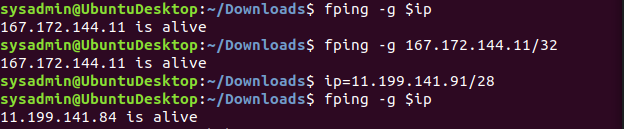
Week 8 Homework

**Phase 1: *"I'd like to Teach the World to Ping"***

You have been provided a list of network assets belonging to RockStar Corp. Use fping to ping the network assets for only the Hollywood office.

* 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**
* **fping -g 15.199.94.91/28**
* **fping -g 11.199.158.91/28**
* **fping -g 167.172.144.11/32**
* **fping -g 11.199.141.91/28**



* Your summary should determine which IPs are accepting connections and which are not.

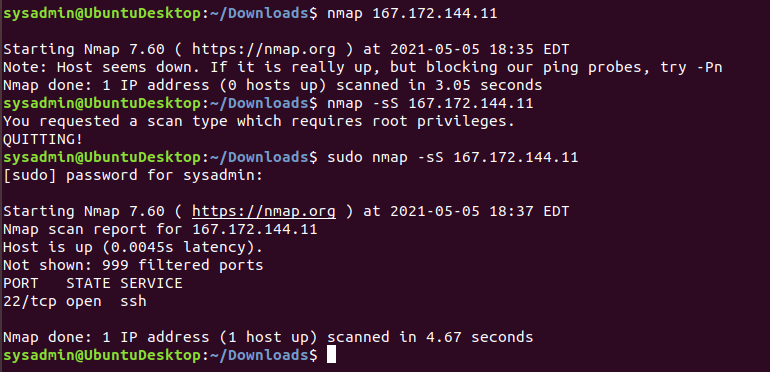
**The IP Addresses 167.172.144.11 and 11.119.141.84 are the only two ports that are open**

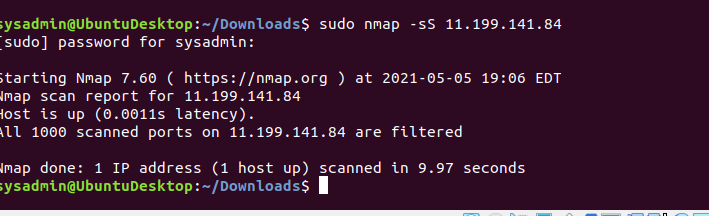
* Also indicate at which OSI layer your findings are found.

**Layer 3: Network Layer**

**Phase 2: *"Some Syn for Nothin`"***

With the IP(s) found from Phase 1, determine which ports are open:





* Using the results of the SYN SCAN, determine which ports are accepting connections.

**Sudo nmap -sS 167.172.144.11**

**Sudo nmap -sS 11.199.141.84**

* Add these findings to the summary and be sure to indicate at which OSI layer your findings were found.

**OSI layer 4: Transport layer is being used**

 The results show the port number / TCP / UDP , the state of the port, and the service / protocol for the ports that are either open or filtered (stopped by a firewall).

 Closed ports are not shown, indicated on the line: Not shown: 988 closed ports.

 For the purpose of this exercise, document which ports are open on the RockStar Corp server, and which OSI layer SYN scans run on.

