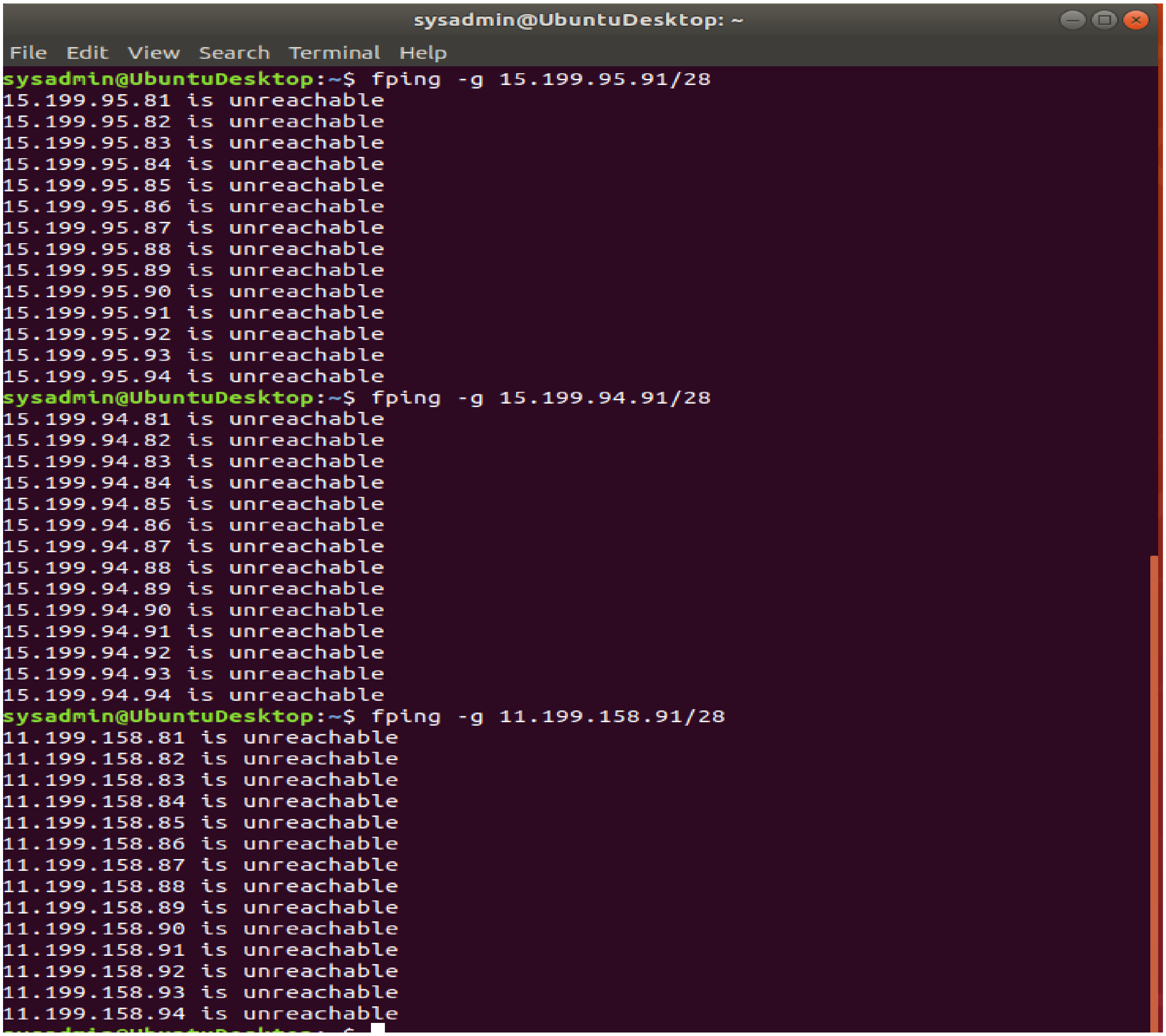
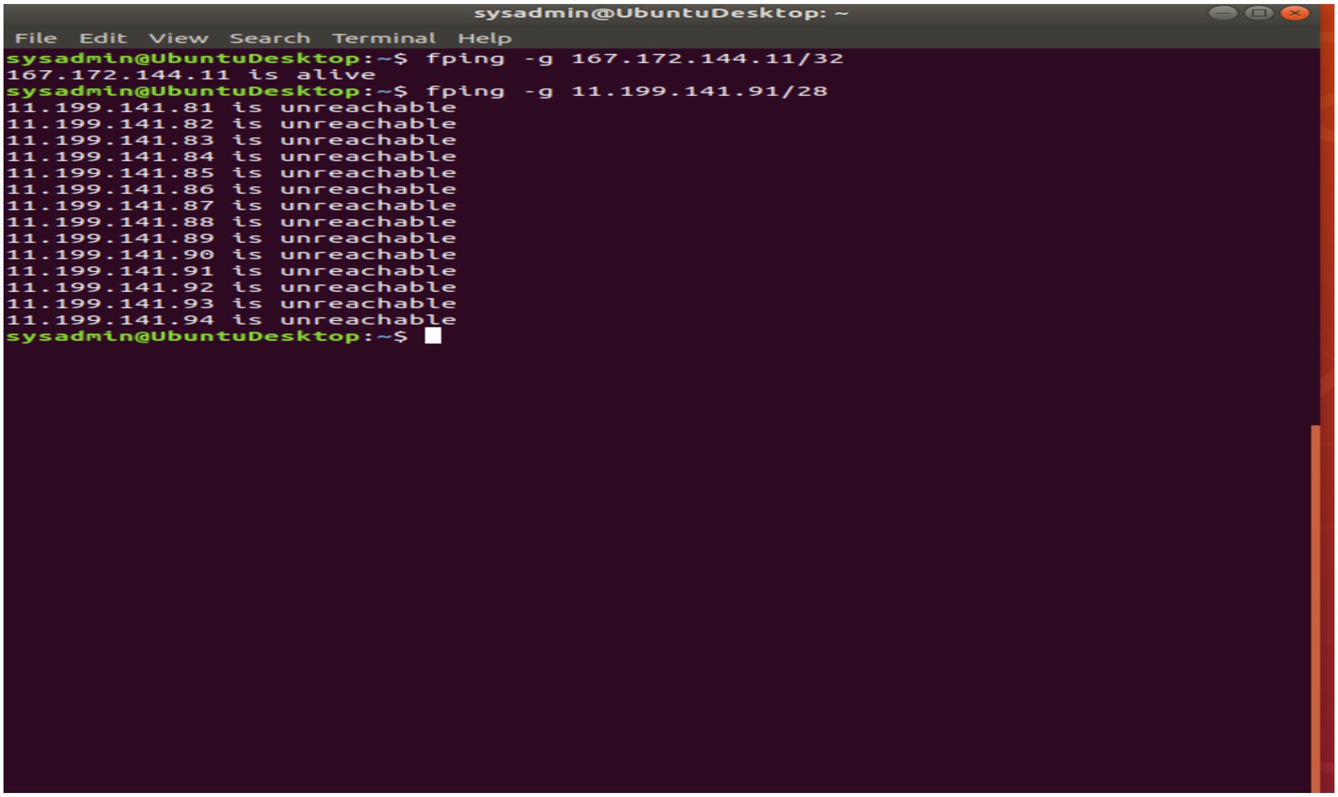
Homework 08:Networking Fundamentals Homework: Rocking your Network!

