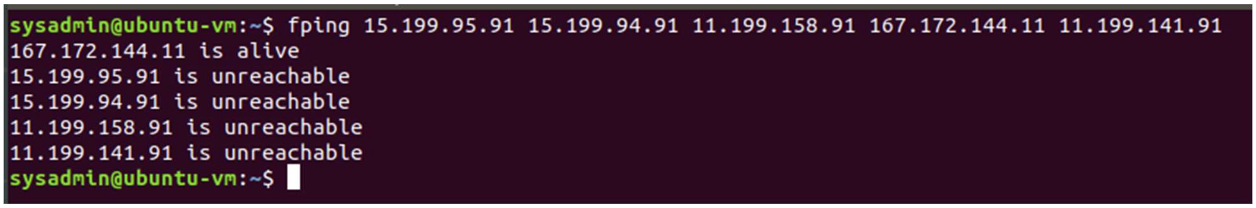
HOMEWORK 8 – GAVIN FAUGHT

Phase 1

- List the steps and commands used to complete the tasks.

```
fping 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91
```



```
sysadmin@ubuntu-vm:~$ fping 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91
167.172.144.11 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
11.199.158.91 is unreachable
11.199.141.91 is unreachable
sysadmin@ubuntu-vm:~$ 
```

- List any vulnerabilities discovered.

RockStar Corp doesn’t want any of their servers, even if they are up, indicating they are accepting connections.

167.172.144.11 is “alive” → meaning, it’s reachable

- List any findings associated to a hacker.

There doesn’t appear to be any malicious activities.

- Document the mitigation recommendations to protect against the discovered vulnerabilities.

It’s the Hollywood application server that’s reachable to the general public. I would recommend “hiding” the server in a LAN with a private IP address, like 192.168.1.1. Also, add a firewall and have “white-list” entries

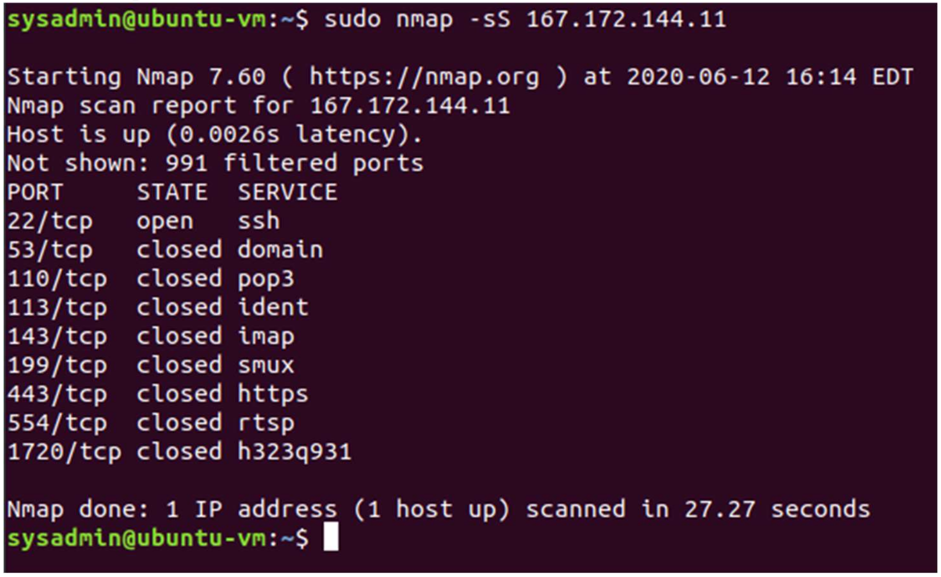
Do some research on hiding servers from users, like the following: https://www.techrepublic.com/article/protect-your-network-servers-by-hiding-them-from-users/

- Document the OSI layer where the findings were found.
  Fping, like ping, operates on Layer 3 (Network) of the OSI Model.

