**Phase 1**

1. fping -c 4 -g 15.199.95.91 15.199.95.107
2. fping -c 4 -g 15.199.94.91 15.199.94.107
3. fping -c 4 -g 11.199.158.91 11.199.158.107
4. **fping -c 4 167.172.144.11**167.172.144.11 : [0], 84 bytes, 42.8 ms (42.8 avg, 0% loss)

167.172.144.11 : [1], 84 bytes, 40.8 ms (41.8 avg, 0% loss)

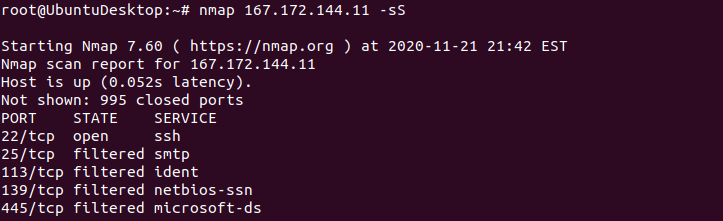
167.172.144.11 : [2], 84 bytes, 36.7 ms (40.1 avg, 0% loss)

167.172.144.11 : [3], 84 bytes, 35.7 ms (39.0 avg, 0% loss)

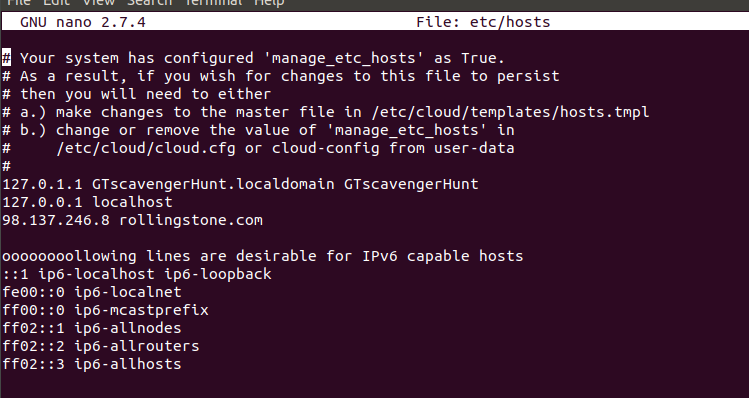
1. fping -c 4 -g 11.199.141.91 11.199.141.107

As mentioned during lecture, to ping an IP address is an action that takes place at the Network layer in the OSI Model. Ping the IP address for Hollywood, California it is evident that only 1 of the address is results in a response with no packet loss. As indicated above number 1,2,3, and 5 were all unsuccessful with no ICMP echo replies. However number 4-to address 167.172.144.11, resulted an ICMP echo reply. This indicates that the other servers were located on private IP addresses that did not want to be found. Raz indicated that this is normal because there are various types of attacks that can be performed on servers who provide a reply. For example, tunnel attacks and DOS attacks.

**Phase 2**



As mentioned in the student guide, layer 4 is responsible for transmitting data across the network. It is responsible for assigning the source and destination ports. Performing a SYN SCAN the results are displayed above.

**Phase 3**  
**Commands used:**  
*ssh jimi@167.172.144.11 -p 22*

*nano etc/hosts*

*q*

*exit*

*nslookup 98.137.246.8*

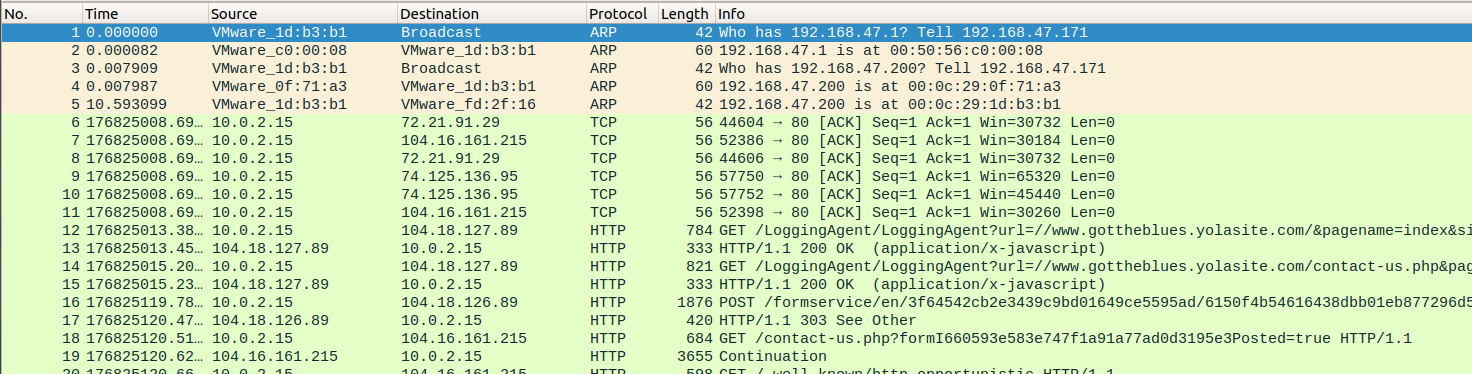
*name = media-router-fp72.prod.media.vip.gq1.yahoo.com*

After determining the server, and performing an NMAP to find the open port; the server could be access using the SSH command and the user and login provided. Within the server the etc/hosts config file shows that when the user attempts to access the http://www.rollingstone.com website, he is redirected to another IP address. The nslookup indicates that the IP address redirect to is an organization called Oath Holdings that is hosted by yahoo. The act of this redirection affects the transport and application layer. Hackers who have root access to the etc/hosts can configure it and perform DNS hijacking to redirect users to malicious sites.

**Phase 4  
Commands used:**

*ssh jimi@167.172.144.11 -p 22*

*find . -type f -iname packet\**

Using Wireshark it becomes evident that duplicate IP address detected for 192.168.47.200. The address is associated with two mac address -00:0c:29:1d:b3:b1 and also in use by 00:0c:29:0f:71:a3. The attacker could be mac address ending in b3:b1 while the actual owner of the IP address is mac ending 71:a3.