Pinging Hosts

Fping is a program that sends ICMP echo requests to network hosts. In this case, it is used to test whether a host accepts a connection.

Run sudo apt install fping to install fping if not already installed.

fping 15.199.95.91 → unreachable

fping 15.199.94.91 → unreachable

fping 11.199.158.91 → unreachable

fping 167.172.144.11 → alive

fping 11.199.141.91 → unreachable

The OSI layer is layer 3 the network layer.

Running a SYN Scan

SYN Scan against IP accepting connections to determine which are ports are accepting connections. In this case, the SSH port is accepting connections, which is strange.

sudo nmap -sS 167.172.144.11

22/tcp open ssh – open port is 22

The OSI layer is layer 4 transport layer.

NSLOOKUP

nslookup utility to query DNS records since "rollingstone.com" maybe corrupted.

- nslookup rollingstone.com – 151.101.128.69
- ssh jimi@167.172.144.11 yes hendrix
- cat/etc/hosts
- exit
- nslookup 98.137.246.8

The OSI layer is layer 7 the application layer.

Identifying the Hacker

- Ssh jimi:167.172.144.11 hendrix
- ls/etc
- cat etc/packetcaptureinfo.txt

Hacker on POST /formservice/

Hacker has MAC address of 00:0c:29:1d:b3:b1

Vulnerabilities:

1. RockStar Corp. did not want to accept any connections, and IP 167.172.144.11 accepted a connection. Therefore, it is a vulnerability.
2. After a SYN Scan was conducted the results showed that port 22 is open, which also can be a vulnerability if left open.
3. Utilizing the nslookup tool rollingstone.com returned with multiple Ips, which means there is probably some ARP poisoning going where requests for rollingstone.com are going somewhere else instead of the intended server.
4. It was confirmed that there is hacker somewhere with the MAC address **00:0c:29:1d:b3:b1** probably redirecting requests.

Recommendations:

1. Restrict ICMP echo requests against IP **167.172.144.11** to prevent any successful requests.
2. Filter port 22 to so that vulnerability cannot be exploited.
3. There are a few methods for preventing ARP attacks, but it really depends on identifying the attack (i.e., DOS, MIM, etc.):
    a. Utilizing a static ARP in the sever to prevent the issue with spoofing.
    b. IDS tools or detection tools that can send alerts in regard to suspicious activity.