**PHASE 1.**

Hollywood Database Server IP address pings

Only IP address to give a response is

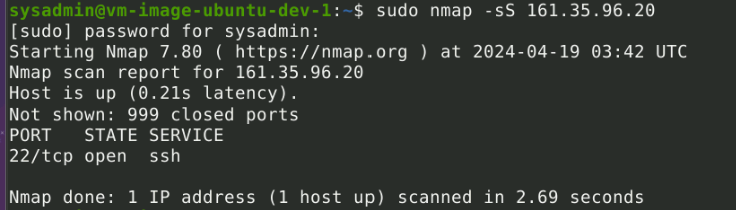
“Hollywood Application Server 1” @ 161.35.96.20

Command used to ping: ping 161.35.96.20

The OSI layer that ping works on is the **Network** layer.

**PHASE 2.**

Command used: sudo nmap -sS 161.35.96.20 *(sudo used as root privileges required)*



**This shows that port 22 is open with ssh service**

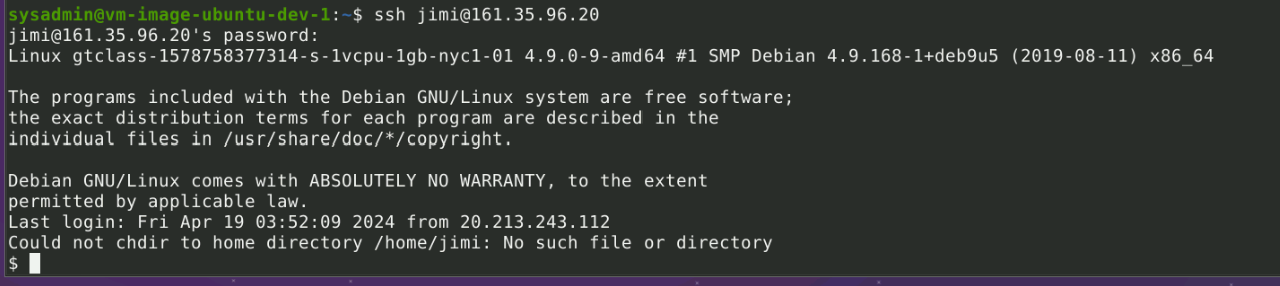
**PHASE 3.**

Username: jimi

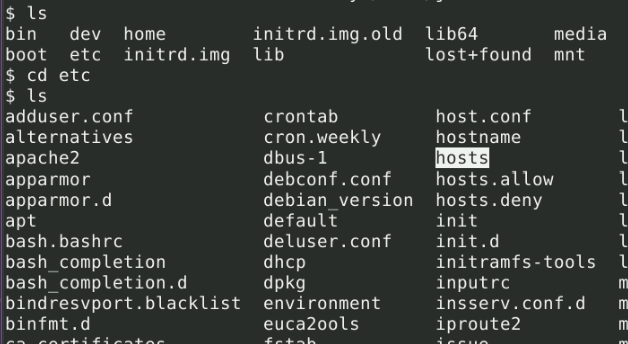
Password: hendrix

Command used: ssh jimi@161.35.96.20

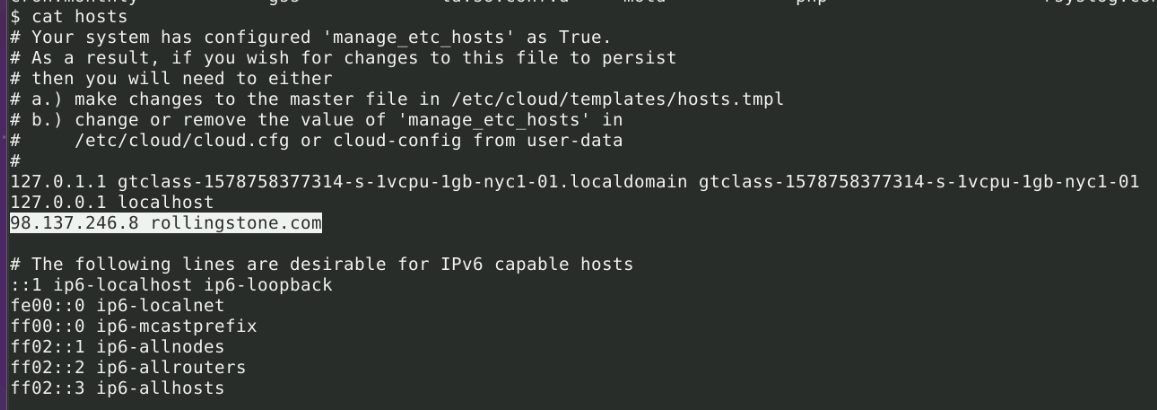
This prompted me to confirm connection, I entered yes, then was asked for password, I entered hendrix, which gave me root privileges.



