Rachel Murphy

April 19, 2021

Networking Fundamentals Homework: Rocking your Network!

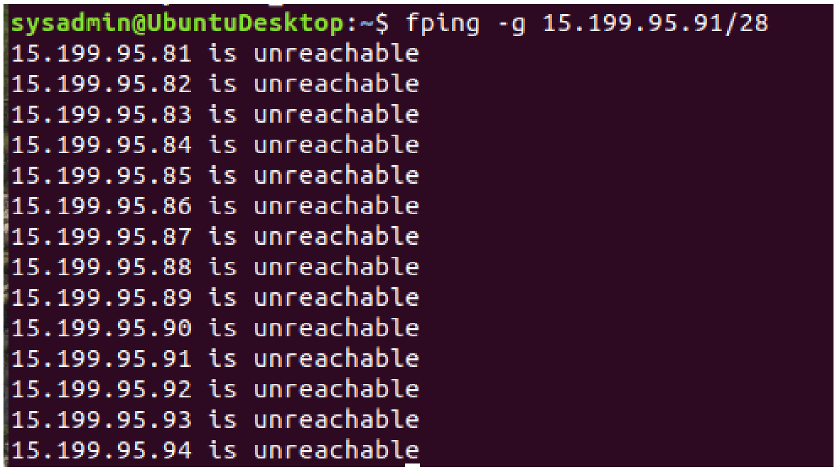
Phase 1: *"I'd like to Teach the World to Ping"*

Steps & Commands:

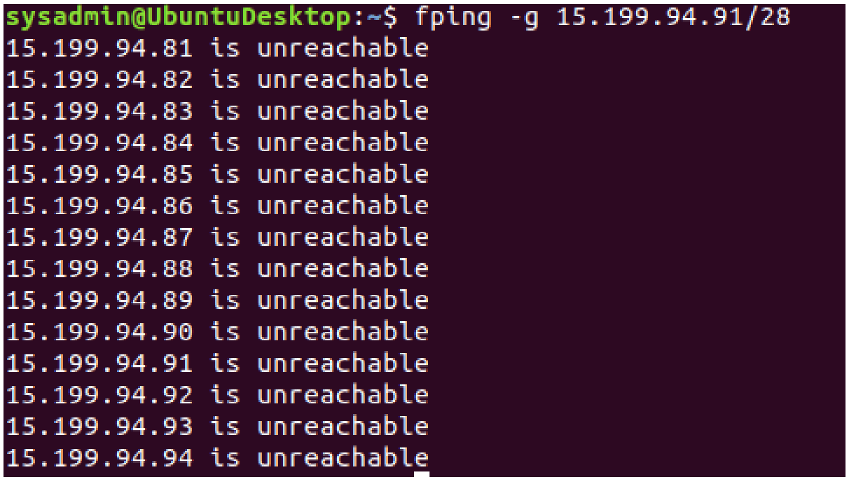
Extracted Hollywood IP Addresses from excel file provided.

IP Address	Hollywood Servers	Host (Up/Down)
15.199.95.91/28	Hollywood Database Servers	Down
15.199.94.91/28	Hollywood Web Servers	Down
11.199.158.91/28	Hollywood Web Servers	Down
167.172.144.11/32	Hollywood Application Servers	Up
11.199.141.91/28	Hollywood Application Servers	Down

