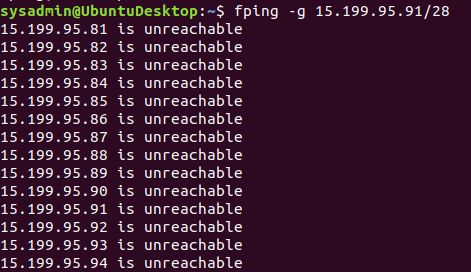
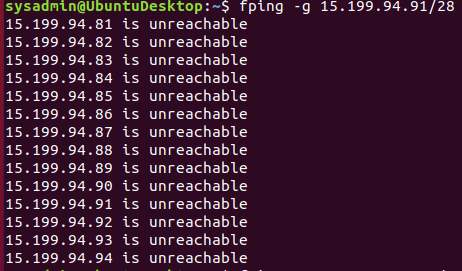
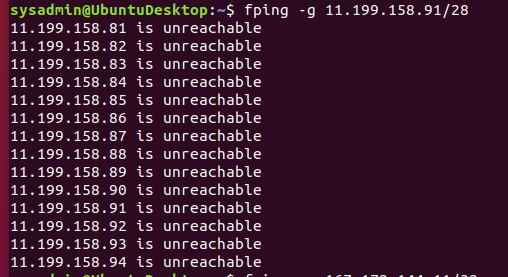
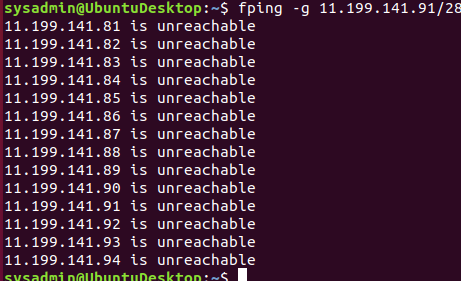
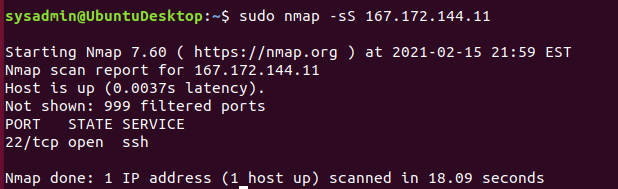
**Phase 1: *"I'd like to Teach the World to Ping"***

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.

* Determine the IPs for the Hollywood office and run fping against the IP ranges in order to determine which IP is accepting connections.
  + 15.199.95.91/28 Hollywood Database Servers
  + 15.199.94.91/28 Hollywood Web Servers
  + 11.199.158.91/28 Hollywood Web Servers
  + 167.172.144.11/32 Hollywood Application Servers
  + 11.199.141.91/28 Hollywood Application Servers
* RockStar Corp doesn't want any of their servers, even if they are up, indicating that they are accepting connections.
  + Use fping <IP Address> and ignore any results that say "Request timed out".
    - 15.199.95.91/28 Hollywood Database Servers
    - 15.199.94.91/28 Hollywood Web Servers
    - 11.199.158.91/28 Hollywood Web Servers
    - 11.199.141.91/28 Hollywood Application Servers
    - All these IPs say unreachable.
  + If any of the IP addresses send back a Reply, enter Ctrl+C to stop sending requests.
    - 167.172.144.11/32 Hollywood Application Servers
* 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 only IP accepting a connection is 167.172.144.11
* Also indicate at which OSI layer your findings are found.
  + fping works on the third layer of the OSI model by sending ICMP echo request packets and receives echo reply packets.

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

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

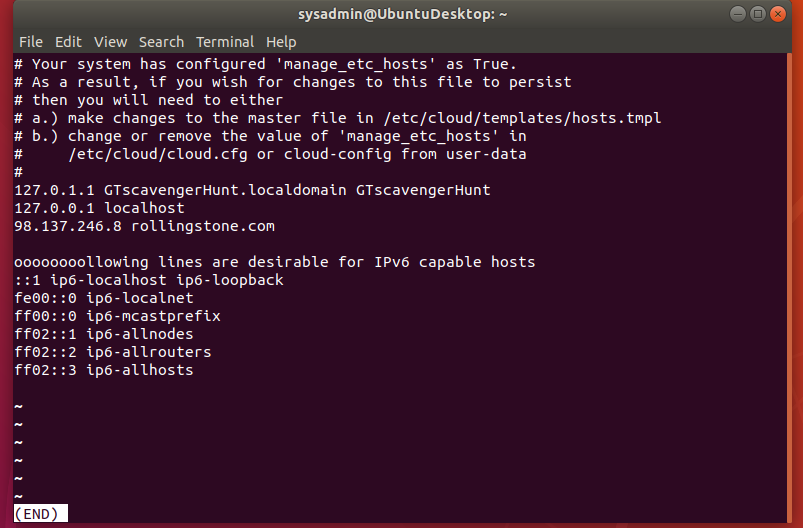
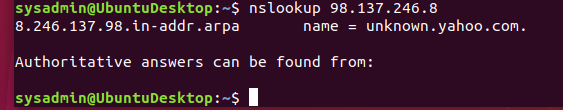
* You will run a SYN SCAN against the IP accepting connections. See **SYN SCAN Instructions** below.
  + Sudo nmap -sS
* Using the results of the SYN SCAN, determine which ports are accepting connections.
  + 
* Add these findings to the summary and be sure to indicate at which OSI layer your findings were found.
  + Nmap works on the transport layer because it uses tcp/udp to check the port

