



# Cybersecurity

## Networking Challenge Submission File

### Networking Fundamentals: Rocking your Network

Make a copy of this document to work in. For each phase, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

#### Phase 1: “I’d like to Teach the World to ping”

1. Command(s) used to run ping against the IP ranges:

```
fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
```

A screenshot of a Linux desktop environment, specifically Ubuntu, running in Oracle VM VirtualBox. The terminal window shows the command `fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0` being executed. The output indicates that only the IP 161.35.96.20 is alive, while the others are unreachable.

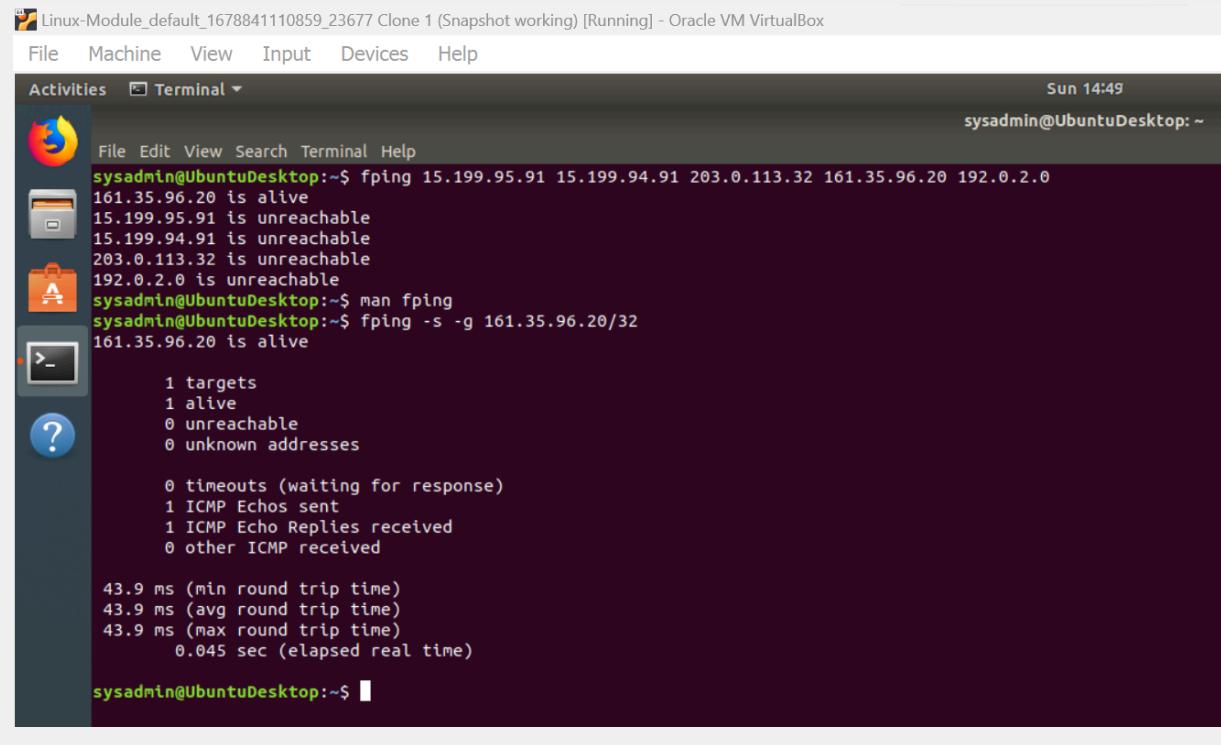
```
Linux-Module_default_167884110859_23677 Clone 1 (Snapshot working) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 14:20
sysadmin@UbuntuDesktop: ~
File Edit View Terminal Help
sysadmin@UbuntuDesktop:~$ fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
161.35.96.20 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
203.0.113.32 is unreachable
192.0.2.0 is unreachable
sysadmin@UbuntuDesktop:~$
```

2. Summarize the results of the ping command(s):

The results of the fping command show us that only the IP 161.35.96.20 is reachable.

