**Unit 8 Homework**

### Your Goal

You will follow instructions to work through four phases of the network assessment. For each phase, include the following:

* The steps and commands used to complete the tasks.
* A summary of your findings for each testing phase.
* Any network vulnerabilities discovered.
* Findings associated with a hacker.
* Recommended mitigation strategy.
* Document the OSI layer where the findings were found.

**Phase 1**

1. Create a summary file in a word document that lists out the fping command used, as well as a summary of the results:

* fping -g 15.199.95.91/28
  + Result: Unreachable
* fping -g 15.199.94.91/28
  + Result: Unreachable
* fping -g 11.199.158.91/28
  + Result: 167.172.144.11 is alive, the rest are unreachable
* fping -g 167.172.144.11/32
  + Result: Unreachable

To fping all of the Hollywood office IP ranges, I did the following command:

fping -g <IP Range>

Based on the results, there was only one IP address that was alive, 167.172.144.11. The rest of the IP addresses were unreachable as they are supposed to be. To remedy this, the proper ports need to be closed. This does not mean that this is a hack as it could just have been improperly configured. The layer that this was found was Layer 3 (Network).

**Phase 2**

The command that I used to perform a SYN SCAN was: sudo nmap -sS 167.172.144.11. Based on the scan, Port 22 is open when it should be closed. Still, this does not necessarily mean that there is a hacker as it could have just been a misconfiguration. The layer that this was found was Layer 4 (Transport).

**Phase 3**

The command that I used to login to the RockStar server was:

* sudo ssh [jimi@167.172.144.11](mailto:jimi@167.172.144.11)

Then, once inside, I used the following command to search for rollingstone.com:

* Grep -r rollingstone.com

Here, I found:

* hosts:98.137.246.8 rollingstone.com

Then, I did the following command to display the host file which provided an IP address of 98.137.246.8:

* cat /etc/hosts

To nslookup the IP address I did the following command:

* nslookup 98.137.246.8

Going through this assessment, I was able to find that the host file had been altered to 98.137.246.8. After doing the nslookup on the IP, I found that the domain was unknown.yahoo.com. The recommendation is now to correct the IP address and close Port 22. It does seem that this was modified, so this does seem like a hacker. The layer at which nslookup is Layer 7 (Application).

**Phase 3**

To find the packet capture information, I did the command:

* cat packetcaptureinfo.txt

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Based on my investigation of the pcap file found from the hacker, it appears that there is ARP Spoofing and a Man in the middle attack. There is a duplicate IP address detected for 192.168.47.200 and a logging agent redirect. My recommendation is to close Port 22, correct the IP address in the host file, and make sure to use a Static ARP. The layer at which Wireshark operates at is Layer 2 (Data Link Layer).