HW8

Phase 1.

16	15.199.95.91/28		Hollywood Database Servers
17	15.199.94.91/28		Hollywood Web Servers
18	11.199.158.91/28		Hollywood Web Servers
19	**167.172.144.11**/32		Hollywood Application Servers
20	11.199.141.91/28		Hollywood Application Servers

Found “167.172.144.11 is alive” and can be fping’d. The other 4 IP addresses in red were “unreachable”. This would affect layer 3 Network due to certain IP address being able to be ping’d and the other IPs being unreachable. This vulnerability could be prevented by restricting the ICMP echo requests to all servers

Phase 2.

```
sysadmin@UbuntuDesktop:~$ nmap 167.172.144.11 -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:15 EST
Nmap scan report for 167.172.144.11
Host is up (0.11s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
```

Performed command nmap 167.172.144.11 -Pn and found “port 22/tcp open ssh”. This would affect layer 4:Transport because it puts data onto the network and assigns source and destination ports. This vulnerability could be prevented by closing port 22.

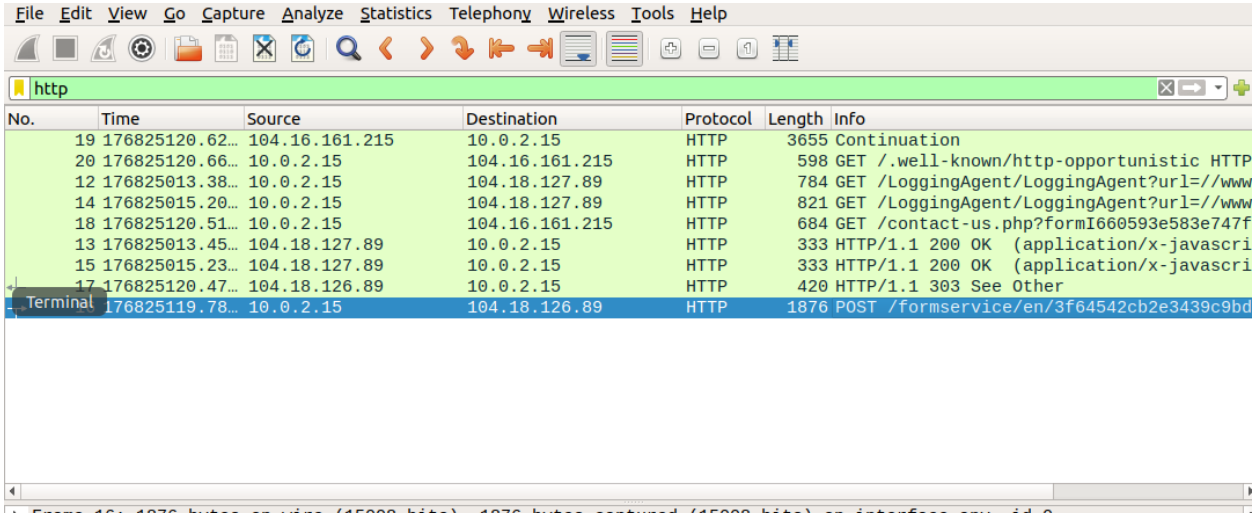
Phase 3.

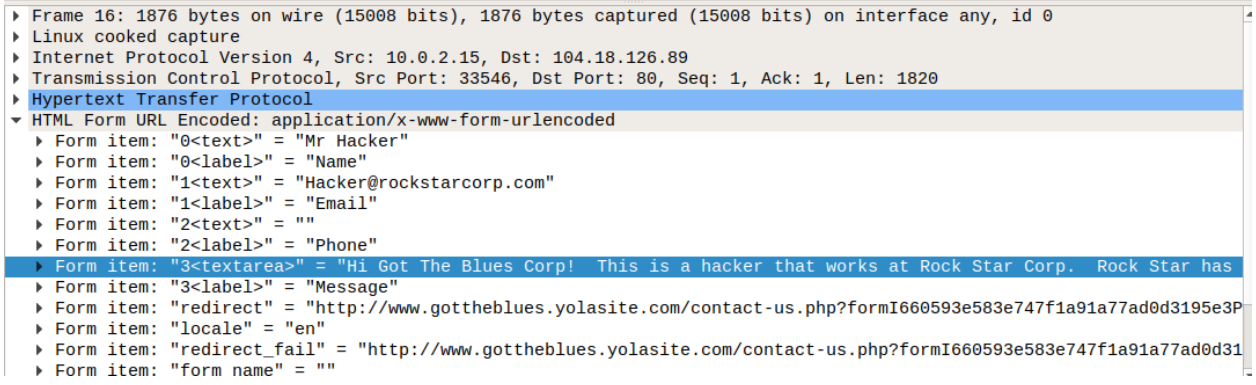
```
$ cat hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /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

ooooooooollowing lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

$
```

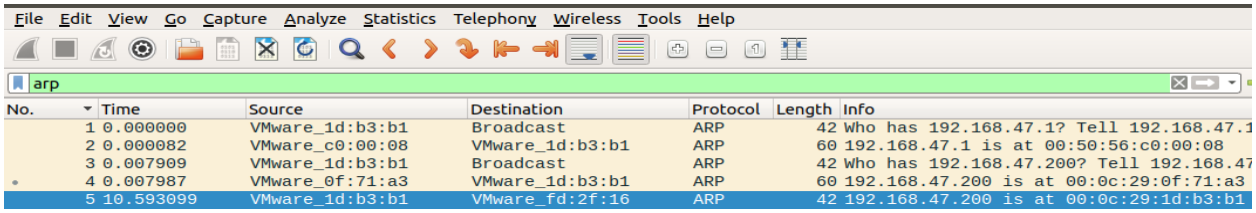
```
dmin@UbuntuDesktop:~$ nslookup 98.137.246.8
6.137.98.in-addr.arpa       name = media-router-fp72.prod.media.vip.gq1.yahoo.com.

oritative answers can be found from:
```

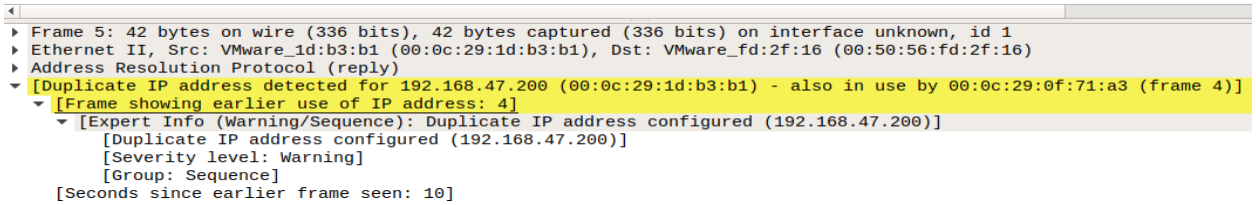
This will affect the Layer 7 application the IP address that is being requested is being sent to a different address from the browser. This vulnerability could be prevented by resetting the default user and password and limiting sudo access so files cant be edited.

Phase 4.









This will affect layer 2 datalink because the ARP is being spoofed. This vulnerability could be prevented by setting up static ARP entries as well as RockstarCorp purchasing Host Intrusion Prevention software to detect if an ARP was spoofed. It would also be advised to find the owner of 00:0c:29:1d:b3:b1 and find the source jof 10.0.2.15 that caused the redirect.