3. List of IPs responding to echo requests:

```
fping -s -g 161.35.96.20/32  
This command shows that this IP
```



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Activities Terminal". The terminal content shows the output of the fping command. The output indicates that the target IP 161.35.96.20 is alive, while other IPs in the range (15.199.95.91, 15.199.94.91, 203.0.113.32) are unreachable. The man page for fping is also displayed.

```
Linux-Module_default_167884110859_23677 Clone 1 (Snapshot working) [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Activities Terminal Sun 14:49  
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0  
161.35.96.20 is alive  
15.199.95.91 is unreachable  
15.199.94.91 is unreachable  
203.0.113.32 is unreachable  
192.0.2.0 is unreachable  
sysadmin@UbuntuDesktop:~$ man fping  
sysadmin@UbuntuDesktop:~$ fping -s -g 161.35.96.20/32  
161.35.96.20 is alive  
  
      1 targets  
      1 alive  
      0 unreachable  
      0 unknown addresses  
  
      0 timeouts (waiting for response)  
      1 ICMP Echos sent  
      1 ICMP Echo Replies received  
      0 other ICMP received  
  
    43.9 ms (min round trip time)  
    43.9 ms (avg round trip time)  
    43.9 ms (max round trip time)  
    0.045 sec (elapsed real time)  
  
sysadmin@UbuntuDesktop:~$
```

#### 4. Explain which OSI layer(s) your findings involve:

The OSI layer in the findings involve the Network layer.

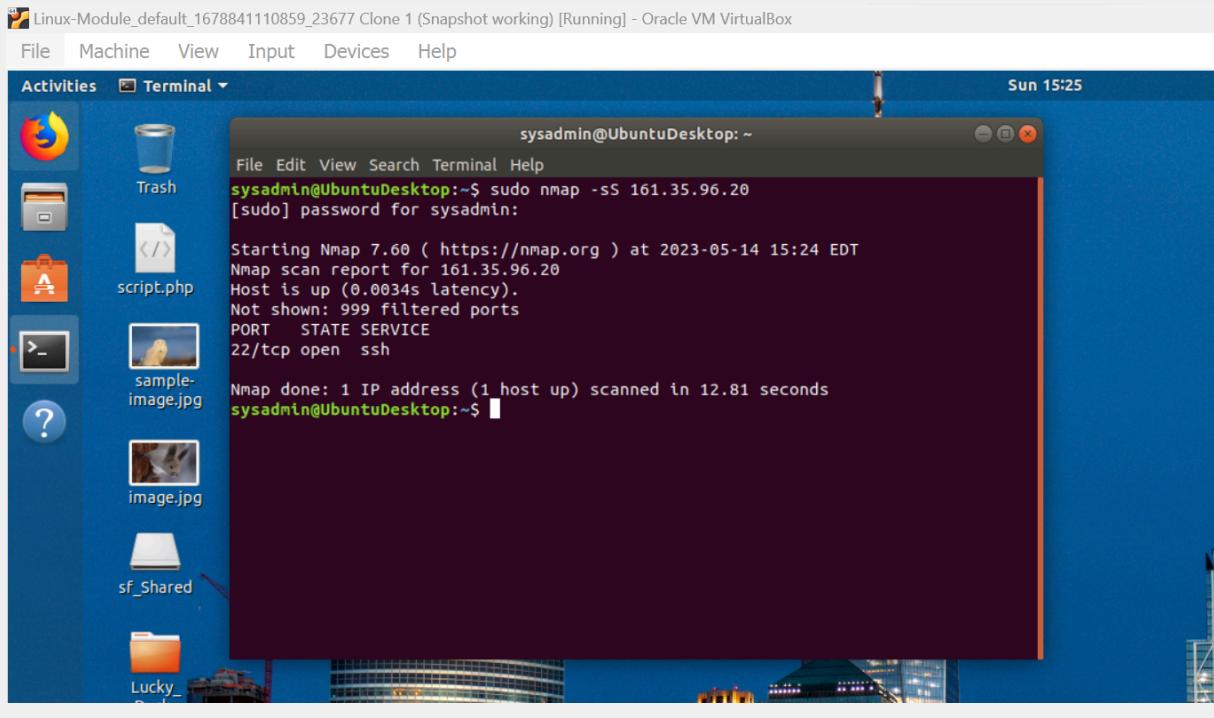
#### 5. Mitigation recommendations (if needed):

Using the fping command we were able to see that the IP 161.35.96.20 is alive and is accepting pings. Rockstar Corp did not want any of their IP address to respond to requests and since this IP is it could lead to a vulnerability as it could allow for unauthorized access. We need to make adjustments to make sure that all servers are alive but show as unreachable and also make sure that our ports are closed as we don not want to be a victim of a DoS attack.

