

With a text file named serverList.txt that contains all the Hollywood IPs the command:

```
fping -r < serverList.txt
```

yielded that only the 167.172.144.11/32 from this list was accepting connections, while 15.199.95.91/28, 15.199.94.91/28, 11.199.158.91/28, and 11.199.141.91/28 were not. These findings are found on the 3rd OSI layer, the network layer.

-Recommend restricting ping on the 167.172.144.11 IP.

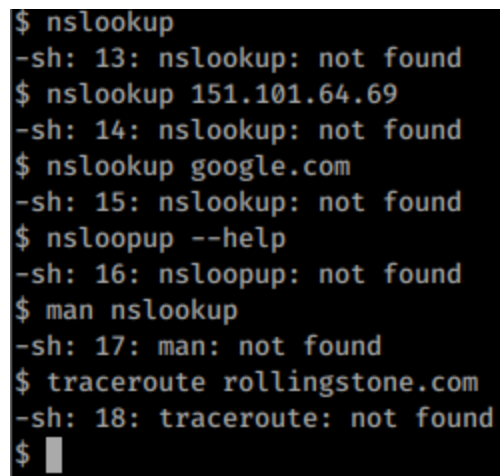
As 167.172.144.11/32 is the only IP open on Layer 3 of the OSI model it has the only open port of these addresses being port 22/tcp ssh.

Using ssh -l jimi 167.172.144.11 and password hendrix I was able to gain access into this server. OSI layer 3

-Recommend disabling port 22.

While trying to use nslookup to query the Domain Name System, it seems as though it is not available on the host system.

-Attempted to rectify using apt-get install nslookup unsuccessfully, lacking sudo privileges.



```
$ nslookup
-sh: 13: nslookup: not found
$ nslookup 151.101.64.69
-sh: 14: nslookup: not found
$ nslookup google.com
-sh: 15: nslookup: not found
$ nslookup --help
-sh: 16: nslookup: not found
$ man nslookup
-sh: 17: man: not found
$ traceroute rollingstone.com
-sh: 18: traceroute: not found
$
```

However, by navigating to /etc and looking at the hosts file I was able to determine that requests to rollingstone.com were being redirected to 98.137.246.8, which seems to be a yahoo site.

```
$ cat hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tpl
# b.) change or remove the value of 'manage_etc_hosts' in
#    /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
127.0.0.1 localhost
98.137.246.8 rollingstone.com
```

The DNS runs parallel to the HTTP in the Application Layer, OSI layer 7.

-Recommend restrictions on who has access to change the hosts file.

Found packet captures left by hacker.

Duplicate IP addresses found

-Recommend blocking the following mac addresses:

Sender MAC address: VMware_0f:71:a3 (00:0c:29:0f:71:a3)

Target MAC address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)

Layer 2: Data link Layer.

Hacker is an insider using forms on yola.com to sell company vulnerabilities, user names and passwords.

Using Mac address: 08:00:27:f8:42:a7

It seems the insider hacker is using a virtual machine to hide their activities.

-Recommend closing port 80 and potentially using the Mac and IP addresses and other packet info to find Hacker and restrict what websites users can visit.

Transmission Control Protocol (TCP) Layer 4.