Phase 1: "I'd like to Teach the World to *Ping*"

- Entered the command: fping 167.172.144.11 15.199.95.91 15.199.94.91 11.199.158.91 11.199.141.91 to determine which IP is accepting connections. Results shown below:

- 167.172.144.11 is alive
  15.199.95.91 is unreachable
  15.199.94.91 is unreachable
  11.199.158.91 is unreachable
  11.199.141.91 is unreachable

- After running the fping command, it's determined most of the Hollywood offices don't accept connections. Except for IP address 167.172.144.11, which is one of the Hollywood Application Servers. This finding falls under Layer 3 (Network) of the OSI model as it retains to the IP addresses.

Phase 2: "Some of *Syn* for Nothin'"

- Ran the command: nmap -sS 167.172.144.11 to determine which ports are open. Results shown below:

- PORT STATE SERVICE
  22/tcp open ssh
  25/tcp filtered smtp
  135/tcp filtered msrpc
  139/tcp filtered netbios-ssn
  445/tcp filtered microsoft-ds

- Based on the results above, port 22/tcp is open on the Rockstar Corp Server. With this port open and accepting connections, a hacker can use this vulnerability to access Rockstar Corp's data. The SYN scans fall under Layer 4 (Transport) of the OSI model as it scans the transport protocols.

Phase 3: "I Feel a *DNS* Change Comin' On"

- To log onto the Rockstar sever, ssh jimi@167.172.144.11 is the command used with the given password hendrix.
- Next, I navigated to the etc directory with cd etc then nano hosts to determine what entry is set for rollingstone.com. Entry shown as: 98.137.246.8 rollingstone.com
- The command used to find which domain is associated with the above IP: nslookup 98.137.246.8. Results shown below:
- 8.246.137.98.in-addr.arpa name = unknown.yahoo.com

- While logged into the Rockstar server, the hosts file entry for rollingstone.com is set to ip address 8.246.137.98, which is not the correct IP for rollingstone.com. Hence, the reason why Rockstar Corp cannot access the website. Another vulnerability found is the Rockstar Corp's login, as it's the same default password across the site. This falls into layer 7 (Application) of the OSI Model.

Phase 4: "Sh*ARP* Dressed Man"

- While in the Rockstar Server, I listed all files under the etc directory with command ls and found a file named packetcaptureinfo.txt. Next command used to see its content was cat packetcaptureinfo.txt. Results shown below:
- https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
- Once the packet capture was downloaded and analyzed through Wireshark, the ARP filter revealed line 5 having a duplicate IP address. Along with the HTTP filter, showing line 16 is a POST HTTP. Findings associated to a hacker was the name "Mr Hacker", and email Hacker@rockstarcorp.com. Additionally, they left a note revealing they are a Rockstar Corp employee and stated the port 22 SSH was open if anyone wanted to hack in. This finding falls under both the Data Link layer (ARP) and Application Layer (HTTP).