## Phase 2: “Some SYN for Nothin”

#### 1. Which ports are open on the RockStar Corp server?

After running the nmap command, we are able to see that port 22 is open



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "sysadmin@UbuntuDesktop: ~". The terminal output shows the results of a sudo nmap -sS 161.35.96.20 scan:

```
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 161.35.96.20
[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-14 15:24 EDT
Nmap scan report for 161.35.96.20
Host is up (0.0034s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 12.81 seconds
sysadmin@UbuntuDesktop:~$
```

2. Which OSI layer do SYN scans run on?

a. OSI layer:

The OSI layer the SYN scans run on are the Transport layer.

b. Explain how you determined which layer:

In class we discussed TCP and the three way handshake that is needed to establish a connection. The port that is open is 22 and it involves TCP to establish a connection for the SSH.

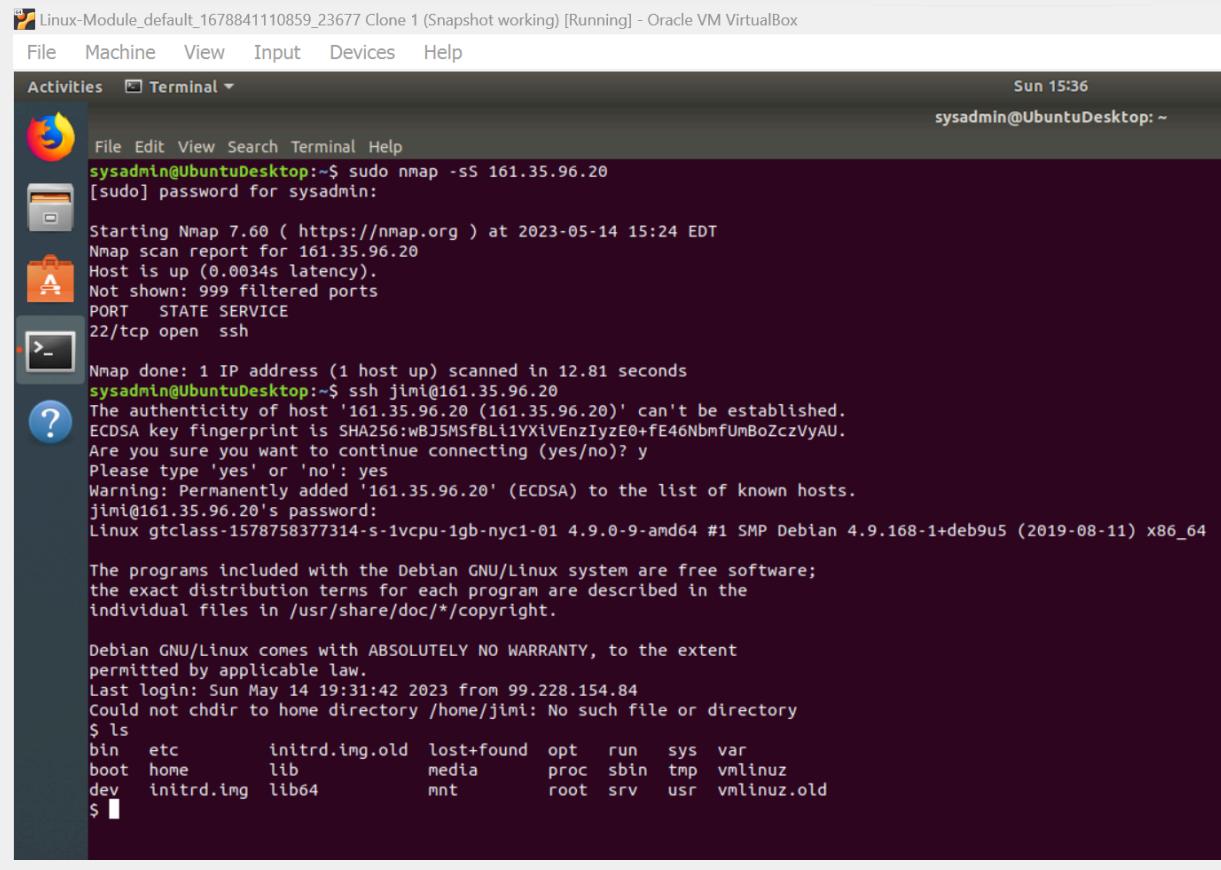
3. Mitigation suggestions (if needed):

Port 22 needs to be shut down so no bad actor is able to SSH into the system.