From here I could navigate to the etc directory, and found a file named “hosts”



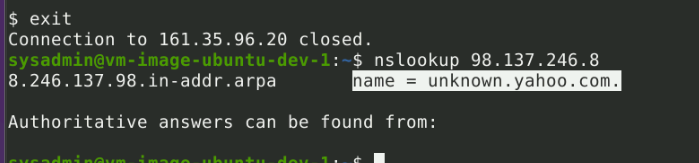
To view file contents I ran command: cat hosts



**Which showed rollingstone.com IP address as: 98.137.246.8**

I then closed the session by typing command: exit

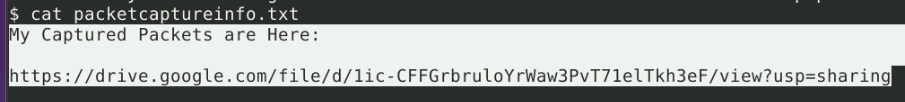
I ran the nslookup command: nslookup 98.137.246.8



Which shows as name = unknown.yahoo.com.

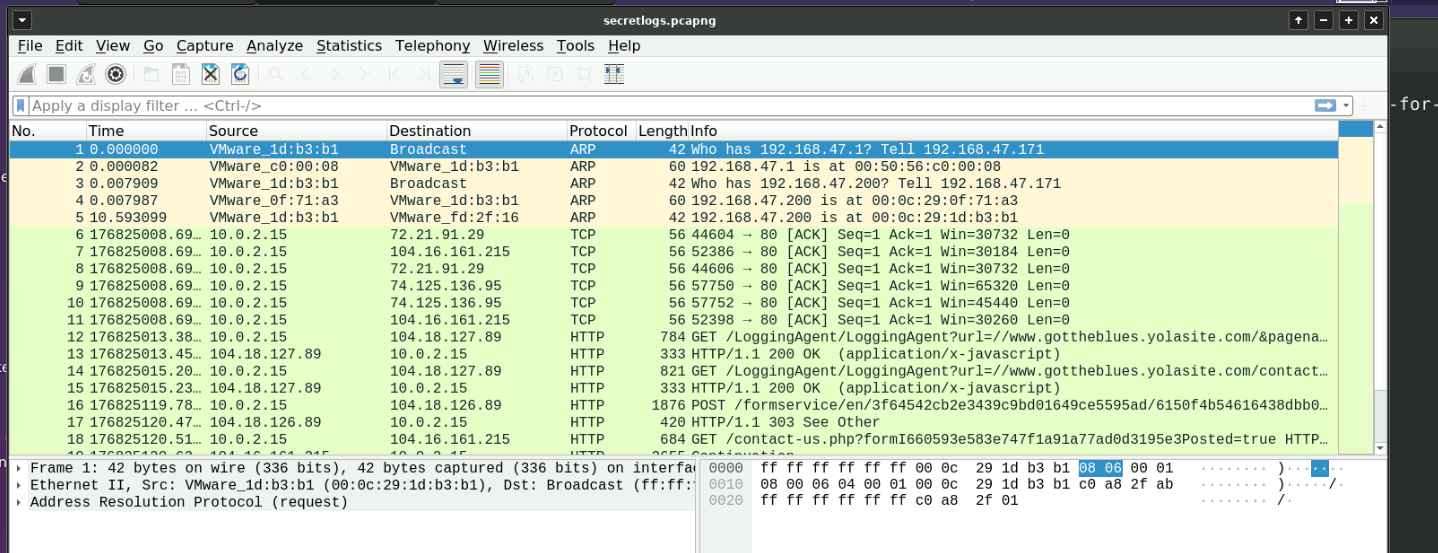
**PHASE 4.**

After ssh back into Rockstar server and navigating to the etc directory, I found the packet capture file. Ran the contents of the file and got the link below.



<https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing>

**Leads to secretlogs.pcapng which opens with Wireshark.**



Upon examining the contents of this log, **found that the hacker sent an email**

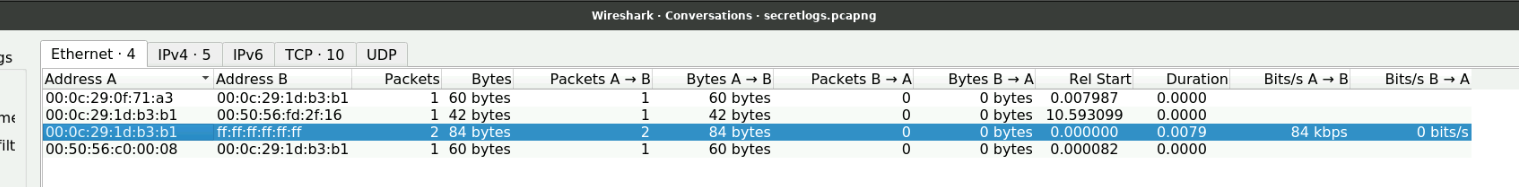
*Name: Mr Hacker*

*Email:* [*Hacker@rockstarcorp.com*](mailto:Hacker@rockstarcorp.com)

*Body:*

*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.*

To find the hacker MAC address, I went to Statistics –> Conversations. I can see there is one line that has 2 packets, which means broadcast and response.



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

**QUIZ**