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

1. Command & Tools- fping



```
sysadmin@UbuntuDesktop:~$ fping -g 15.199.95.91/28
15.199.95.81 is unreachable
15.199.95.82 is unreachable
15.199.95.83 is unreachable
15.199.95.84 is unreachable
15.199.95.85 is unreachable
15.199.95.86 is unreachable
15.199.95.87 is unreachable
15.199.95.88 is unreachable
15.199.95.89 is unreachable
15.199.95.90 is unreachable
15.199.95.91 is unreachable
15.199.95.92 is unreachable
15.199.95.93 is unreachable
15.199.95.94 is unreachable
sysadmin@UbuntuDesktop:~$ fping -g 15.199.94.91/28
15.199.94.81 is unreachable
15.199.94.82 is unreachable
15.199.94.83 is unreachable
15.199.94.84 is unreachable
15.199.94.85 is unreachable
15.199.94.86 is unreachable
15.199.94.87 is unreachable
15.199.94.88 is unreachable
15.199.94.89 is unreachable
15.199.94.90 is unreachable
15.199.94.91 is unreachable
15.199.94.92 is unreachable
15.199.94.93 is unreachable
15.199.94.94 is unreachable
sysadmin@UbuntuDesktop:~$ fping -g 11.199.158.91/28
11.199.158.81 is unreachable
11.199.158.82 is unreachable
11.199.158.83 is unreachable
11.199.158.84 is unreachable
11.199.158.85 is unreachable
11.199.158.86 is unreachable
11.199.158.87 is unreachable
11.199.158.88 is unreachable
11.199.158.89 is unreachable
11.199.158.90 is unreachable
11.199.158.91 is unreachable
11.199.158.92 is unreachable
11.199.158.93 is unreachable
11.199.158.94 is unreachable
sysadmin@UbuntuDesktop:~$
```



sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

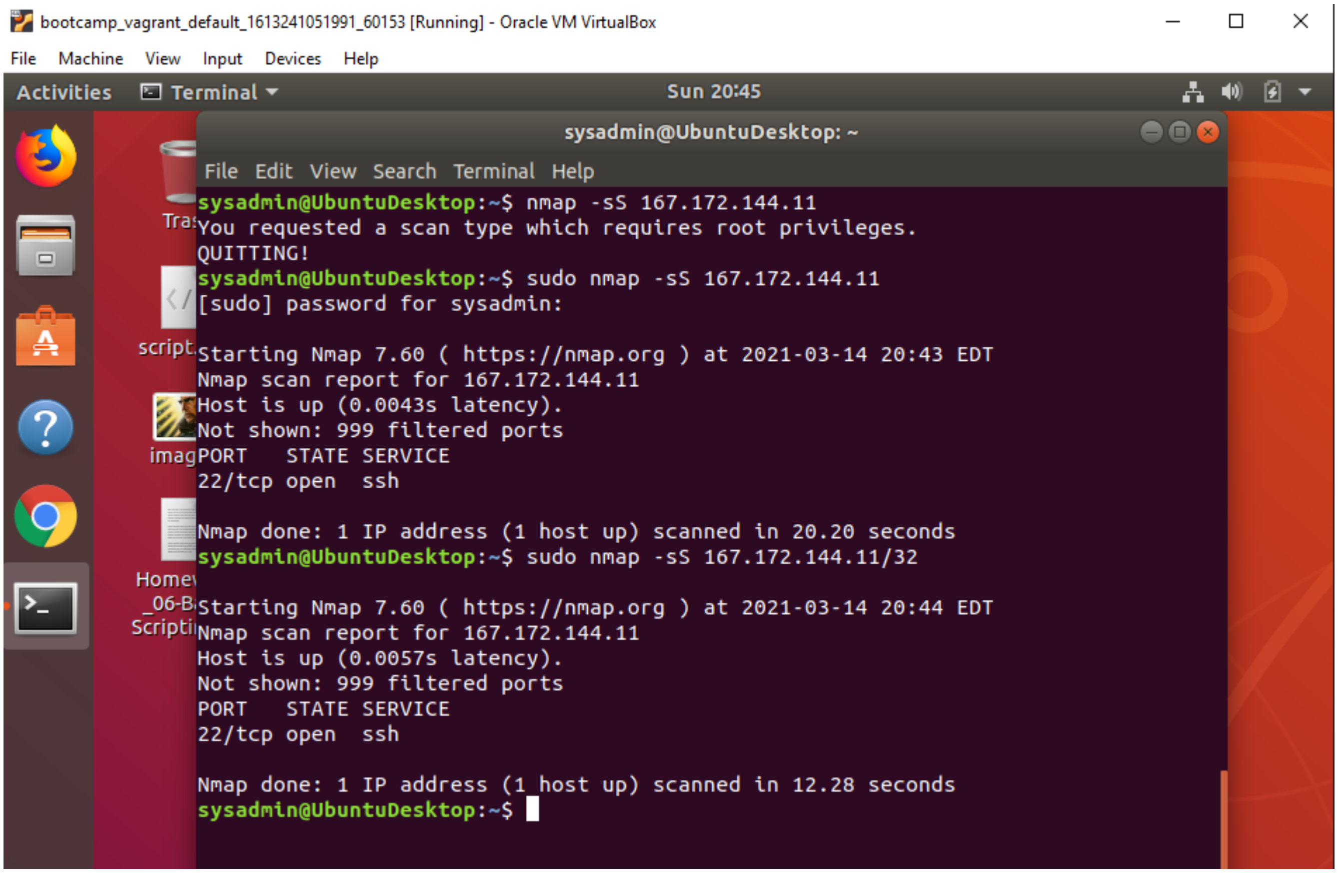
```
sysadmin@UbuntuDesktop:~$ fping -g 167.172.144.11/32
167.172.144.11 is alive
sysadmin@UbuntuDesktop:~$ fping -g 11.199.141.91/28
11.199.141.81 is unreachable
11.199.141.82 is unreachable
11.199.141.83 is unreachable
11.199.141.84 is unreachable
11.199.141.85 is unreachable
11.199.141.86 is unreachable
11.199.141.87 is unreachable
11.199.141.88 is unreachable
11.199.141.89 is unreachable
11.199.141.90 is unreachable
11.199.141.91 is unreachable
11.199.141.92 is unreachable
11.199.141.93 is unreachable
11.199.141.94 is unreachable
sysadmin@UbuntuDesktop:~$ 
```

The only one that was reachable was 167.172.144.11/32.

The ***ping*** command uses the services of the ***Internet Control Message Protocol*** (ICMP), OSI Layer 3 Network.

2.

