**Section 1**

Command: Fping 167.172.144.11

IP 167.172.144.11 is reachable and presents a vulnerability. I recommend restricting ICMP echo requests against IP 167.172.144.11 to prevent a fping response.

fping operates on the Network layer

**Section 2**

Command: Sudo nmap -sS 167.172.144.11

Starting Nmap 7.60 ( https://nmap.org ) at 2022-02-15 12:28 EST

Nmap scan report for 167.172.144.11

Host is up (0.013s latency).

Not shown: 999 filtered ports **– *indicates 1 port was found opens and the remain 999 common ports are filtered.***

PORT STATE SERVICE

22/tcp open ssh **- *Indicated this port is open***

Nmap done: 1 IP address (1 host up) scanned in 6.08 seconds

Syn scans operate on the Transportation layer.

**Section 3**

Command: ssh [jimi@167.172.144.11](mailto:jimi@167.172.144.11)

Pw Hendrix

Cd etc

Nano hosts : found entry “98.137.246.8 rollingstone.com”

nslookup rollingstone.com – 151.101.192.69

nslookup 98.137.246.8 – unknown.yahoo.com

I was able to ssh into the Hollywood server and I determined an unknown ip address was added the to the etc/hosts file to direct any traffic for rollingstones.com to the unknown ip address. Utilizing the nslookup command I determined the rolingstone.com ip was 151.101.192.69 and the ip used(98.137.246.8) directed traffic to unknown.yahoo.com

The etc/hosts file and the ns lookup command run on the application layer.

**Section 4**

Packet 5 utilized a duplicate IP address used by 00:0c:29:id:b3:b1

Packet 16 shows a message sent by Mr. Hacker at [hacker@rockstarcorp.com](mailto:hacker@rockstarcorp.com) sent a message indicating port 22 is opena dna can be utilized to gain access to the system. The email , hacker@rockstarcorp, also indicated the hacker may have root privileges and was able to create an email to utilize while inside the system.