Phase 2

- List the steps and commands used to complete the tasks.

sudo nmap -sS 167.172.144.11



```
sysadmin@ubuntu-vm:~$ sudo nmap -sS 167.172.144.11

Starting Nmap 7.60 ( https://nmap.org ) at 2020-06-12 16:14 EDT
Nmap scan report for 167.172.144.11
Host is up (0.0026s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
53/tcp   closed domain
110/tcp  closed pop3
113/tcp  closed ident
143/tcp  closed imap
199/tcp  closed smux
443/tcp  closed https
554/tcp  closed rtsp
1720/tcp closed h323q931

Nmap done: 1 IP address (1 host up) scanned in 27.27 seconds
sysadmin@ubuntu-vm:~$
```

- List any vulnerabilities discovered.

SSH (port 22) is open.

- List any findings associated to a hacker.

There appears to be no malicious activities; it’s just an open port.

- Document the mitigation recommendations to protect against the discovered vulnerabilities.

The SSH port (22) should be closed so the chance of an intruder is lessened.

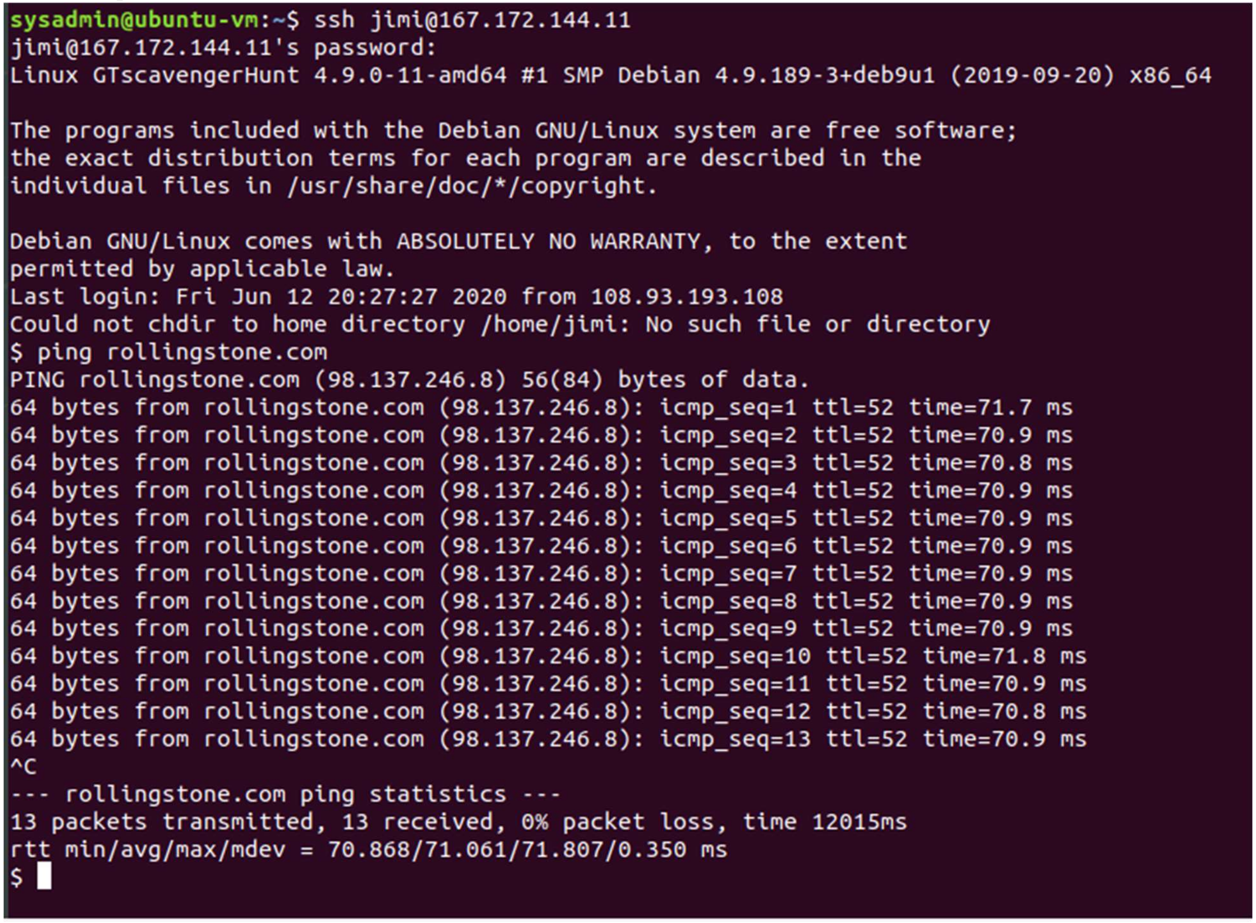
- Document the OSI layer where the findings were found.

