**### \*\*Phase 1\*\*: *\_"I'd like to Teach the World to `Ping`"\_***

- Command used for all Hollywood IP addresses provided on the linux terminal: **fping -s -g [IP address]**

- The IP addresses that are not accepting connections are **15.199.95.91/28, 15.199.94.91/28, 11.199.158.91/28,** and **11.199.141.91/28.** The IP address that is accepting connections is **167.172.144.11/32.**

- Vulnerability discovered is that a successful connection was made to one of the Hollywood office’s IP address.

- A way to mitigate this issue to block ICMP requests.

- This finding is in layer 3, the Network layer, as its key protocol is IP Addresses.

**### \*\*Phase 2\*\*: *\_"Some `Syn` for Nothin`"\_***

- Command used: **sudo nmap -sS 167.172.144.11**

- The results show that port 22 is open and therefore a connection to this computer can be successful.

- The vulnerability to this finding is that a hacker may successfully connect to this IP address to exploit the company.

- To mitigate the company should limit the users SSH access.

- Syn scans run on layer 4, transport layer, as an open SSH port allows two computers to communicate.

**### Phase 3: *\_"I Feel a `DNS` Change Comin' On"\_***

- Command used:

o **ssh jimi@167.172.144.11**

o **cd /etc**

o **cat hosts**

o **nslookup 98.137.246.8**

- When logged into the compromised server we see that the hosts file was configured and shows that rollingstone.com has been spoofed and is being redirected to a different IP address 98.137.246.8 which is an unknown yahoo page.

- Vulnerability found is possible DNS spoofing.

- Possible mitigation is to constantly check the DNS server to check if its being compromised, also restricting access to hosts file therefore configuration of file will not be allowed/

- OSI layer is application layer 7 as it is a web application being accessed.

**### Phase 4: *\_"Sh`ARP` Dressed Man"\_***

- Command used:

o **ssh jimi@167.172.144.11**

o **cd /etc**

o cat packetcaptureinfo.txt

o sudo wireshark

§ checking ARP

using arp.opcode == 2

3 packets show up and duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)

o filter to see if hacker sent out communication

o http.request.method == "POST"

o HTML Value: 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 Milliion Dollars I will provide you the user and password!

o **http://www.gottheblues.yolasite.com/contact-us.php\r\n**

- We were able to locate the packet captures in the user’s directory, we know that the hacker is person from within the company who is willing to give access to an outside hacker for compensation.

- Vulnerability found is possible ARP poisoning attacks.

- Possible way to mitigate against ARP poising attacks is by creating static ARP entries in the server to reduce the risks.

- OSI layer is layer 2 and layer 7. Layer 2 is the data link layer which establishes links between nodes and ensures data gets to final destination primary protocols at MAC addresses and ARP. Layer 7 is the application layer which represents data to be understood by an individual interacting with it.