John Sowers - Homework 08

Phase 1

* First I converted Rockstarserverlist.xlxs to Rockstarserverlist.**csv** format using google docs. To find which IP addresses were accepting connections I ran the following:
  + **awk -F "/" '{print $1}' ~/Homework08/Rockstarserverlist.csv | fping**
* I found that IP address **167.172.144.11** is potentially vulnerable because it was the only one that responded
* To mitigate this vulnerability I recommend restricting IMCP echo requests to 167.172.144.11 to prevent responses to pings
* This vulnerability occurs on **Layer 3 : Network** due to this being an issue with IP addresses

Phase 2

* To find open ports on **167.172.144.11** I ran the following:
  + **sudo nmap -sS 167.172.144.11**
* I found that port **22/tcp** is open for ssh
* This functions on **Layer 4: Transport** since it has to do with ports

Phase 3

* The following commands are what I used to get information about **rollingstones.com**
  + **ssh jimi@167.172.144.11**
  + **cat /etc/hosts**
* I found that rollingstones.com IP address is routed to **98.137.246.8**
* I then exited RockStars servers and found more information about that IP address
  + **logout**
  + **nslookup 98.137.246.8**
* The results show that the owner of that IP address is routed to domain : **unknown.yahoo.com**
* This information is found on **Layer 7: Application** since nslookup is an application finding domain names

Phase 4

* To find the .pcap file I used the following command:
  + **cat /etc/packetcaptureinfo.txt**
* After downloading the file (curl or wget would not work had to use a browser) I opened it with Wireshark
* Packet 5 indicates an employee set up a man in the middle attack with ARP poisoning and intercepted network traffic (likely found jimi hendrix since that is the the login information that was sold later)
  + The attacker’s IP and MAC address at the time were Duplicate 192.168.47.200 (00:0c:29:1d:b3:b1)
  + This attack happened at OSI **Layer 2: Data Link** since it was an ARP attack
* Packet 16 shows a post to **forms.yola.com** with information about how information was leaked:
  + Email : [Hacker@rockstarcorp.com](mailto:Hacker@rockstarcorp.com)
  + This person is an employee at rockstar who sold information on open ports, user names, and passwords for 1 Million dollars
  + This attack was at **Layer 7: Application** since information was leaked via website