**HW 8**

**C Spencer**

**Phase 1**

It was determined the appropriate IP ranges to scan were the IP addresses belonging to the Hollywood servers listed in the table below.

The **fping -s -g** command was used on the Hollywood IP address ranges in the table below to determine which, if any, are accepting connections. The only address accepting connections was the following:

167.172.144.11

The following IP address ranges were not accepting connections:

15.199.94.91/28

15.199.95.91/28

11.199.158.91/28

11.199.141.91/28

**Summary Table**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IP Range** | **Starting Address** | **Ending Address** | **Number of Targets (n)** | **Alive Targets (n)** | **Unreachable Targets (n)** | **Reachable Target** |
| 15.199.94.91/28 | 15.199.94.81 | 15.199.94.94 | 14 | 0 | 14 | None |
| 15.199.95.91/28 | 15.199.95.81 | 15.199.95.94 | 14 | 0 | 14 | None |
|  | 11.199.158.81 | 11.199.158.94 | 14 | 0 | 14 | None |
| 167.172.144.11/32 | 167.172.144.11 | 167.172.144.11 | 1 | 1 | 0 | 167.172.144.11 |
| 11.199.141.91/28 | 11.199.141.81 | 11.199.141.94 | 14 | 0 | 14 | None |

The **fping** command uses the Internet Connection Message Protocol (ICMP) which exists on L3, the Network Layer, of the OSI model. Having 167.172.144.11 accepting connections/echo requests is a potential vulnerability and it is recommended ICMP echo requests be restricted against this IP address; especially since RockStar Corp does not want any request responses.

**Phase 2**

A SYN SCAN was used to detect open ports, the state of any open ports, and the service associated with any open ports. This was performed on the entire set of IP ranges provided in the Rockstarserlist file because I did not read the instructions. The IP address ranges were copied into a text file, read into nmap, and output to a text file for analysis using the following command:

sudo nmap -sS -iL ip.txt > syn\_scan.txt

Pertinent data was extracted from syn\_scan.txt using the following command:

grep -B 5 -A 5 ‘open’ syn\_scan.txt

And resulted in the following findings:

12-205-151-1.cpe.att.net (12.205.151.1)

PORT STATE SERVICE

22/tcp open ssh

167.172.144.11  
PORT STATE SERVICE  
22/tcp open ssh

TCP operates on the L4 – Transport Layer and this is where nmap and SYN SCAN operate to detect open ports. The open ports identified indicate that Port 22 providing ssh is a potential vulnerability and should be closed to prevent network penetration by ssh connection on 167.172.144.11.

**Phase 3**The ssh vulnerability was used to connect to the server at 167.172.144.11 using the following command and credentials:

ssh jimi@167.172.144.11

jimi@167.172.144.11's password:Hendrix

/etc/hosts was investigated to determine why the attempted viewing of rollingstone.com was routing to a different, unrelated site. It was discovered in the /etc/hosts file that the following IP address is mapped to rollingstone.com:

98.137.246.8 rollingstone.com

This IP address was investigated on the sysadmin account using the following command:

nslookup 98.137.246.8

This resulted in the following discovery:

8.246.137.98.in-addr.arpa name = media-router-fp72.prod.media.vip.gq1.yahoo.com.

The conclusion is that attempts to access rollingstone.com are being redirected to the yahoo.com address above for the potential theft of personal and private information or the distribution of malware. This is occurring on L7-Application Layer, where the DNS operates. It is recommended that port 22 providing ssh connections be closed to prevent network penetration and file alteration.

**Phase 4**

While investigating /etc/hosts a file named packetcaptureinfo.txt was discovered containing the following information and URL

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

Navigating to this path resulted in finding the following file:

Secretlogs.pcap

Investigating the logs in Wireshark led to the discovery of duplicate IP addresses belonging to two different MAC address as noted below:

Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3

This is indicative of ARP poisoning and IP spoofing. ARP poisoning occurs at L2-Data Link layer and HTTP spoofing occurs at the L3-Network Layer. It is recommended that any wireless communications be routed through a VPN if connections are remote, force traffic to HTTPS for secure connections, and encryption software to prevent packet sniffing, IP spoofing and ARP poisoning.