The “port scanner” core of Nmap works on Layer 4 (Transport) of the OSI Model.

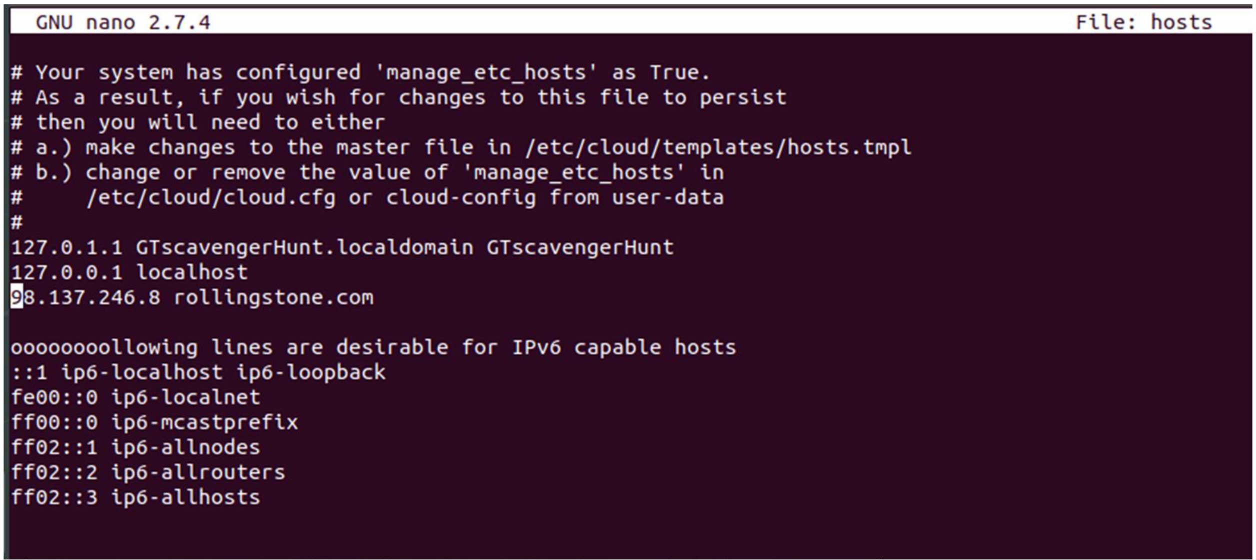
Phase 3

- List the steps and commands used to complete the tasks.