## Phase 3: “I Feel a DNS Change Comin’ On”

1. Summarize your findings about why access to rollingstone.com is not working as expected from the RockStar Corp Hollywood office:

I was able to ssh into the system, which means a hacker would also be able to access the system and set up a backdoor and change the IP address.



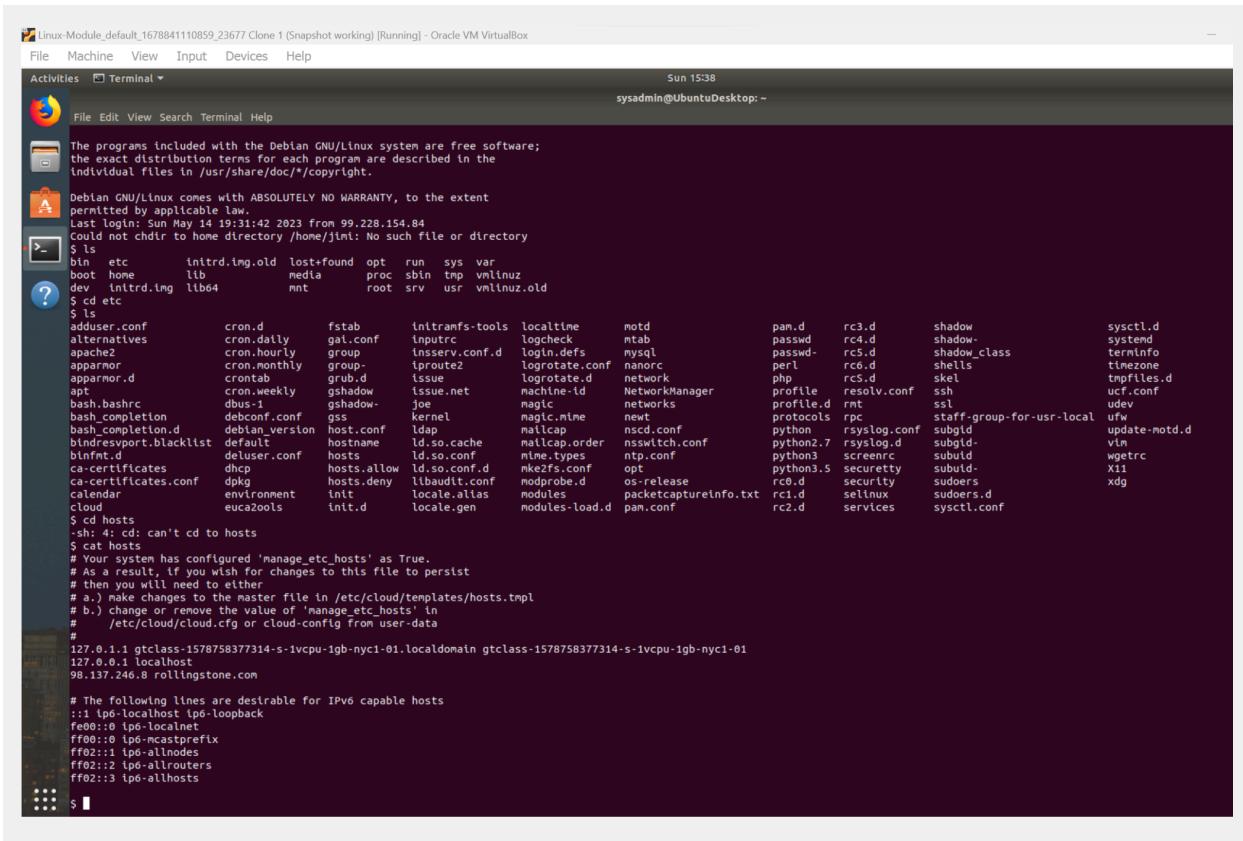
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Linux-Module\_default\_1678841110859\_23677 Clone 1 (Snapshot working) [Running] - Oracle VM VirtualBox". The terminal content shows a user named "sysadmin" performing a security audit:

```
File Edit View Terminal Help
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 161.35.96.20
[sudo] password for sysadmin:
Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-14 15:24 EDT
Nmap scan report for 161.35.96.20
Host is up (0.0034s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 12.81 seconds
sysadmin@UbuntuDesktop:~$ ssh jimi@161.35.96.20
The authenticity of host '161.35.96.20 (161.35.96.20)' can't be established.
ECDSA key fingerprint is SHA256:wBJ5MSfBLi1YXiVEnzIyzE0+fE46NbmfUmBoZczVyAU.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '161.35.96.20' (ECDSA) to the list of known hosts.
jimi@161.35.96.20's password:
Linux gtclass-1578758377314-s-1vcpu-1gb-nyc1-01 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u5 (2019-08-11) 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 May 14 19:31:42 2023 from 99.228.154.84
Could not chdir to home directory /home/jimi: No such file or directory
$ ls
bin  etc      initrd.img.old  lost+found  opt   run   sys   var
boot home     lib           media       proc  sbin  tmp   vmlinuz
dev  initrd.img lib64        mnt        root  srv   usr   vmlinuz.old
$
```



```

Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot working) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 15:38
sysadmin@UbuntuDesktop: ~

File Edit View Search Terminal Help

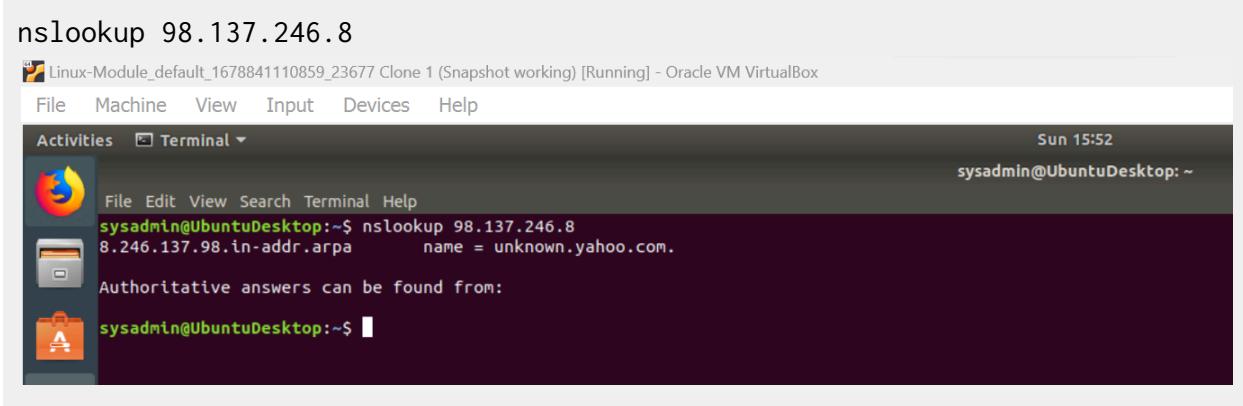
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 14 19:31:42 2023 from 99.228.154.84
Could not chdir to home directory /home/jml: No such file or directory
$ ls
bin  etc  initrd.img.old  lost+found  opt  run  sys  var
boot  home  lib  media  proc  sbin  tmp  vmlinuz
