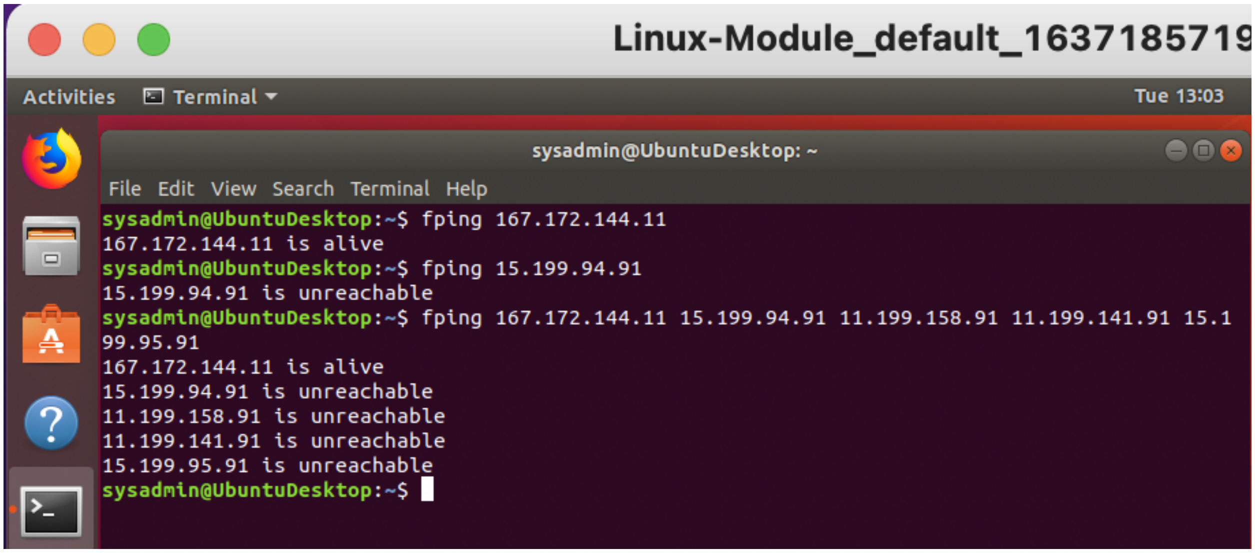
Network Vulnerability Assessment Instructions

Please note that you will be using your Vagrant virtual machine for this homework.

Phase 1: *"I'd like to Teach the World to Ping"*

- List the steps and commands used to complete the tasks.
  fping 167.172.144.11
- List any vulnerabilities discovered.

  List any findings associated to a hacker
  Document the OSI layer where the findings were found.


