DIRECTIONS:

1. List the steps and commands used to complete the tasks.
2. List any vulnerabilities discovered.
3. List any findings associated to a hacker.
4. Document the mitigation recommendations to protect against the discovered vulnerabilities.
5. Document the OSI layer where the findings were found.

PHASE 1:

1. IP ranges for Hollywood offices:

15.199.95.91

15.199.94.91

11.199.158.91

167.172.144.11

11.199.141.91

fping -s 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91

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

1. RockStar Corp advised that they don’t want to respond to any requests, and since 167.172.144.11 is responding, this is a potential vulnerability.
2. Mitigation recommendations: restrict allowing ICMP echo requests against IP 167.172.144.11 to prevent successful responses from PING requests.
3. These findings occurred in the Network Layer.

PHASE 2:

1. Sudo nmap -sS 167.172.144.11/32
2. The results show that Port 22 is in an Open state (service: ssh); Port 22 is accepting connections.
3. SYN uses TCP, TCP is connection based, which means that this occurred in the Transport Layer.

PHASE 3:

ssh jimi@167.172.144.11 -22

ping rollingstone.com

sudo nano hosts

nano hosts

add to the nano file under localhost IP: 98.137.246.8 rollingstone.com

nslookup

name = unknown.yahoo.com

DNS runs in the Application Layer (Layer 7).

PHASE 4:

Hacker file found in: packetcaptureinfo.txt

cat packetcaptureinfo.txt

“ https://drive.google.com/file/d/lic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing “

Open this link in VM internet browser

File secretlogs.pcapng

Open in Wire Shark

Filter for the ARP only files

First line of the ARP files:

* Line 4 shows MAC address 00:0c:29:0f:71:a3
* Line 5 shows MAC address of 00:0c:29:1d:b3:b1
* Line 5 is a “spoofed” MAC address

Filter for only HTTP files

Line 16 of the HTTP files shows “POST” from hacker on website, including information such as:

* Mr Hacker
* [Hacker@rockstarcorp.com](mailto:Hacker@rockstarcorp.com)
* 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 wi…
* site\_name GottheBlues

This occurred in the Application Layer (Layer 7).