Command & Tool- nmap -sS 167.172.144.11

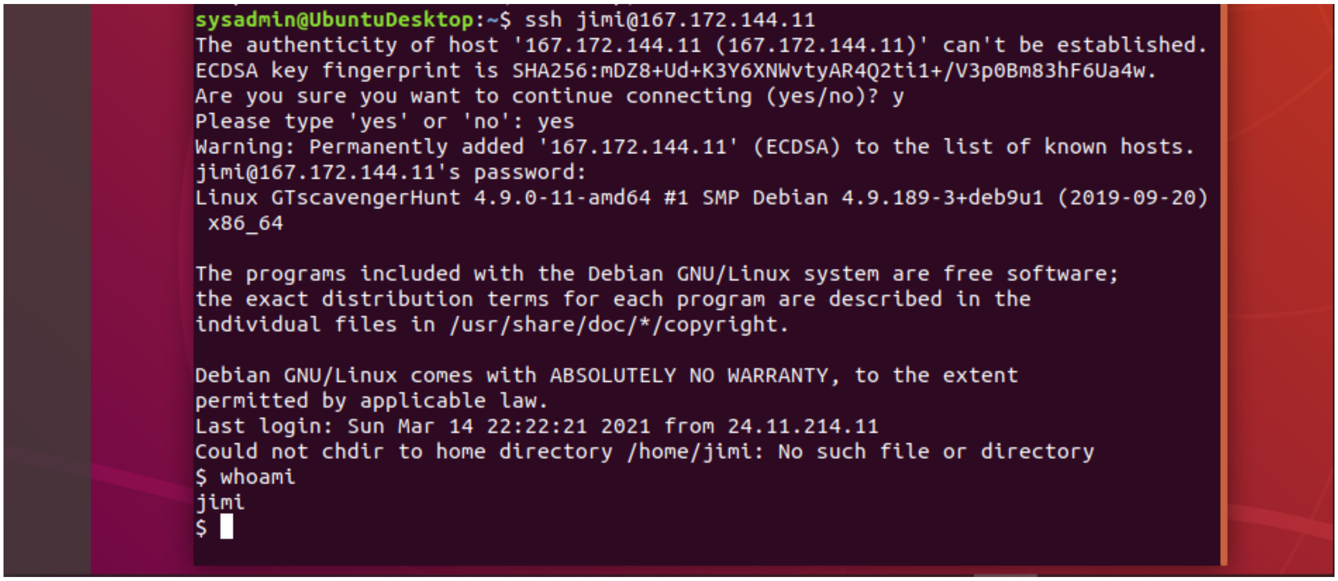

bootcamp_vagrant_default_1613241051991_60153 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Sun 20:45
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~$ nmap -sS 167.172.144.11
You requested a scan type which requires root privileges.
QUITTING!
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 167.172.144.11
[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2021-03-14 20:43 EDT
Nmap scan report for 167.172.144.11
Host is up (0.0043s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 20.20 seconds
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 167.172.144.11/32

