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

Phase 1:

* fping -g 167.172.144.11/32 is alive
* fping -g (all other IPs / one at a time)
* IPs : 15.199.95.91/28 15.199.94.91/28 11.199.158.91/28 11.199.141.91/28 are not responding
* IP 167.172.144.11 is alive
* OSI Layer 3 Network

Phase 2:

* sudo nmap -sS 167.172.144.11

Starting Nmap 7.60 ( https://nmap.org ) at 2021-04-21 23:20 EDT

Nmap scan report for 167.172.144.11

Host is up (0.0014s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE  
 22/tcp open ssh

* open port 22 is a vulnerability
* OSI Layer 4 Transport

Phase 3:

* ssh jimi@167.172.144.11 password: hendrix
* found hosts file under /etc on jimi
* opening the hosts file lists 98.137.246.8 rollingstone.com
* nslookup 98.137.246.8 -- name = unknown.yahoo.com does not start with media-
* Hacker - using same credentials --- Change passwords to mitigate
* OSI Layer 7 Application

Phase 4:

* back into ssh jimi@167.172.144.11 password: hendrix
* cd into the /etc to find packetcaptureinfo.txt
* cat or less the file to get Captured Packets are here:

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

* arp
  + When running arp 192.168.47.171 have the same IP but different MAC addresses
  + This is suspicious, also after line 4, the time response is 10 seconds?
* http
  + 10.0.2.15 is talking to 104.18.126.89
  + This was the found info --- Mr Hacker - [Hacker@rockstarcorp.com](mailto:Hacker@rockstarcorp.com) - 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!
  + Port 22 was left open and should be closed to prevent this
* OSI Layer - ARP 2 and 3 - HTTP Layer 7