Linux-Module_default_1637185719
Activities
Terminal
Tue 13:03
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~$ fping 167.172.144.11
167.172.144.11 is alive
sysadmin@UbuntuDesktop:~$ fping 15.199.94.91
15.199.94.91 is unreachable
sysadmin@UbuntuDesktop:~$ fping 167.172.144.11 15.199.94.91 11.199.158.91 11.199.141.91 15.1
99.95.91
167.172.144.11 is alive
15.199.94.91 is unreachable
11.199.158.91 is unreachable
11.199.141.91 is unreachable
15.199.95.91 is unreachable
sysadmin@UbuntuDesktop:~$
```

Summary:

- I ran nping against the four ip addresses hosted in Hollywood, only one of which (167.172.144.11) is alive. As seen in the results, 167.172.144.11 was the only address with no packet loss. The process of port scanning happens on the network layer . This could be the result of a malicious actor having gained access to one of Rockstar Corp's servers and having opened a port for future remote access. This could be resolved by implementing network scanning and logging procedures, patching the network firewall and disabling icmp pinging,

Phase 2: *"Some Syn for Nothin`"*

With the IP(s) found from Phase 1, determine which ports are open:

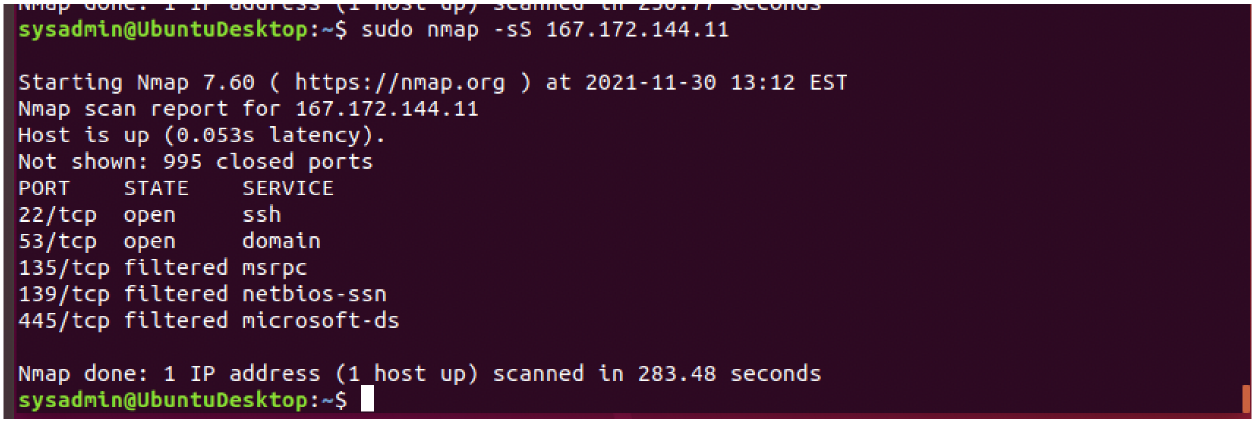
- You will run a SYN SCAN against the IP accepting connections. See **SYN SCAN Instructions** below.

  Sudo nmap -*sS* 167.172.144.11

- Using the results of the SYN SCAN, determine which ports are accepting connections.

