**PHASE 1:**

All of the Hollywood Server IPs couldn’t establish a connection besides the Hollywood Application Server with IP ranges from 167.172.144.11/32 excluding 19 and 25 and has a total of 20 IPs that are accepting connections.

The ‘fping’ command operates on OSI Layer 3 (Network Layer)

$ fping -s -g -a 15.199.95.28 15.199.95.91  
 64 targets

0 alive

64 unreachable

0 unknown addresses

64 timeouts (waiting for response)

256 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

5.172 sec (elapsed real time)

$ fping -s -g -a 15.199.94.28 15.199.94.91

64 targets

0 alive

64 unreachable

0 unknown addresses

64 timeouts (waiting for response)

256 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

5.107 sec (elapsed real time)

$ fping -s -g -a 11.199.158.28 11.199.158.91

64 targets

0 alive

64 unreachable

0 unknown addresses

64 timeouts (waiting for response)

256 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

5.009 sec (elapsed real time)

$ fping -s -g -a 167.172.144.11 167.172.144.32

167.172.144.11

167.172.144.12

167.172.144.13

167.172.144.14

167.172.144.15

167.172.144.16

167.172.144.17

167.172.144.18

167.172.144.20

167.172.144.21

167.172.144.22

167.172.144.23

167.172.144.24

167.172.144.26

167.172.144.27

167.172.144.28

167.172.144.29

167.172.144.30

167.172.144.31

167.172.144.32

22 targets

20 alive

2 unreachable

0 unknown addresses

2 timeouts (waiting for response)

28 ICMP Echos sent

20 ICMP Echo Replies received

0 other ICMP received

63.6 ms (min round trip time)

65.1 ms (avg round trip time)

70.8 ms (max round trip time)

4.265 sec (elapsed real time)

$ fping -s -g -a 11.199.141.28 11.199.141.91

64 targets

0 alive

64 unreachable

0 unknown addresses

64 timeouts (waiting for response)

256 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

5.290 sec (elapsed real time)

**PHASE 2:**

List of Open Ports:

167.172.144.11 - 22

167.172.144.12 - 22

167.172.144.13 - 22, 80, 443, 50002

167.172.144.14 - 22, 80, 443

167.172.144.15 - 135, 139, 445, 3389, 49152, 49153, 49154, 49155, 49156, 49157, 49158

167.172.144.16 - 22, 80, 443

167.172.144.17 - 22, 80 ,443

167.172.144.18 - 22, 80, 90

167.172.144.20 - 22, 80, 3306

167.172.144.21 - 22, 80, 443

167.172.144.22 - 22, 80, 443

167.172.144.23 - 22, 80

167.172.144.24 - 22, 80, 443

167.172.144.26 - 22

167.172.144.27 - 22, 3000

167.172.144.28 - 22, 80, 443

167.172.144.29 - 22, 80, 443

167.172.144.30 - 21, 22, 53, 80, 106, 110, 143, 443, 465, 993, 995, 8443

167.172.144.31 - 22, 80, 443

167.172.144.32 - 22, 80, 222, 443, 587, 993

Syn Scan operates on OSI Layer 4 (Transport Layer)

**PHASE 3:**

The hosts file within RockStar Corp was modified to redirect traffic from rollingstone.com to 98.137.426.8. This IP is associated with the domain

media-router-fp72.prod.media.vip.gq1.yahoo.com.

Both nslookup and ssh operate on OSI Layer 7 (Application Layer)

Inside /etc/hosts -  
98.137.426.8 rollingstone.com

Nslookup 98.137.246.8 -

Name = media-router-fp72.prod.media.vip.gq1.yahoo.com

**PHASE 4:**

As shown in Frames 4 and 5, the hacker (VMware\_1d:b3:b1) was able to change their IP address from 192.168.47.171 to 192.168.47.200 which was already in use by VMware\_0f:71:a3. This allows the hacker to trick the server into thinking they are someone they are not.

In Frame 16 of secretlogs.pcapng, Mr. Hacker sent an email using [hacker@rockstarcorp.com](mailto:hacker@rockstarcorp.com) with the message “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!".

ARP primarily operates on OSI Layer 2 (Data Link Layer) however, ARP can also show some Layer 3 (Network Layer) information like IP addresses.

HTTP operates on OSI Layer 7 (Application Layer)