Starting Nmap 7.60 ( https://nmap.org ) at 2021-03-14 20:44 EDT
Nmap scan report for 167.172.144.11
Host is up (0.0057s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 12.28 seconds
sysadmin@UbuntuDesktop:~$
```

Hollywood Application Servers – 167.172.144.11/32 – PORT 22/tcp STATE open SERVICE ssh. The SSH protocol is apart of the Layer 7: Application Layer.

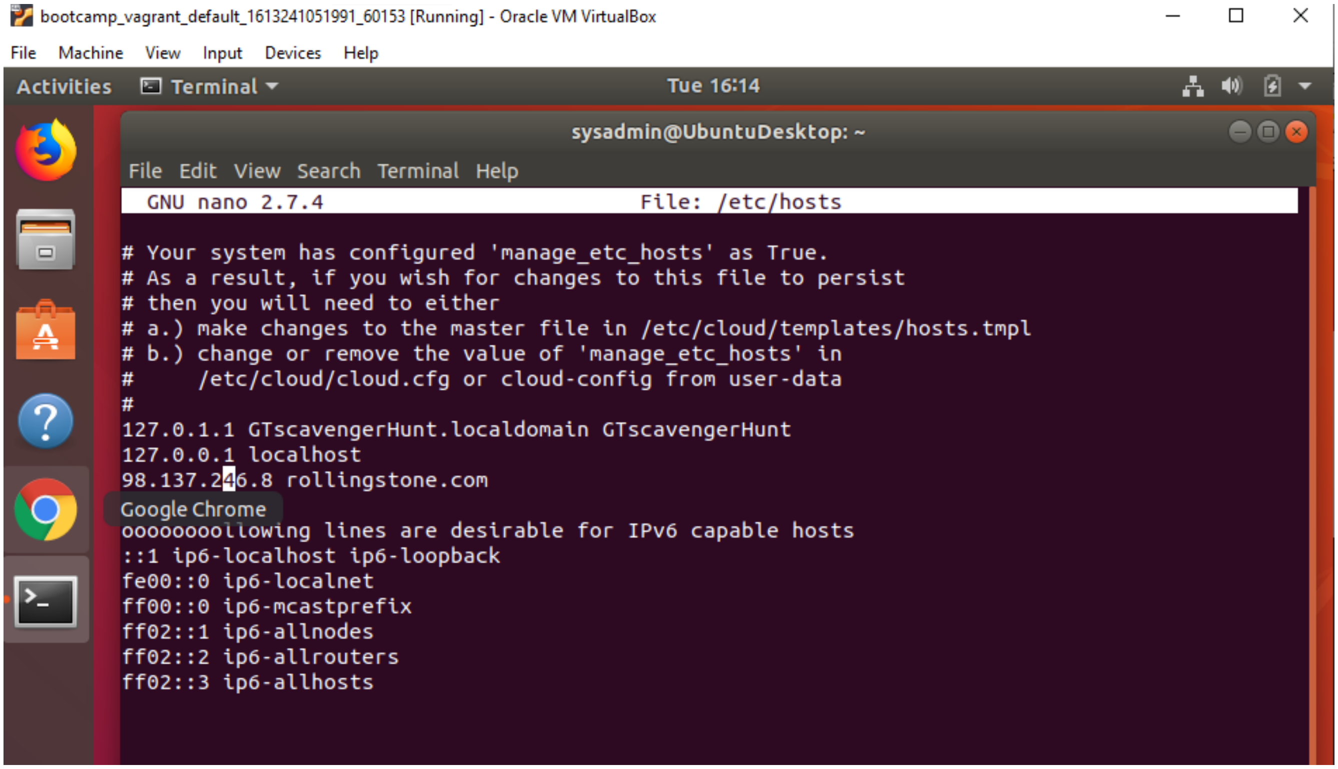
3.

Command: ssh jim@167.172.144.11 PW: hendrix to log onto the network.



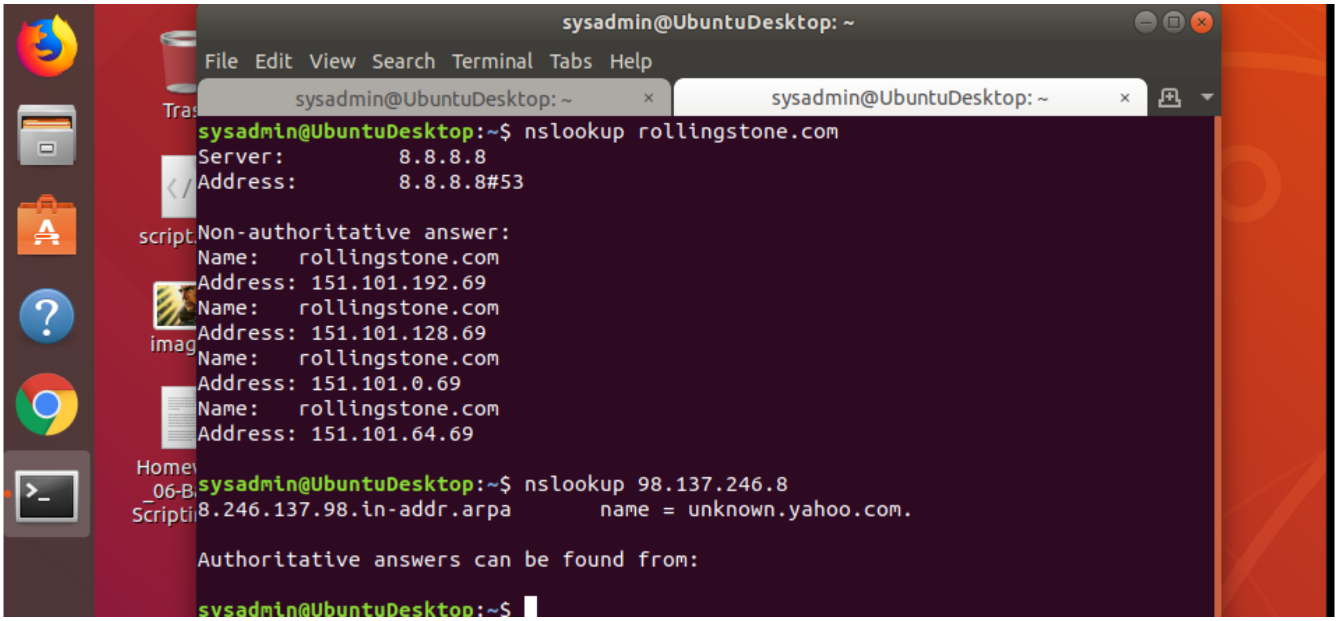
```
sysadmin@UbuntuDesktop:~$ ssh jimi@167.172.144.11
The authenticity of host '167.172.144.11 (167.172.144.11)' can't be established.
ECDSA key fingerprint is SHA256:mDZ8+Ud+K3Y6XNWvtyAR4Q2ti1+/V3p0Bm83hF6Ua4w.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '167.172.144.11' (ECDSA) to the list of known hosts.
jimi@167.172.144.11's password:
Linux GTscavengerHunt 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20)
 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar 14 22:22:21 2021 from 24.11.214.11
Could not chdir to home directory /home/jimi: No such file or directory
$ whoami
jimi
$
```

Logging in with supplied credentials was successful. Username-jimi PW-hendrix


bootcamp_vagrant_default_1613241051991_60153 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Tue 16:14
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Google Chrome