dev  initrd.img  lib64  mnt  root  srv  usr  vmlinuz.old
$ cd etc
$ ls
adduser.conf      cron.d      fstab      initramfs-tools  localtime      motd      pam.d      rc3.d      shadow      sysctl.d
alternatives     cron.daily   gal.conf   inputrc       logcheck      mtab      passwd      rc4.d      shadow      systemd
apache2          cron.hourly group      inserv.conf    login.defs    mysql      passwd      rc5.d      shadow_class  terminfo
apparmor         cron.monthly group      iproute2     logrotate.conf  nanorc    perl       rc6.d      shells      timezone
apparmor.d        cron.weekly gshadow   issue.net     logrotate.d    network   php       rc7.d      ssh       tmux
apt              cronab     gshadow   issue.net     machine-id   NetworkManager-profile  resolv.conf  rsyslog  ssh
bash.bashrc       dbus-1      gshadow   issue.net     machine-id   NetworkManager-profile  resolv.conf  rsyslog  ssh
bash_completion   debconf.conf gss       kernel      magic.mime   newt      protocols  rnt      ssh       udev
bash_completion.d debian_version host.conf  ldap       nscd.conf   nsслtch.conf  python   rsyslog.d  subgid  update-motd.d
bindresport.blacklist default    hostname  ld.so.cache  maticap.order  nsswitch.conf  python2.7  rsyslog.d  subgid  ufw
blinfmt.d         deluser.conf hosts     ld.so.conf.d  mke2fs.conf  mime.types  ntp.conf   python3   screencr  subuid  vim
ca-certificates   dhcp       hosts.allow ld.so.conf.d  mke2fs.conf  mime.types  ntp.conf   python3.5  security  subuid  wgetrc
ca-certificates.conf dpkg       hosts.deny libaudit.conf modprobe.d  os-release  opt      python3.5  security  sudoers  X11
calendar          environment init      locale.alias modules     packetcaptureinfo.txt  rc0.d   security  sudoers  sudoers.d  xdg
cloud             euca2ools  init.d    locale.gen   modules-load.d pam.conf   rc1.d   selinux  sudoers  sysctl.conf
$ cd hosts
$ sh-4.4: can't cd to hosts
$ 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
#
# The following 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
127.0.0.1 gtclass=1578758377314-s-1vcpu-1gb-nyc1-01.localdomain gtclass=1578758377314-s-1vcpu-1gb-nyc1-01
127.0.0.1 localhost
98.137.246.8 rollingstone.com

$ 