### 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.

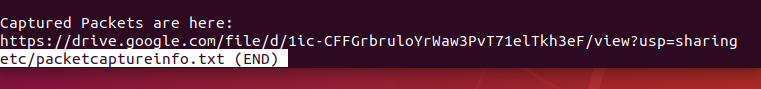
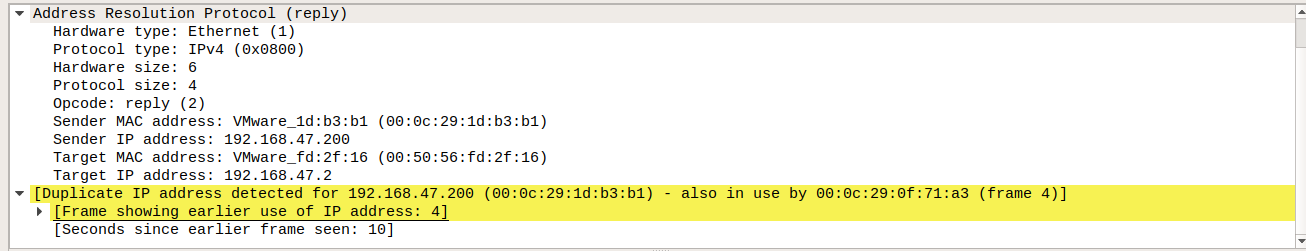
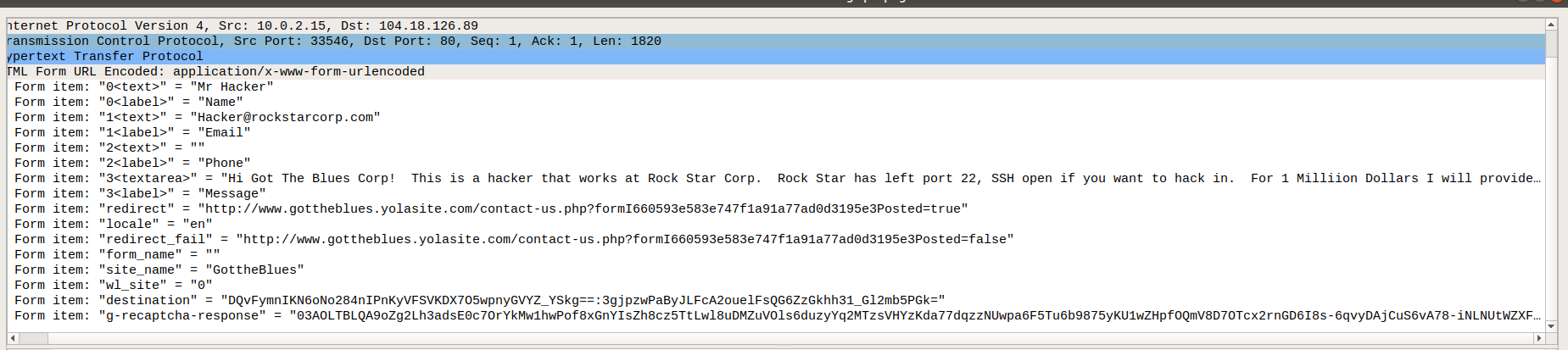
* RockStar typically uses the same default username and password for most of their servers, so try this first:
  + **Username:** jimi
  + **Password:** hendrix
* Try to figure out which port/service would be used for remote system administration, and then using these credentials, attempt to log into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

RockStar Corp recently reported that they are unable to access rollingstone.com in the Hollywood office. Sometimes when they try to access the website, a different, unusual website comes up.

* While logged into the RockStar server from the previous step, determine if something was modified on this system that might affect viewing rollingstone.com within the browser. When you successfully find the configuration file, record the entry that is set to rollingstone.com.
  + 
* Terminate your ssh session to the rollingstone server, and use nslookup to determine the real domain of the IP address you found from the previous step.
  + 
* Add your findings to your summary and be sure to indicate which OSI layer they were found on.
  + Ssh and nslookup are part of the application 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.
  + 
* These are packets that were captured from the activity in the Hollywood Office.
* Use Wireshark to analyze this pcap file and determine if there was any suspicious activity that could be attributed to a hacker.
  + 
  + Potential Arp poisoning attack
  + 
  + Proof of a hacker trying to sell our secrets.
* Add your findings in your summary and be sure to indicate at which OSI layer they were found.
  + WireShark works on the data link layer decoding packets.