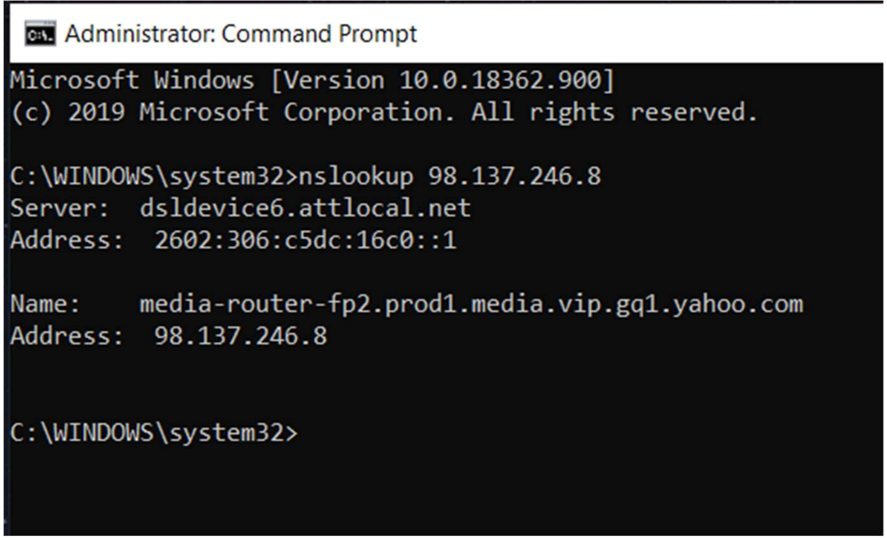
in Linux:
ssh jimi@167.172.144.11
<password 'hendrix'>
nslookup 98.137.246.8
Edit etc/hosts file ---- > remove "98.137.246.8 rollingstone.com"
nslookup 98.137.246.8



```
sysadmin@ubuntu-vm:~$ ssh jimi@167.172.144.11
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: Fri Jun 12 20:27:27 2020 from 108.93.193.108
Could not chdir to home directory /home/jimi: No such file or directory
$ ping rollingstone.com
PING rollingstone.com (98.137.246.8) 56(84) bytes of data.
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=1 ttl=52 time=71.7 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=2 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=3 ttl=52 time=70.8 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=4 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=5 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=6 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=7 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=8 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=9 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=10 ttl=52 time=71.8 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=11 ttl=52 time=70.9 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=12 ttl=52 time=70.8 ms
64 bytes from rollingstone.com (98.137.246.8): icmp_seq=13 ttl=52 time=70.9 ms
^C
--- rollingstone.com ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12015ms
rtt min/avg/max/mdev = 70.868/71.061/71.807/0.350 ms
$
```



```
  GNU nano 2.7.4                                                            File: 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
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>nslookup 98.137.246.8
Server:  dsldevice6.attlocal.net
Address:  2602:306:c5dc:16c0::1

Name:    media-router-fp2.prod1.media.vip.gq1.yahoo.com
Address:  98.137.246.8


C:\WINDOWS\system32>
```

(the final nslookup; the Name has “media” first so it’s legitimate)

- List any vulnerabilities discovered.

The hosts file was writeable.
This whole mess wouldn’t happened if port 22 were closed.

- List any findings associated to a hacker.

The hosts file was modified!!

- Document the mitigation recommendations to protect against the discovered vulnerabilities.

Close the ssh port already.
Make the hosts file only accessible to the superuser (administrator).

- Document the OSI layer where the findings were found.

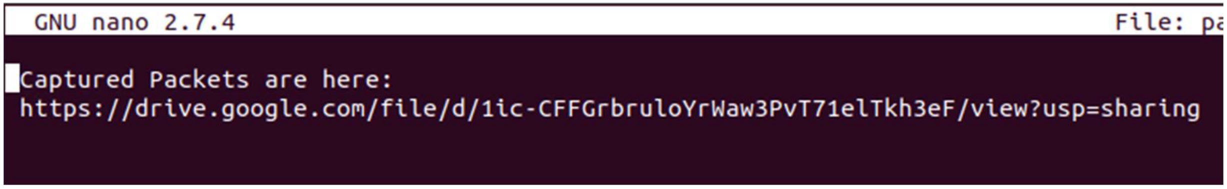
* nslookup troubleshoots DNS issues. DNS is layer 7. Thus, nslookup is on the 7th layer too (Application.)

* ssh is layer 7 too

Phase 4

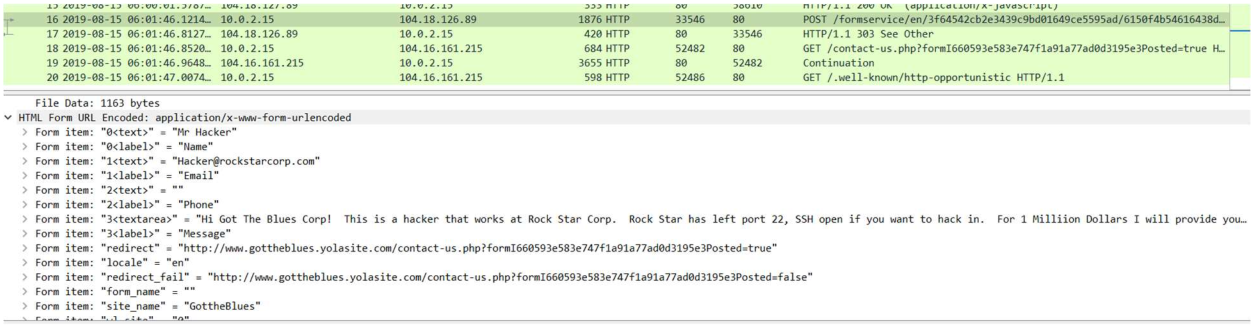
- List the steps and commands used to complete the tasks.