```
  GNU nano 2.7.4                         File: /etc/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

oooooooollowing 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
```

In the /etc/hosts file, wrong IP address provided for rollingstone.com.



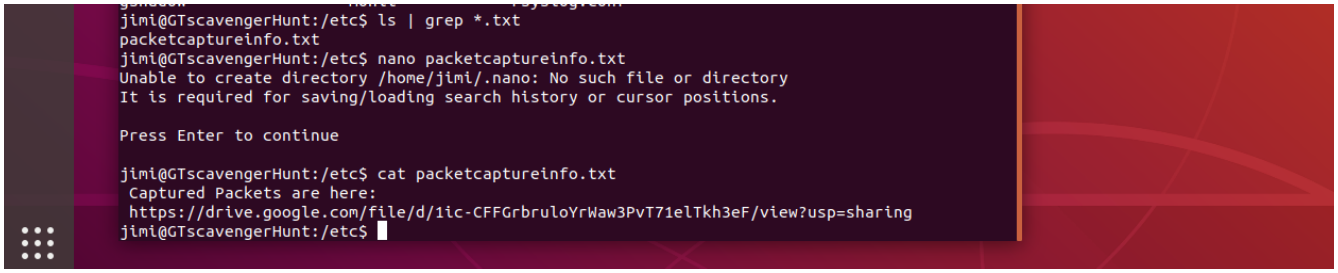
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Tabs Help
sysadmin@UbuntuDesktop: ~
sysadmin@UbuntuDesktop: ~

```
sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   rollingstone.com
Address: 151.101.192.69
Name:   rollingstone.com
Address: 151.101.128.69
Name:   rollingstone.com
Address: 151.101.0.69
Name:   rollingstone.com
Address: 151.101.64.69

sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

Tools: nslookup

From personal computer I performed a nslookup of rollingstone.com search. I found that actual IP address was different and looked up 98.137.246.8 found that its a unknown.
Layer 7 Application Layer.
Nslookup is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.

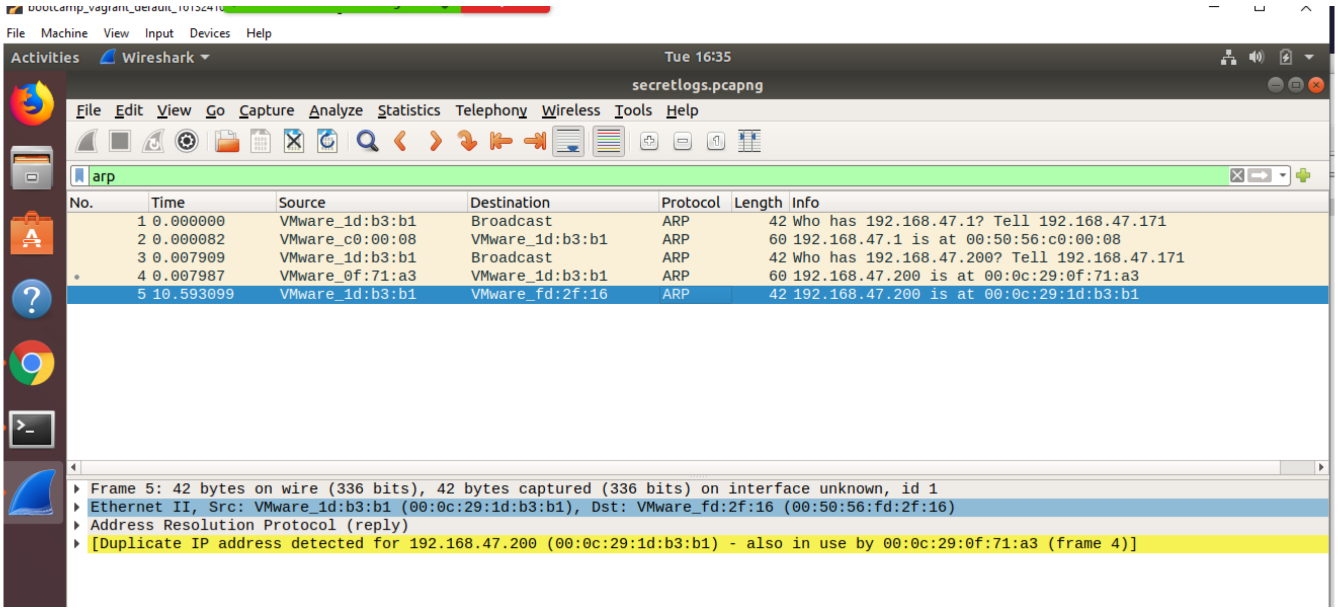
4.



```
jimi@GTscavengerHunt:/etc$ ls | grep *.txt
packetcaptureinfo.txt
jimi@GTscavengerHunt:/etc$ nano packetcaptureinfo.txt
Unable to create directory /home/jimi/.nano: No such file or directory
It is required for saving/loading search history or cursor positions.

Press Enter to continue

jimi@GTscavengerHunt:/etc$ cat packetcaptureinfo.txt
 Captured Packets are here:
 https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
jimi@GTscavengerHunt:/etc$
```

In the same directory (/etc), the hacker left a .txt file to some packet captures.