```

## 2. Command used to query Domain Name System records:



```

nslookup 98.137.246.8
Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot working) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sun 15:52
sysadmin@UbuntuDesktop: ~

File Edit View Search Terminal Help
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:~$ 

```

## 3. Domain name findings:

There seems to another domain found unknown.yahoo.com.

## 4. Explain what OSI layer DNS runs on:

The OSI layer that the DNS runs on is the application layer (layer 7).

## 5. Mitigation suggestions (if needed):

The IP address needs to be changed immediately to the original and port 22 should be closed ASAP so the hacker cannot get back in and change the IP address. As an extra level of caution a DNS filter should be added for security.

## Phase 4: “ShARP Dressed Man”

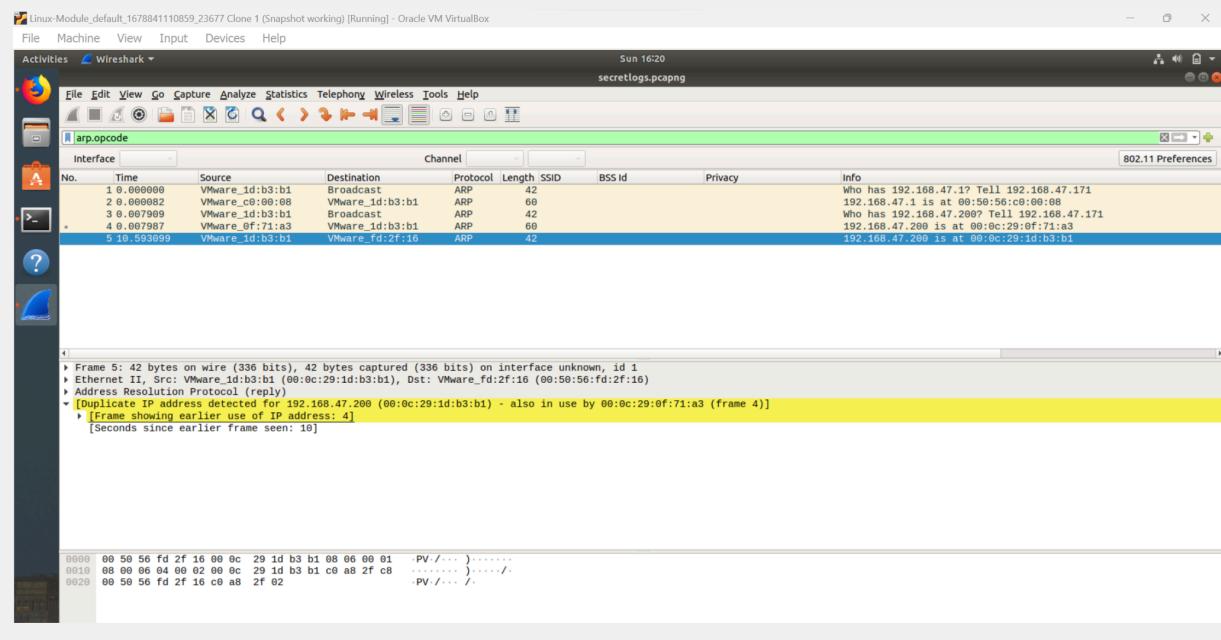
### 1. Name of file containing packets:

