\*\*Phase 1\*\*

I broke down the IP Ranges using an online calculator tool and determined the ranges and fpinged them using:

fping -s -g <start\_of\_range end\_of\_range> for the following IP ranges.

15.199.95.81 - 15.199.95.94

15.199.94.81 - 15.199.94.94

11.199.141.81 - 11.199.141.94

167.172.144.11

11.199.158.81 - 11.199.158.94

With fping, the 167.172.144.11 IP address is the only one that returned as active which is one of the Hollywood Application Servers.

Rockstar could stop this by not allowing that ip address to respond to pings

This vulnerability is on the network layer of the osi model which is layer 3.

\*\*Phase 2\*\*

Running “sudo nmap -sS 167.172.144.11” gave me the result of port 22 open.

The hacker can use this to gain access to secure areas of the network and deploy packages without Rockstar knowing.

One way to stop this would to be to go in and turn off port 22 on the network and make sure that the hacker did not leave anything to continue remote access with.

These types of attacks typically happen on the application layer which is layer 7 on the osi model.

\*\*Phase 3\*\*

ssh jimi@167.172.144.11

Cd /etc

Cat hosts

Exit

Nslookup 98.137.248.8

From there you can see that some changed the ip of rollingstone.com to unknown.yahoo.com. Changing this will give the hacker the ability to steal confidential information.

This would be a dns highjacking vulnerability which occurs at layer 5

\*\*Phase 4\*\*

Ssh back into jimi

Cd /etc

Cat packetcaptureinfo.txt

Open the google doc.

Download and open the pcap file

Arp filter

In packet 5 there was a duplicate ip that had a mac address of 00:0c:29:1d:b3:b1 and was trying to look like the original which was 00:0c:29:0f:71:a3

Http filter

In packet 115 there you can see there was a text post made by a “Mr Hacker” asking for 1 million dollars to give Got The Blues Corp the username and password to hack into the system.

To fix this I would suggest finding the employee that is on the device with the mac address ending in b1 and fire them then close the port.

This would be an example of DNS poisoning which is on layer 5.