Tools: Wireshark

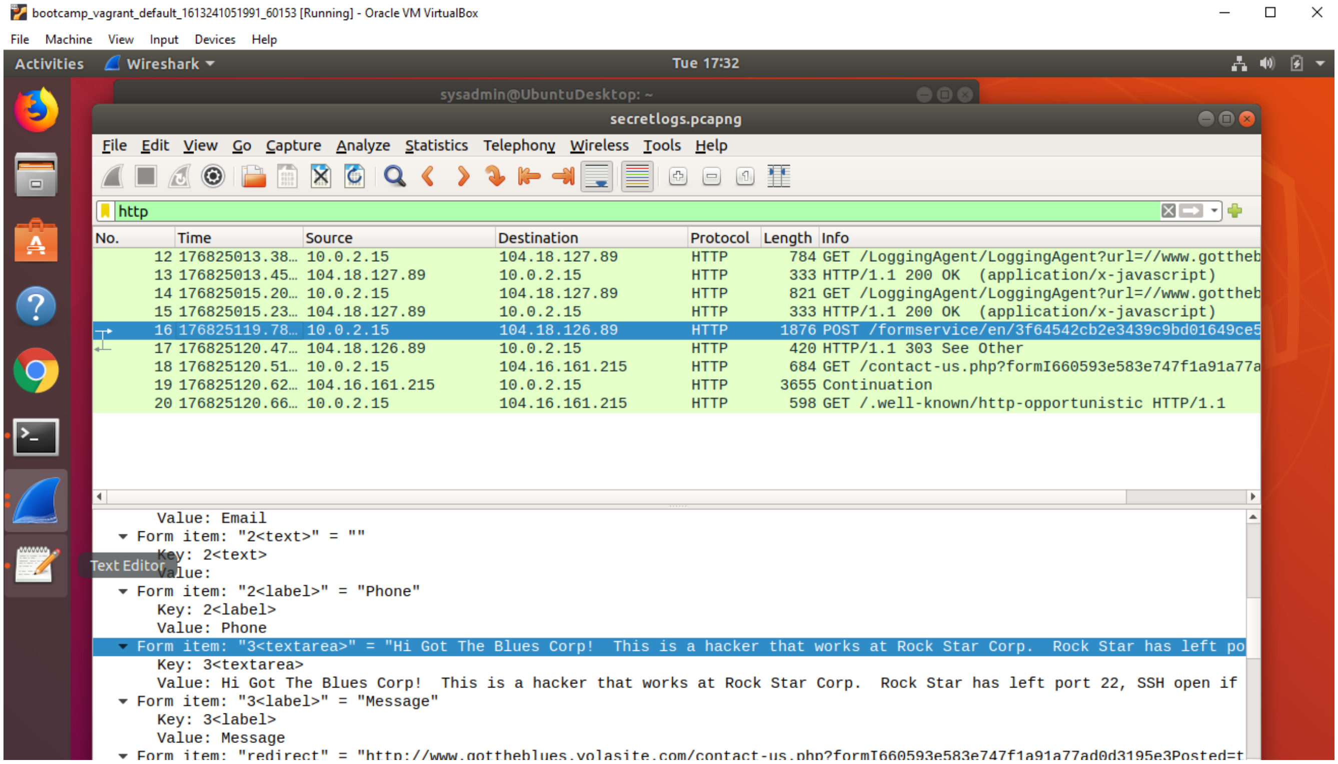


File Machine View Input Devices Help
Activities
Wireshark
Tue 16:35
secretlogs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp

No.     Time        Source             Destination        Protocol Length Info
      1 0.000000    VMware_1d:b3:b1    Broadcast          ARP         42 Who has 192.168.47.1? Tell 192.168.47.171
      2 0.000082    VMware_c0:00:08    VMware_1d:b3:b1    ARP         60 192.168.47.1 is at 00:50:56:c0:00:08
      3 0.007909    VMware_1d:b3:b1    Broadcast          ARP         42 Who has 192.168.47.200? Tell 192.168.47.171
      4 0.007987    VMware_0f:71:a3    VMware_1d:b3:b1    ARP         60 192.168.47.200 is at 00:0c:29:0f:71:a3
      5 10.593099   VMware_1d:b3:b1    VMware_fd:2f:16    ARP         42 192.168.47.200 is at 00:0c:29:1d:b3:b1