  Port 22/tcp is open

- Add these findings to the summary and be sure to indicate at which OSI layer your findings were found.



```
Nmap done: 1 IP address (1 host up) scanned in 230.77 seconds
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 167.172.144.11

Starting Nmap 7.60 ( https://nmap.org ) at 2021-11-30 13:12 EST
Nmap scan report for 167.172.144.11
Host is up (0.053s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
53/tcp   open     domain
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 283.48 seconds
sysadmin@UbuntuDesktop:~$ 
```

Summary:

With the ip address given in the last phase, it is clear that an ssh port is open, as well as a number of remote access service ports. Nmap takes advantage of a number of osi layers, but predominantly uses the transport layer for spidering TCP, UDP, and SCTP protocols for open ports. The best way for RockStar Corp to protect against malicious attacks, while leaving these ports open, would be to increase firewall provisioning, with additional ruling for these ports.

Phase 3: *"I Feel a DNS Change Comin' On"*

With your findings from Phase 2, determine if you can access the server that is accepting connections.

- RockStar typically uses the same default username and password for most of their servers, so try this first:
  - **Username:** jimi
  - **Password:** hendrix

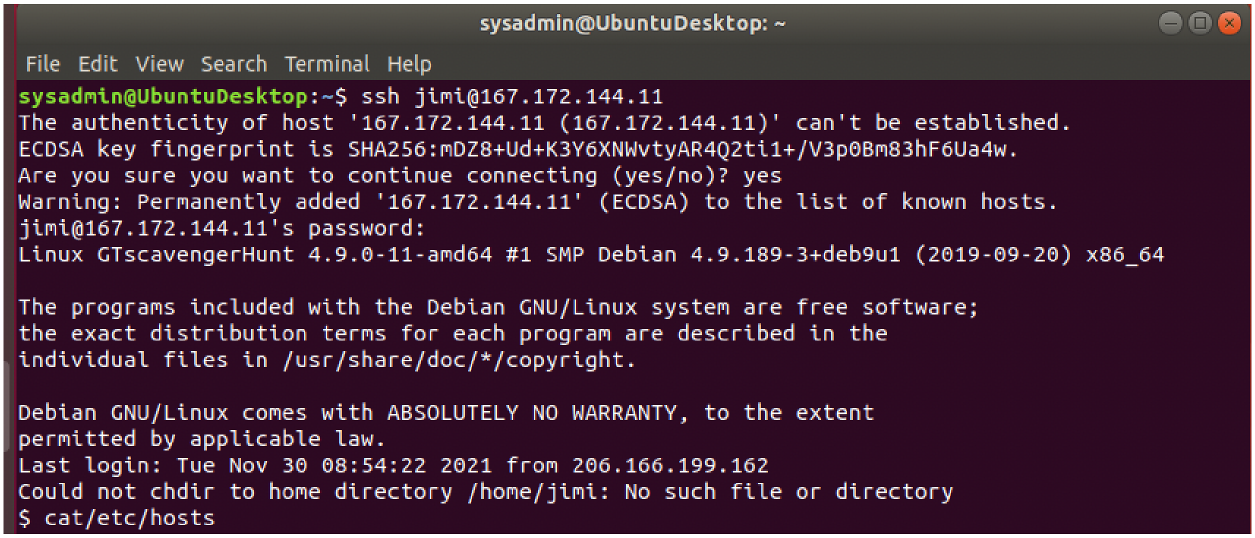
```
sudo ssh jimi@167.172.144.11 was the command