**Layer 4: Transport layer**

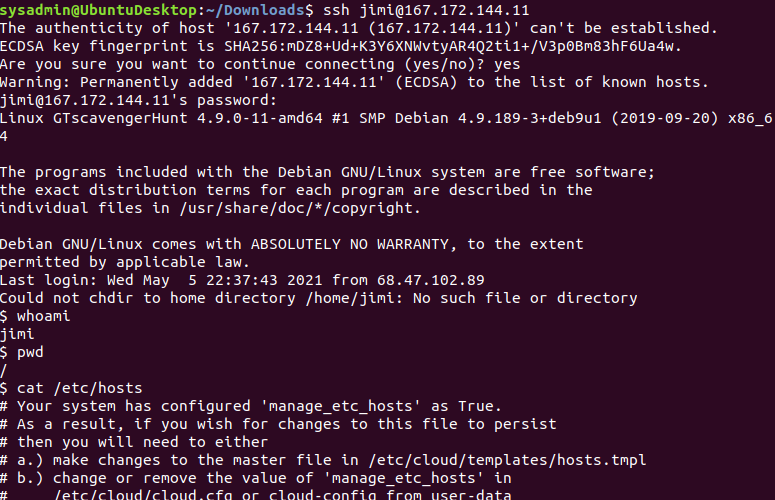
**11.199.141.84 is alive**

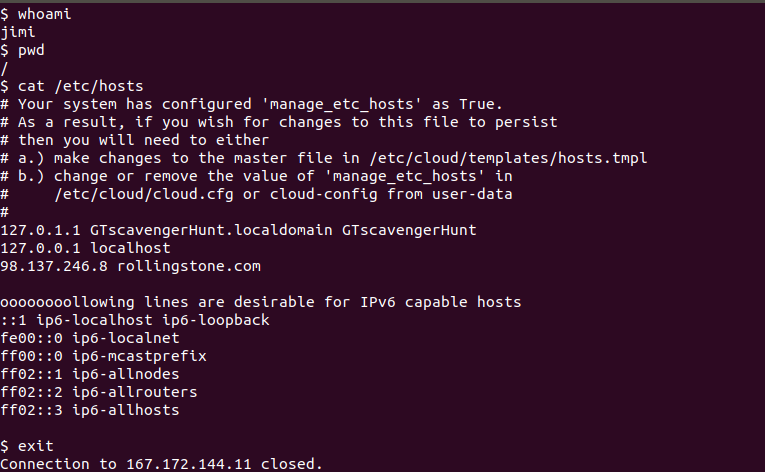
**167.172.144.11 is alive**

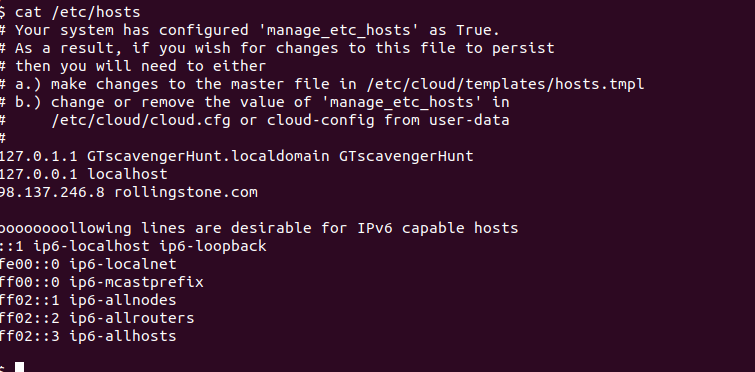
**Phase 3: *"I Feel a DNS Change Comin' On"***

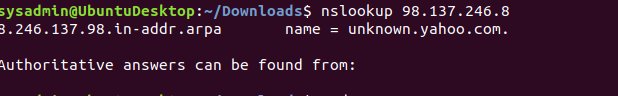
With your findings from Phase 2, determine if you can access the server that is accepting connections.

* RockStar typically uses the same default username and password for most of their servers, so try this first:
  + **Username:** jimi
  + **Password:** hendrix
* Try to figure out which port/service would be used for remote system administration, and then using these credentials, attempt to log into the IP that responded to pings from **Phase 1**.









* Add your findings to your summary and be sure to indicate which OSI layer they were found on.

\*It did not display “media” at all on the screen. We brought this up in class with Instructor John and he said it’s ok IP’s change all the time

**Layer 5: Session Layer**

**Phase 4: *"ShARP Dressed Man"***

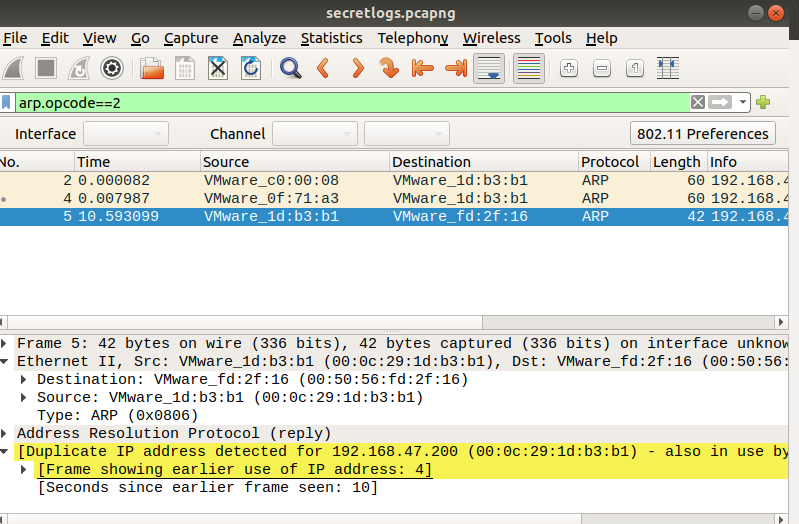
Within the RockStar server that you SSH'd into, and in the same directory as the configuration file from **Phase 3**, the hacker left a note as to where he stored away some packet captures.

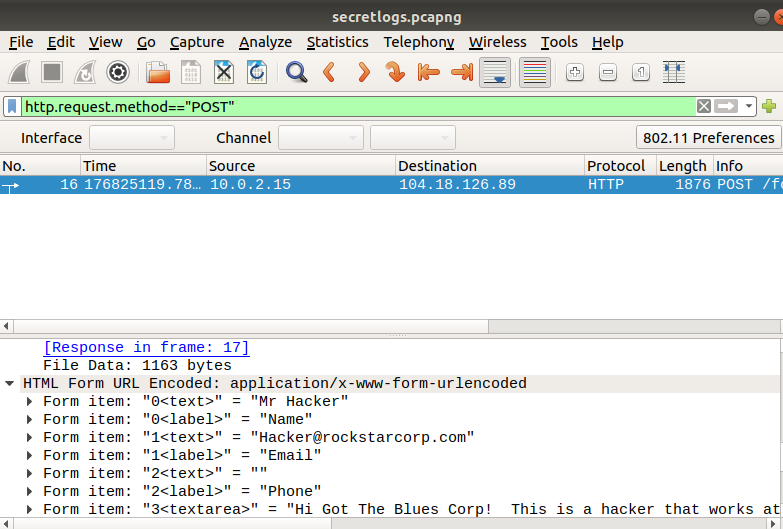
* View the file to find where to recover the packet captures.

**cd etc**

**cat packetcaptureinfo.txt**

* Use Wireshark to analyze this pcap file and determine if there was any suspicious activity that could be attributed to a hacker.
  + **Hint**: Focus on the ARP and HTTP protocols. Recall the different types of HTTP request methods and be sure to thoroughly examine the contents of these packets.





**Form item: "3<textarea>" = "Hi Got The Blues Corp! This is a hacker that works at Rock Star Corp. Rock Star has left port 22, SSH open if you want to hack in. For 1 Milliion Dollars I will provide you the user and password!"**

* Add your findings in your summary and be sure to indicate at which OSI layer they were found.

**Layer 6**