**Networking Fundamentals Homework: Rocking your Network!**

**Phase 1**: "I'd like to Teach the World to *Ping*"

 The steps and commands used to complete the tasks.

Hollywood Database Servers:

fping -c 4 -g 15.199.95.91 15.199.95.106

Hollywood Web Servers

fping -c 4 -g 15.199.94.91 15.199.94.106

Hollywood Web Servers

fping -c 4 -g 11.199.158.91 11.199.158.106

Hollywood Application Servers

fping -c 4 167.172.144.11

Hollywood Application Servers

fping -c 4 -g 11.199.141.91 11.199.141.106

 A summary of your findings for each testing phase.

The Hollywood Application Server on IP 167.172.144.11 is active with 0% loss

 Any network vulnerabilities discovered.

RockStar Corp does not want any reposes so there is a vulnerability on IP 167.172.144.11

 Recommended mitigation strategy.

Restrict allowing ICMP echo requests against IP 167.172.144.11 to prevent successful responses from PING requests.

 Document the OSI layer where the findings were found.

Network layer

**Phase 2**: "Some *Syn* for Nothin`"

 The steps and commands used to complete the tasks.

sudo nmap -sS 167.172.144.11

 A summary of your findings for each testing phase.

Port 22/tcp is in an open state with a ssh service

 Any network vulnerabilities discovered.

Having an Open Port is a vulnerability as RockStar Corp does not want any of their servers to be accepting any connections.

 Recommended mitigation strategy.

RockStar Corp would want to close Port 22 or at least set up a firewall.

 Document the OSI layer where the findings were found.

Transport layer

**Phase 3:** "I Feel a *DNS* Change Comin' On"

 The steps and commands used to complete the tasks.

ssh jimi@167.172.144.11 -p22 is used to log into the server with the password Hendrix.

Then cd etc and then nano hosts to see what IP address is associated with Rolling Stone.

nslookup 98.137.246.8

 A summary of your findings for each testing phase.

98.137.246.8 rollingstone.com

nslookup 98.137.246.8 redirects to an ‘unknown.yahoo.com’ site.

 Any network vulnerabilities discovered.

The DNS cache had been changed for rollingstone.com with an IP address that routed RockStar employees to a different site.

 Findings associated with a hacker.

The manual changes to the DNS cache signs of a hacker infiltrating the server in a form of DNS Hijacking.

 Recommended mitigation strategy.

Manually fix the cache for the rollingstone.com in etc/hosts/ and installing a firewall.

 Document the OSI layer where the findings were found.

Application

**Phase 4:** "Sh*ARP* Dressed Man"

 The steps and commands used to complete the tasks.

nano packetcaptureinfo.txt

Captured Packets are here:

<https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing>

connected to site and downloaded packet: secretlogs.pcapng.

 A summary of your findings for each testing phase.

There is a duplicate IP address detected for 192.168.47.200 which is a potential indicator of an ARP poisoning attack.

 Any network vulnerabilities discovered.

Possible ARP poisoning attack.

 Findings associated with a hacker.

Possible ARP poisoning attack where attackers attempt to insert a malicious server into the ARP cache to steal traffic intended for another server.

 Recommended mitigation strategy.

Create a static ARP entry in the correct server can reduce the risk of ARP poisoning as well as monitoring with third party tools.

 Document the OSI layer where the findings were found.

Network