**Homework 8**

**Phase 1**

Determined the IP ranges to scan were **15.199.95.80** and **15.199.95.95,**

**fping -c 4 -g 15.199.95.80 15.199.95.95**  
 4 packets transmitted, 0 received, 100% loss

Determined the IP ranges to scan were **15.199.94.80** and **15.199.94.95**,

**fping -c 4 -g 15.199.94.80 15.199.94.95**  
 4 packets transmitted, 0 received, 100% loss

Determined the IP ranges to scan were **167.172.144.11**

No ranges of IPs.Only one ip address, all bits are taken.

**ping -c 4 167.172.144.11**  
 4 packets transmitted, 4 received, 0% loss

Since Rockstar doesn't want to respond, this IP address being open is considered to be vulnerable.

The vulnerability occurred on the network layer.

We can **filter (using firewall)** the ip address to restrict access.

Determined the IP ranges to scan were **11.199.141.80** and **11.199.141.95**,

**fping -c 4 -g 11.199.141.80 11.199.141.95**  
 4 packets transmitted, 0 received, 100% loss

Determined the IP ranges to scan were **15.199.95.80** and **15.199.95.95**,

**fping -c 4 -g 15.199.95.80 15.199.95.95**  
 4 packets transmitted, 0 received, 100% loss

**Phase 2**

**sudo nmap -sS 167.172.144.11**

Not shown: 995 closed ports

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

Port 22 is open.The status (open/closed) of the ports were found at layer 4 (transport layer).

**Phase 3**

Accessing the ip address: **sudo ssh jimi@167.172.144.11** password hendrix

**nano etc/host**

Rollingstone.com ip address was changed into **98.137.246.8**

**Exit** from ssh session

**nslookup** **98.137.246.8**

8.246.137.98.in-addr.arpa name = unknown.yahoo.com.

Authoritative answers can be found from:

The finding was on the **application layer (layer 4).**

**Phase 4**

**sudo ssh jimi@167.172.144.11 password: hendrix**

**cd etc, ls etc**

**cat packetcapturerinfo.txt**

[**https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing**](https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing)

**Open With wireshark**

Filter using **arp.opcode==2**

Findings: [**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)]

The suspicious activity was found on the data **link layer (layer 2).**