Password: hendrix

cat /etc/hosts

Exit

nslookup 98.137.246.8
```

- Try to figure out which port/service would be used for remote system administration, and then using these credentials, attempt to log into the IP that responded to pings from **Phase 1**.

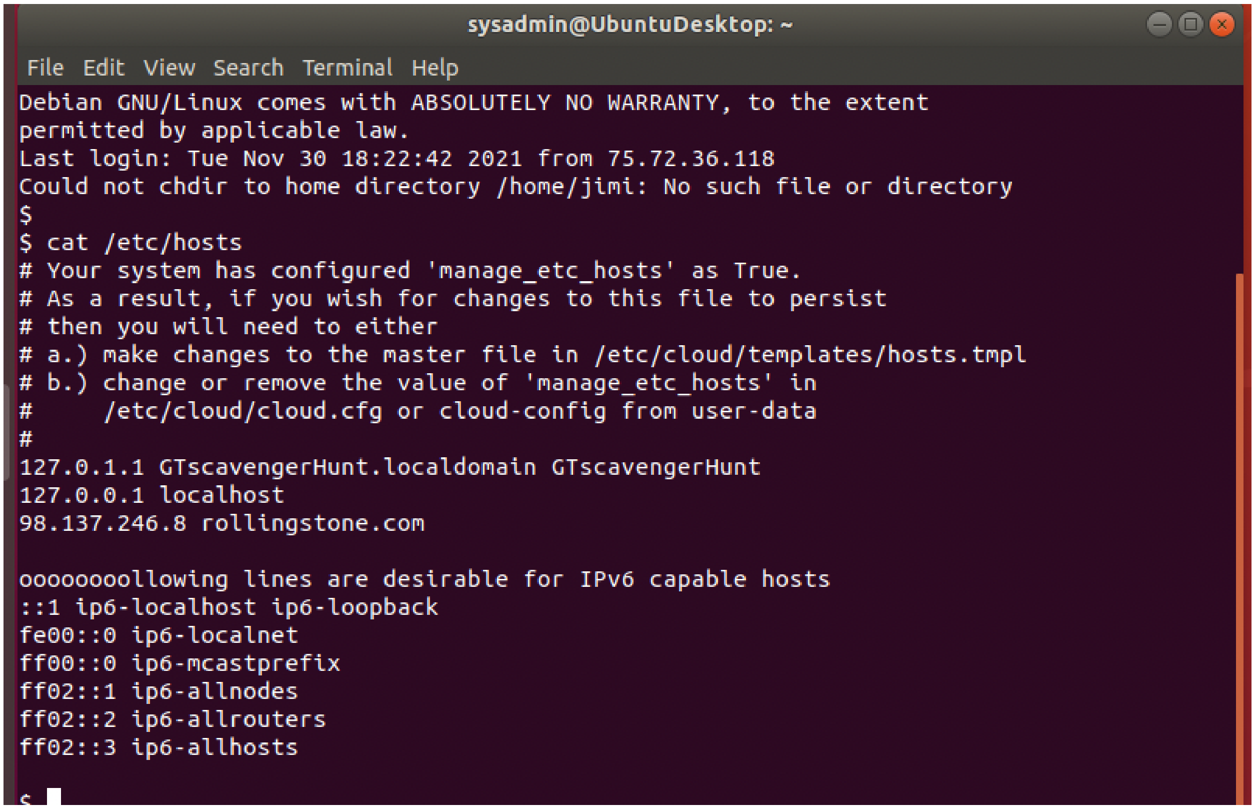
- Add your findings to your summary and be sure to indicate which OSI layer they were found on.

  Summary:

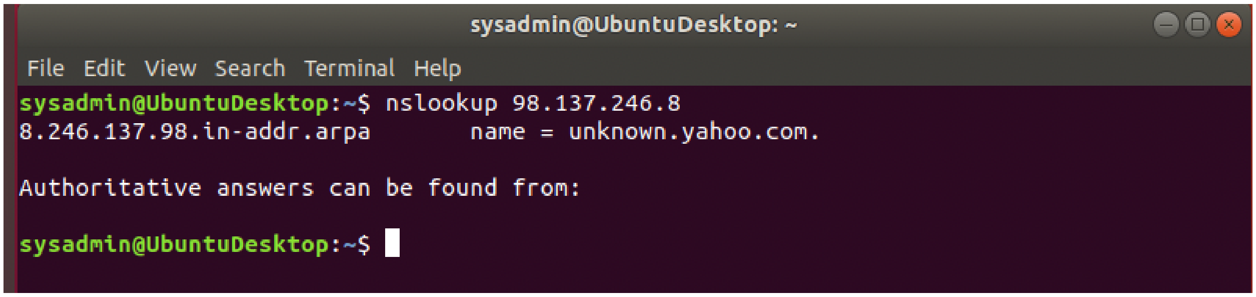
  This hacker has the server and modified the /etc/hosts file to point traffic to another domain. This can be confirmed using nslookup, and my findings are malicious, in fact pointing to an unexpected domain. I strongly recommend closing the port and continuously monitoring their Application layer.


sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
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)? 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: Tue Nov 30 08:54:22 2021 from 206.166.199.162
Could not chdir to home directory /home/jimi: No such file or directory
$ cat/etc/hosts
```


sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Nov 30 18:22:42 2021 from 75.72.36.118
Could not chdir to home directory /home/jimi: No such file or directory
$
$ cat /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

$
```


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:~$
```

Phase 4: *"ShARP Dressed Man"*

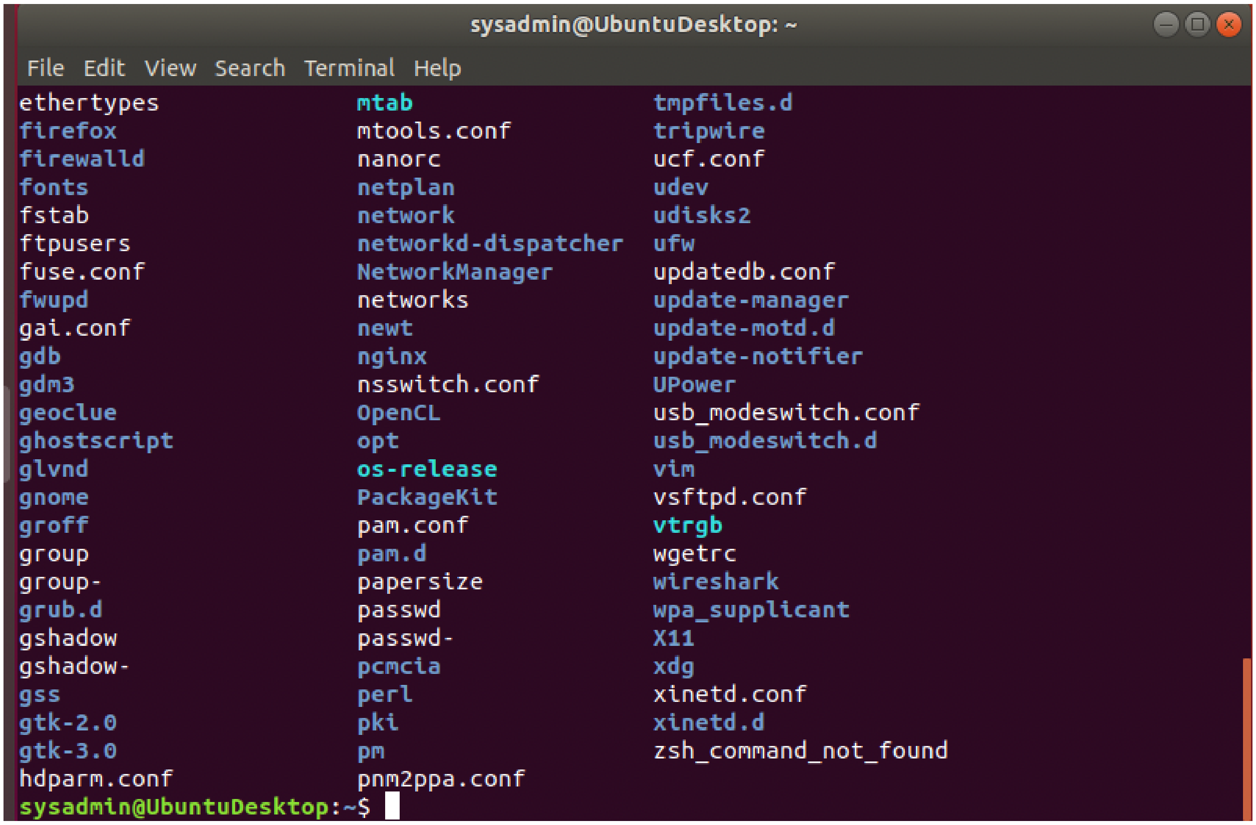
Within the RockStar server that you SSH'd into, and in the same directory as the configuration file from **Phase 3**, the hacker left a note as to where he stored away some packet captures.

- View the file to find where to recover the packet captures.

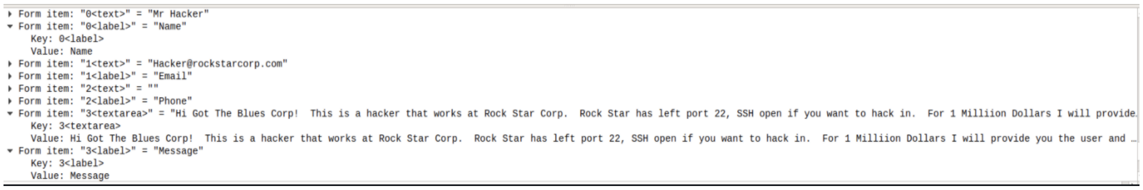
  ssh jimi:167.172.144.11 password hendrix then i use this command to list all the directories and the files inside

  cat /etc/packetcaptureinfo.txt packetcapture

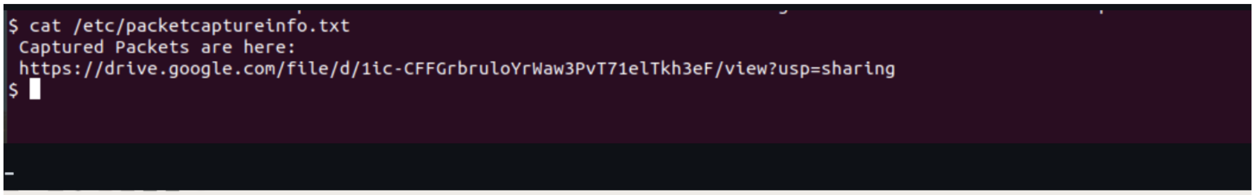
- Use Wireshark to analyze this pcap file and determine if there was any suspicious activity that could be attributed to a hacker.
  - **Hint**: Focus on the ARP and HTTP protocols. Recall the different types of HTTP request methods and be sure to thoroughly examine the contents of these packets.
- Add your findings in your summary and be sure to indicate at which OSI layer they were found.


sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

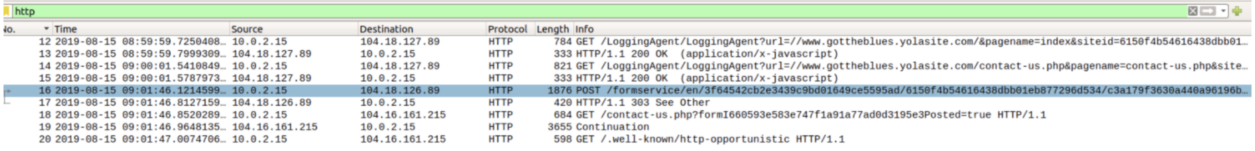
```
ethertypes              mtab                 tmpfiles.d
firefox                 mtools.conf          tripwire
firewalld               nanorc               ucf.conf
fonts                   netplan              udev
fstab                   network              udisks2
ftpusers                networkd-dispatcher  ufw
fuse.conf               NetworkManager       updatedb.conf
fwupd                   networks             update-manager
gai.conf                newt                 update-motd.d
gdb                     nginx                update-notifier
gdm3                    nsswitch.conf        UPower
geoclue                 OpenCL               usb_modeswitch.conf
ghostscript             opt                  usb_modeswitch.d
glvnd                   os-release           vim
gnome                   PackageKit           vsftpd.conf
groff                   pam.conf             vtrgb
group                   pam.d                wgetrc
group-                  papersize            wireshark
grub.d                  passwd               wpa_supplicant
gshadow                 passwd-              X11
gshadow-                pcmcia               xdg
gss                     perl                 xinetd.conf
gtk-2.0                 pki                  xinetd.d
gtk-3.0                 pm                   zsh_command_not_found
hdparm.conf             pnm2ppa.conf
sysadmin@UbuntuDesktop:~$
```



```
▸ Form item: "0<text>" = "Mr Hacker"
▾ Form item: "0<label>" = "Name"
    Key: 0<label>
    Value: Name
▸ Form item: "1<text>" = "Hacker@rockstarcorp.com"
▸ Form item: "1<label>" = "Email"
▸ Form item: "2<text>" = ""
▸ 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 Milliion Dollars I will provide
    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 you want to hack in.  For 1 Milliion Dollars I will provide you the user and …
▾ Form item: "3<label>" = "Message"
    Key: 3<label>
    Value: Message
```



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



No.	Time	Source	Destination	Protocol	Length	Info
12	2019-08-15 08:59:59.7250408…	10.0.2.15	104.18.127.89	HTTP	784	GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616438dbb01…
13	2019-08-15 08:59:59.7999309…	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascript)
14	2019-08-15 09:00:01.5410849…	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&site…
15	2019-08-15 09:00:01.5787973…	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascript)
16	2019-08-15 09:01:46.1214599…	10.0.2.15	104.18.126.89	HTTP	1876	POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196b…
17	2019-08-15 09:01:46.8127159…	104.18.126.89	10.0.2.15	HTTP	420	HTTP/1.1 303 See Other
18	2019-08-15 09:01:46.8520289…	10.0.2.15	104.16.161.215	HTTP	684	GET /contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true HTTP/1.1
19	2019-08-15 09:01:46.9648135…	104.16.161.215	10.0.2.15	HTTP	3655	Continuation
20	2019-08-15 09:01:47.0074706…	10.0.2.15	104.16.161.215	HTTP	598	GET /.well-known/http-opportunistic HTTP/1.1

Summary:

I find out the hacker has MAC address of Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1 this hacker is using OSI layer network layer.He also had note he or she left behind, giving up sensitive information - an open ssh port with user creds in exchange for one million dollars, my result of the hacker redirecting network traffic or backdooring into RockStar Corp's server, set in the server's /etc/hosts. Rockstar corp' should have their firewall denied any unauthorized traffic on port 22 and check for any network modifications.