PHASE ONE: _"I'd like to Teach the World to `Ping`"_

- fping –s 15.199.95.91 (Hollywood Database Servers)
- IP is unreachable
- fping –s 15.199.94.91 (Hollywood Web Server)
- IP is unreachable
- fping –s 11.199.158.91 (Hollywood Web Servers)
- IP is unreachable
- fping –s 11.199.141.91 (Hollywood Application Servers)
- IP is unreachable
- fping –s 167.172.144.11 (Hollywood Application Servers)
- IP is alive
- These findings occur in Layer 3: Network of the OSI model.
- VULNERABILITY: Rockstar does not want anyone seeing that their servers are accepting connections. This could lead to a hacker spoofing one of them and collecting data.
- MITIGATION: restrict ICMP echo requests on the server. Hide the servers

PHASE TWO: _"Some `Syn` for Nothin`"_

- Sudo nmap –sS 167.172.144.11
- Port 22/tcp is open with 999 filtered ports

- This occurs in Layer 4: Transport of the OSI model
- VULNERABILITY: This tells us that SSH is on PORT 22 and exposes teh system to hacking.
- MITIGATION: secure the ports, make it so they cannot be seen. You can also attach the SSH conection to a diffeent port

PHASE THREE: _"I Feel a `DNS` Change Comin' On"_

- sudo ssh jimi@167.172.144.11 with password hendrix
- Cat /etc/hosts
- 127.0.0.1 localhost and 98.137.246.8 rollingstone.com
- I ran the nslookup rollingstone.com and found the following
    - Address is 151.101.0.69
    - Address is 151.101.192.69
    - Address is 151.101.64.69136.
    - Address is 151.101.128.69
- Doing an nslookup occurs in Layer 7, Application.
- VULNERABILITY: Modifying the IP source address can make the hacker appear to be a trusted source to send packets to.
- MITIGATION: DHCP Snooping, a network switch which inspects packets to confirm they are legit.

PHASE FOUR: _"Sh`ARP` Dressed Man"_

- sudo ssh jimi@167.172.144.11 with password hendrix
- cd /etc and then cat packetcaptureinfo.txt which gave us a link to the packets
- put the packet secretlogs.pcapng
- Packet 5 shows an indication of ARP Spoofing, it shows duplicate IP addresses in use for 192.168.47.200. This disguises the hackers IP address for them to do malicious stuff.
- This step and the vulnerability occurred in Layer 2, Data Link.
- VULNERABILITY: ARP Spoofing
- MITIGATION: Switch security and network isolation are some tactics.