Open "packetcaptureinfo.txt" in the /etc/ directory and copy the link and paste it in a browser.



```
GNU nano 2.7.4                                               File: pa

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

Open secretlogs.pcapng in Wireshark.
Analyze the data.



```
15 2019-08-15 06:00:01.5787… 104.18.127.89   10.0.2.15        555 HTTP   80     58610  HTTP/1.1 200 OK  (application/x-javascript)
16 2019-08-15 06:01:46.1214… 10.0.2.15       104.18.126.89   1876 HTTP   33546  80     POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438d…
17 2019-08-15 06:01:46.8127… 104.18.126.89   10.0.2.15        420 HTTP   80     33546  HTTP/1.1 303 See Other
18 2019-08-15 06:01:46.8520… 10.0.2.15       104.16.161.215   684 HTTP   52482  80     GET /contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true H…
19 2019-08-15 06:01:46.9648… 104.16.161.215  10.0.2.15       3655 HTTP   80     52482  Continuation
20 2019-08-15 06:01:47.0074… 10.0.2.15       104.16.161.215   598 HTTP   52486  80     GET /.well-known/http-opportunistic HTTP/1.1

    File Data: 1163 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "0<text>" = "Mr Hacker"
  > Form item: "0<label>" = "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 you…
  > Form item: "3<label>" = "Message"
  > Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"
  > Form item: "locale" = "en"
  > Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false"
  > Form item: "form_name" = ""
  > Form item: "site_name" = "GottheBlues"
  > Form item: "ul_site" = "0"
```

The above is documentation which shows the hacker is trying to sell information for $1 million. The POST detail specifies that the hacker sent a communication (record #16.)

Nefarious activity is also noted in record #5. ARP spoofing

- List any vulnerabilities discovered.

Port 22 is still open. A static ARP entry is not available for the server.

- List any findings associated to a hacker.

* The hacker created a file called "packetcaptureinfo.txt" in the etc directory.
* ARP spoofing (record #5) and an email which states the hacker has identified a port open and will supply the username and password to anyone who has $1 million dollars (record #16.)
* Also, line-based text data. Records #13 and #15 say "//Pixelated!" That's unusual for a program to have exclamation points. Perhaps the hacker is leaving his/her footprint.

- Document the mitigation recommendations to protect against the discovered vulnerabilities.

* Close port 22 already!
* Prevent ARP spoofing by creating a static ARP entry in the server.

Also:

a. Consider buying a 3rd party tool like XArp. It will help detect if you are being attacked by ARP spoofing.

b. Look at the malware monitoring settings and look for categories and selections that monitor for suspicious ARP traffic from endpoints.

c. Work with your security officer or IT Team to run a spoofing attack to see if the techniques you're using are enough to keep your system safe.

- Document the OSI layer where the findings were found.

Port 22 (SSH) – OSI Layer 7 (Application)
ARP spoofing - OSI Layer 2 (Data link)
Analyzing HTTP traffic: OSI Layer 7 (Application)

<u>Gavin's Corner – More about OSI</u>

1) Layer 8 is used to refer to the "user" or "political" layer on top of the 7 layer OSI model of computer networking
2) Layers 1 to 3 are considered the media layers. Layers 4 to 7 are considered the hosts layer
3) The OSI Model was defined in ISO/IEC 7498 which consists of the following parts:
   - ISO/IEC 7498.1 -> The Basic Model
   - ISO/IEC 7498.2 -> Security Architecture
   - ISO/IEC 7498.3 -> Naming and Addressing
   - ISO/IEC 7498.4 -> Management Framework

   ISO = International Organization for Standardizations

   IEC = International Electrotechnical Commission

4) The birth of the OSI model came about in the early 1970s.