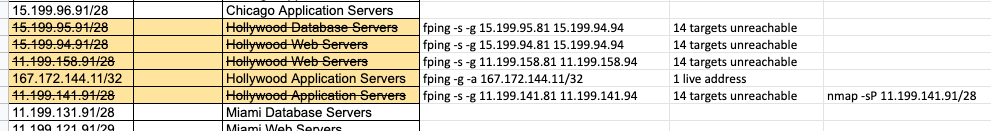
**Hayley Paul**

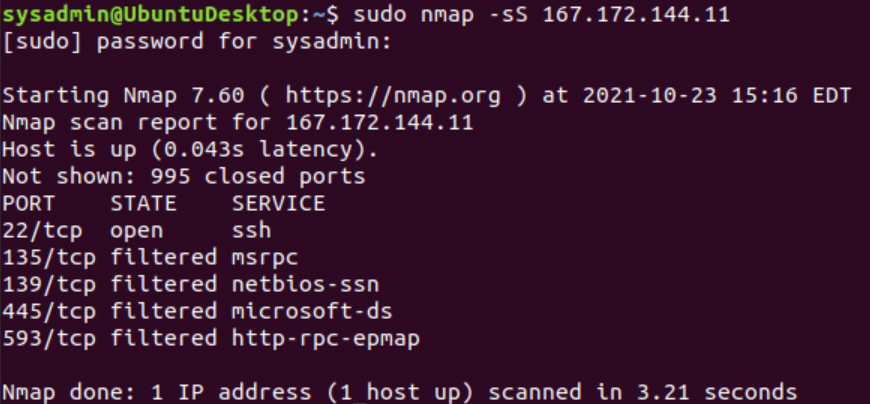
Phase 1:

Scanned using the fping command lines above the IP Addresses for the Hollywood office. I got zero reachable targets. So I used #nmap -sP 1167.172.144.11/32 and saw there was one host up.

The IP addresses crossed off are unreachable. Showing only one reachable IP.

OSI: Layer 2 and Layer 3

Phase 2:

  
I did the SYN SCAN against the open IP address. In the scan it showed that port 22 is open. You can also see in my results, four other addresses that responded.

This scan shows that Port 22 is open and accepting SSH connections. This is a security risk. My recommendation is to atleast filter if closing the port is not available.

OSI: Layer 4

Phase 3:

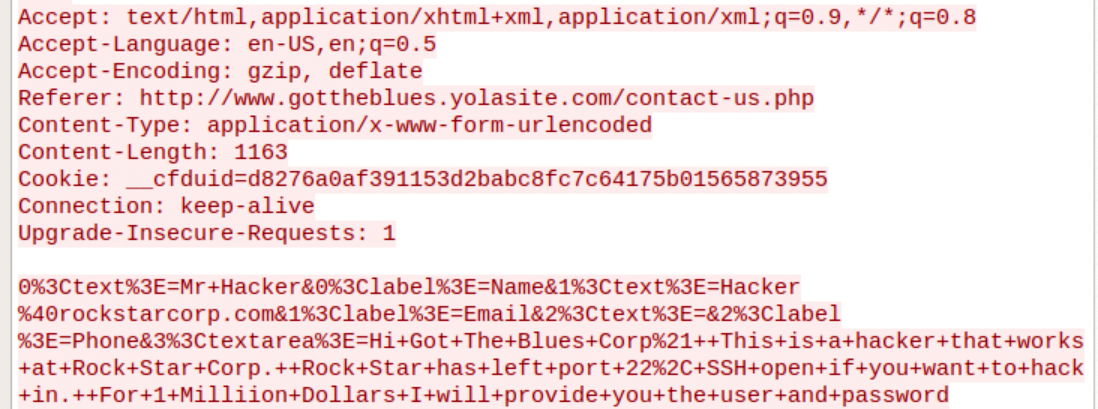
* Ran # sudo ssh jimi@167.172.144.11

Logged in with credential password given : hendrix

After going into the /etc directory, I listed the contents and found a .txt file that seemed out of place. Found a file called packetcaptureinfo.txt. Used CAT and the contents led me to a file to analyze in Wireshark.

* Once again, the network vulnerability is the open port. I’m sure any good hacker could have gained access due to the simple password.
* OSI: Layer 4

Phase 4:

* Reviewing packets in Wireshark for the secretlogs.pcap I found, I found a note in log 15. See below.

* The note is the attack vector and the Hacker is saying port 22 is open. Also that he’ll give the username/password for one million dollars.
* Findings associated with a hacker.
* The recommended strategy is closing port 22 and deny any SSH connections.
* OSI: Layer 7 because this packet’s protocol was HTTP