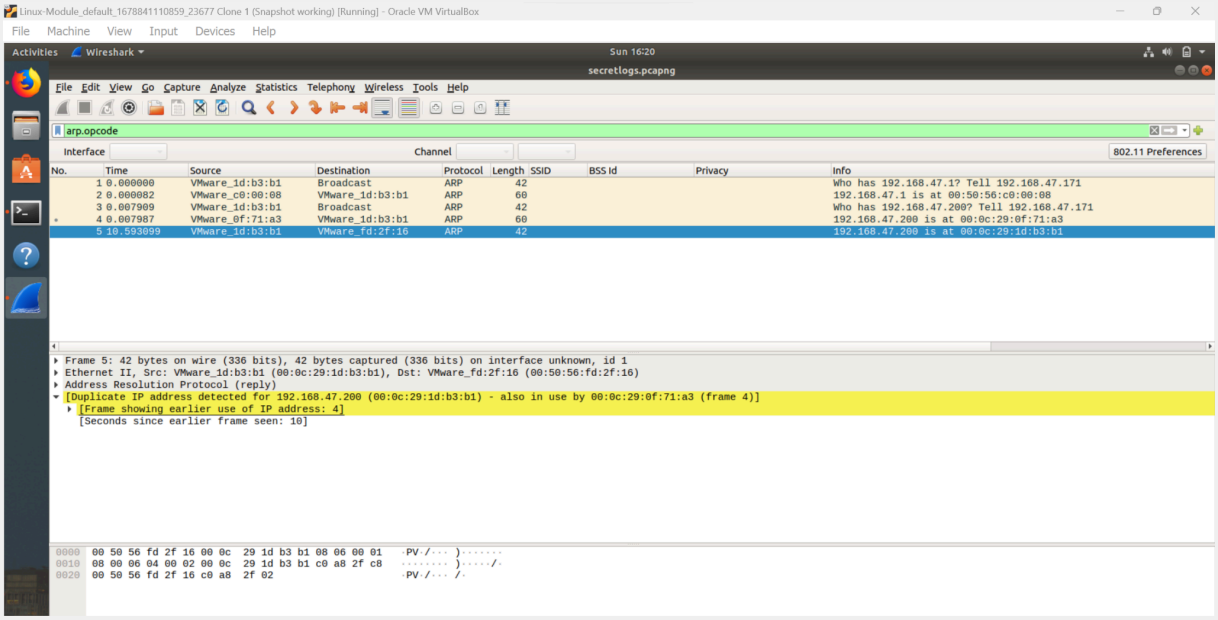
Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

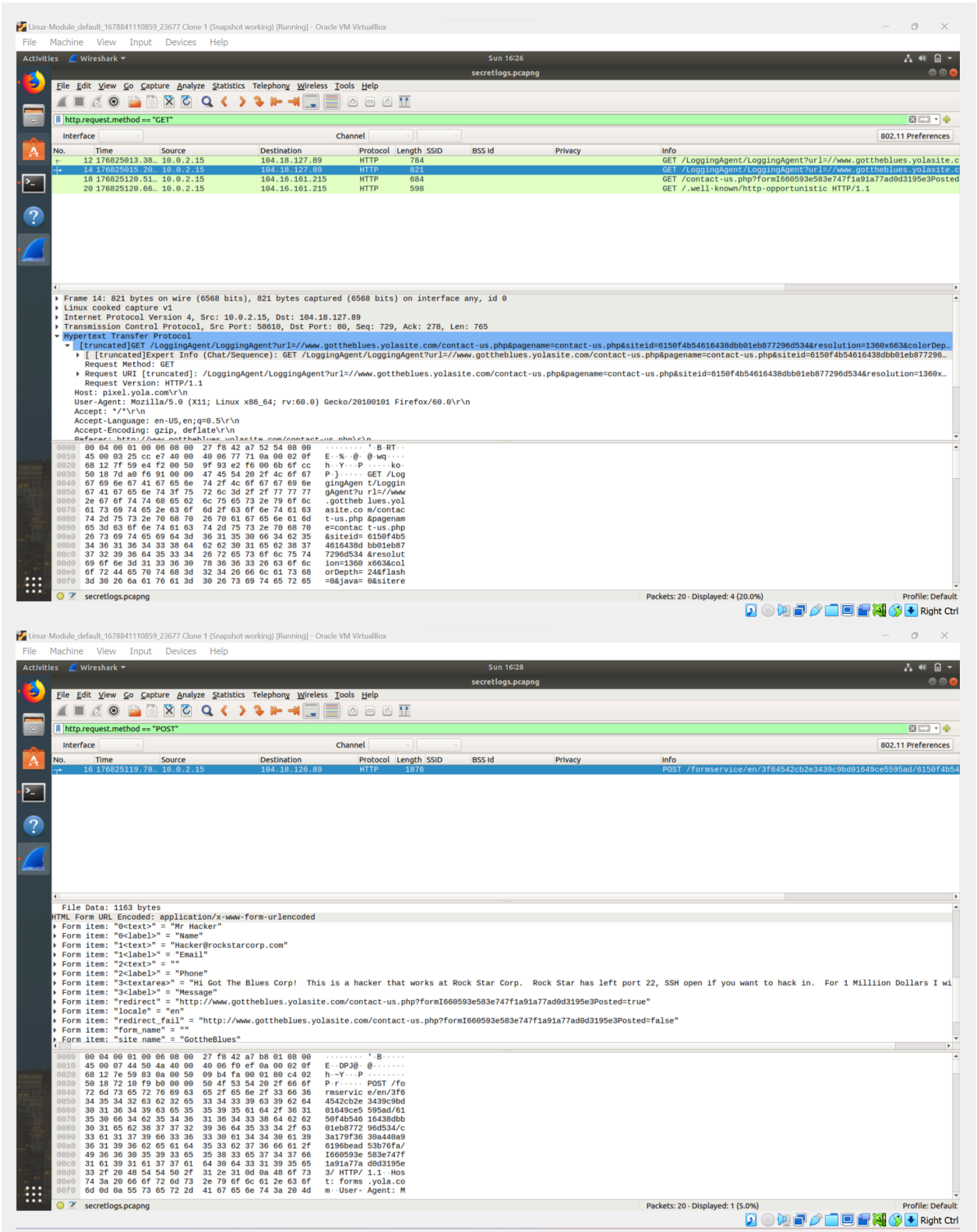
When using SSH again to go back into jimi's log on we navigate to the etc/packetcaptureinfo.txt we see the following link https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
From that link we were able to see the file secretlogs.pcapng which opened up a file in wireshark.

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

The MAC address found is 00:0c:29:1d:b3:b1



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



```
Using the http findings, we were able to see that a request for 1 million
dollars was being made by the hacker who works at Rockstar Corp.
```

4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

```
The OSI layer used for HTTP is the Application layer (layer 7)
```

    b. Layer used for ARP:

```
The OSI layer used for the ARP is the data link layer (layer 2)
```

5. Mitigation suggestions (if needed):

```
Port 22 should be closed and IP addresses should be converted back to the
original. Rockstar Corp should also create password policies so that each
employee has a unique username and password that will enhance security.
Notifications should be established for all logs and these should be
reviewed regularly and any user that is able to SSH should appear in the
logs.
```