When using SSH again to go back into jimi's log on we navigate to the etc/packetcaptureinfo.txt we see the following link  
<https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing>

From that link we were able to see the file secretlogs.pcapng which opened up a file in wireshark.

### 2. ARP findings identifying the hacker's MAC address:

The MAC address found is 00:0c:29:1d:b3:b1



### 3. HTTP findings, including the message from the hacker:

**Wireshark - secretlogs.pcapng**

**http.request.method == "GET"**

No.	Time	Source	Destination	Protocol	Length	SSID	BSS Id	Privacy	Info
12	17/08/2013, 38.10.0.2.15		104.18.127.89	HTTP	784				GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x683&colorDep...
14	17/08/2013, 20.10.0.2.15		104.18.127.89	HTTP	821				GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x683&colorDep...
18	17/08/2013, 51.10.0.2.15		104.16.161.215	HTTP	684				GET /contact-us.php?formI660593e583e747f1a91a7ad0d3195e3Posted
20	17/08/2013, 66.10.0.2.15		104.16.161.215	HTTP	598				GET /.well-known/http-opportunistic HTTP/1.1

```

Frame 14: 821 bytes on wire (6568 bits), 821 bytes captured (6568 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.127.89
Transmission Control Protocol, Src Port: 58610, Dst Port: 80, Seq: 729, Ack: 278, Len: 765
Hypertext Transfer Protocol
  [uncated]GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x683&colorDep...
  L [uncated]Exploit Info (Chat/Sequence): GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x683&colorDep...
  Request URI [uncated]: /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x683&colorDep...
  Request Version: HTTP/1.1
  Host: pixel.yola.com\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Referer: http://www.gottheblues.yolasite.com/contact-us.php\r\n
  
```

Packets: 20 · Displayed: 4 (20.0%) · Profile: Default · Right Ctrl

**Wireshark - secretlogs.pcapng**

**http.request.method == "POST"**

No.	Time	Source	Destination	Protocol	Length	SSID	BSS Id	Privacy	Info
16	17/08/2013, 78.10.0.2.15		104.18.126.89	HTTP	1676				POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54...

```

File Data: 1163 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "0:text" = "Mr Hacker"
Form item: "1:text" = "Name"
Form item: "2:text" = "Hacker@rockstarcorp.com"
Form item: "3:label" = "Email"
Form item: "2:label" = ""
Form item: "2:label" = "Phone"
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 give you full access to the system. If you want to pay me, send me an email to the address above. I will respond as soon as possible."
Form item: "3:label" = "Message"
Form item: "4:label" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a7ad0d3195e3Posted=true"
Form item: "4:label" = "en"
Form item: "5:label" = "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a7ad0d3195e3Posted=false"
Form item: "site_name" = "GottheBlues"
  
```

Packets: 20 · Displayed: 1 (5.0%) · Profile: Default · Right Ctrl

Using the http findings, we were able to see that a request for 1 million dollars was being made by the hacker who works at Rockstar Corp.

4. Explain the OSI layers for HTTP and ARP.

a. Layer used for HTTP:

The OSI layer used for HTTP is the Application layer (layer 7)

b. Layer used for ARP:

The OSI layer used for the ARP is the data link layer (layer 2)

5. Mitigation suggestions (if needed):

Port 22 should be closed and IP addresses should be converted back to the original. Rockstar Corp should also create password policies so that each employee has a unique username and password that will enhance security. Notifications should be established for all logs and these should be reviewed regularly and any user that is able to SSH should appear in the logs.