▸ Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1
▸ Ethernet II, Src: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: VMware_fd:2f:16 (00:50:56:fd:2f:16)
▸ Address Resolution Protocol (reply)
▸ [Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)]
```

Suspicious activities found, filtering by ARP protocol, two different MAC address for the same IP.

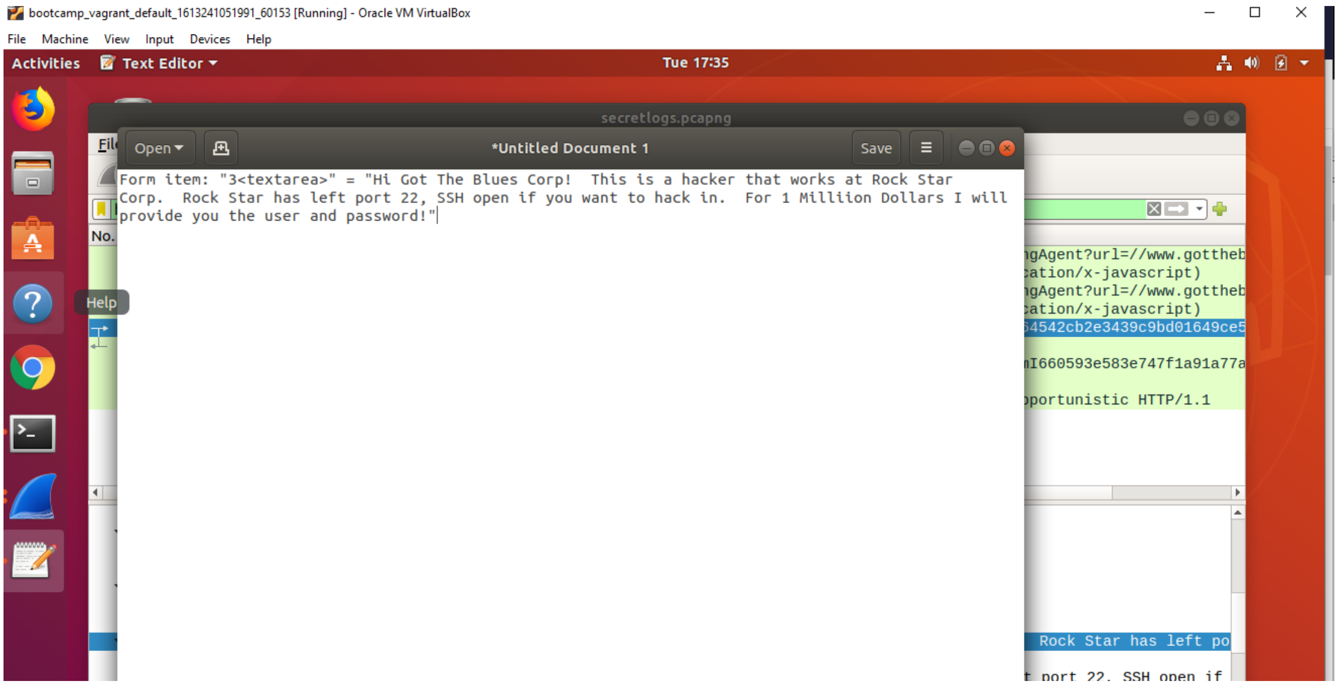
Network: 2nd layer of the OSI model.



bootcamp_vagrant_default_1613241051991_60153 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
Tue 17:32
sysadmin@UbuntuDesktop: ~
secretlogs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Text Editor

```
http

No.     Time              Source            Destination       Protocol Length Info
     12 176825013.38…     10.0.2.15         104.18.127.89     HTTP       784 GET /LoggingAgent/LoggingAgent?url=//www.gottheb
     13 176825013.45…     104.18.127.89     10.0.2.15         HTTP       333 HTTP/1.1 200 OK  (application/x-javascript)
     14 176825015.20…     10.0.2.15         104.18.127.89     HTTP       821 GET /LoggingAgent/LoggingAgent?url=//www.gottheb
     15 176825015.23…     104.18.127.89     10.0.2.15         HTTP       333 HTTP/1.1 200 OK  (application/x-javascript)
     16 176825119.78…     10.0.2.15         104.18.126.89     HTTP      1876 POST /formservice/en/3f64542cb2e3439c9bd01649ce5
     17 176825120.47…     104.18.126.89     10.0.2.15         HTTP       420 HTTP/1.1 303 See Other
     18 176825120.51…     10.0.2.15         104.16.161.215    HTTP       684 GET /contact-us.php?formI660593e583e747f1a91a77a
     19 176825120.62…     104.16.161.215    10.0.2.15         HTTP      3655 Continuation
     20 176825120.66…     10.0.2.15         104.16.161.215    HTTP       598 GET /.well-known/http-opportunistic HTTP/1.1

      Value: Email
  ▾ Form item: "2<text>" = ""
      Key: 2<text>
      Value:
  ▾ Form item: "2<label>" = "Phone"
      Key: 2<label>
      Value: Phone
  ▾ Form item: "3<textarea>" = "Hi Got The Blues Corp!  This is a hacker that works at Rock Star Corp.  Rock Star has left po
      Key: 3<textarea>
      Value: Hi Got The Blues Corp!  This is a hacker that works at Rock Star Corp.  Rock Star has left port 22, SSH open if
  ▾ Form item: "3<label>" = "Message"
      Key: 3<label>
      Value: Message
  ▾ Form item: "redirect" = "http://www.gottheblues.volasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=t
```

Suspicious activities found, filtering by http protocol, message found in packet # 16 by Mr.Hacker.
Network: 2nd layer of the OSI model.



```
Form item: "3<textarea>" = "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 Million Dollars I will
provide you the user and password!"
```

```
ngAgent?url=//www.gottheb
cation/x-javascript)
ngAgent?url=//www.gottheb
cation/x-javascript)
64542cb2e3439c9bd01649ce5

mI660593e583e747f1a91a77a

pportunistic HTTP/1.1
```

```
 Rock Star has left po
t port 22. SSH open if
```

In summary, service ICMP should be restricted. PORT 22 left open, should be closed. All compromised and false accounts/username/PW should be deleted or changed.