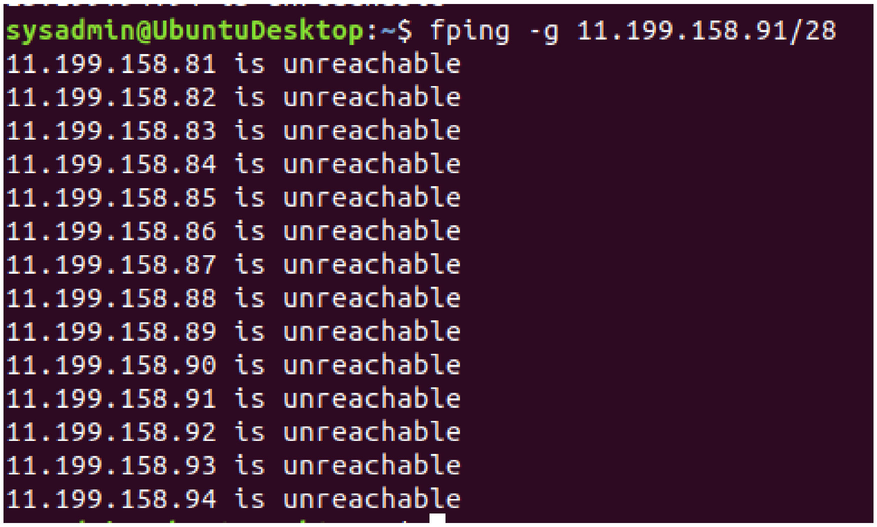
Ran fping -g against all IPs to determine which hosts were responding.



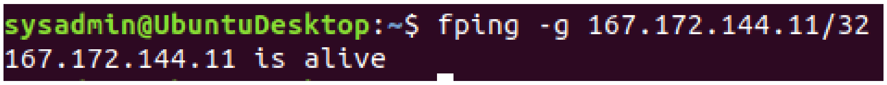
```
sysadmin@UbuntuDesktop:~$ fping -g 15.199.95.91/28
15.199.95.81 is unreachable
15.199.95.82 is unreachable
15.199.95.83 is unreachable
15.199.95.84 is unreachable
15.199.95.85 is unreachable
15.199.95.86 is unreachable
15.199.95.87 is unreachable
15.199.95.88 is unreachable
15.199.95.89 is unreachable
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
```



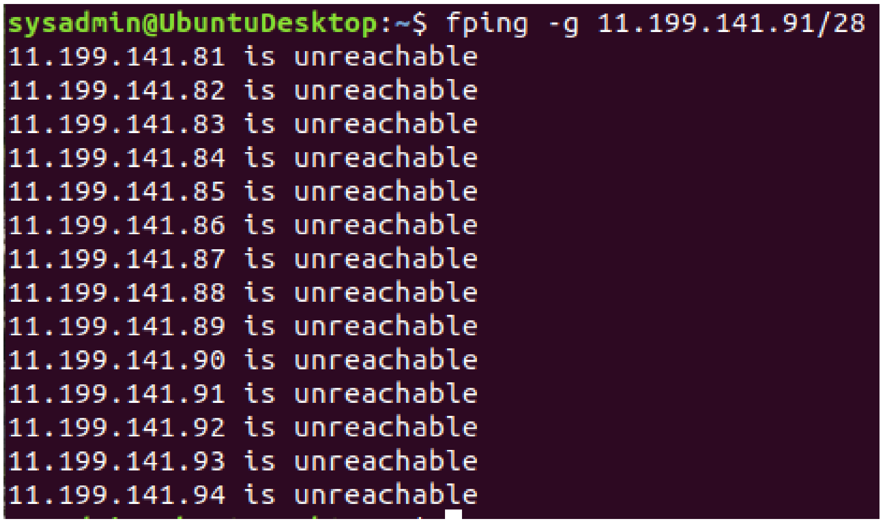
```
sysadmin@UbuntuDesktop:~$ fping -g 15.199.94.91/28
15.199.94.81 is unreachable
15.199.94.82 is unreachable
15.199.94.83 is unreachable
15.199.94.84 is unreachable
15.199.94.85 is unreachable
15.199.94.86 is unreachable
15.199.94.87 is unreachable
15.199.94.88 is unreachable
15.199.94.89 is unreachable
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:~$ 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
```

Summary:

Phase 1

- Determined IP ranges to scan were 15.199.95.91, 15.199.95.94.91, 11.199.158.91, 167.172.144.11, and 11.199.141.91.

    - Used the following commands to run fping:

        - fping -g 15.199.95.91/28
        - fping -g 15.199.94.91/28
        - fping -g 11.199.158.91/28
        - fping -g 167.172.144.11/32
        - fping -g 11.199.141.91/28

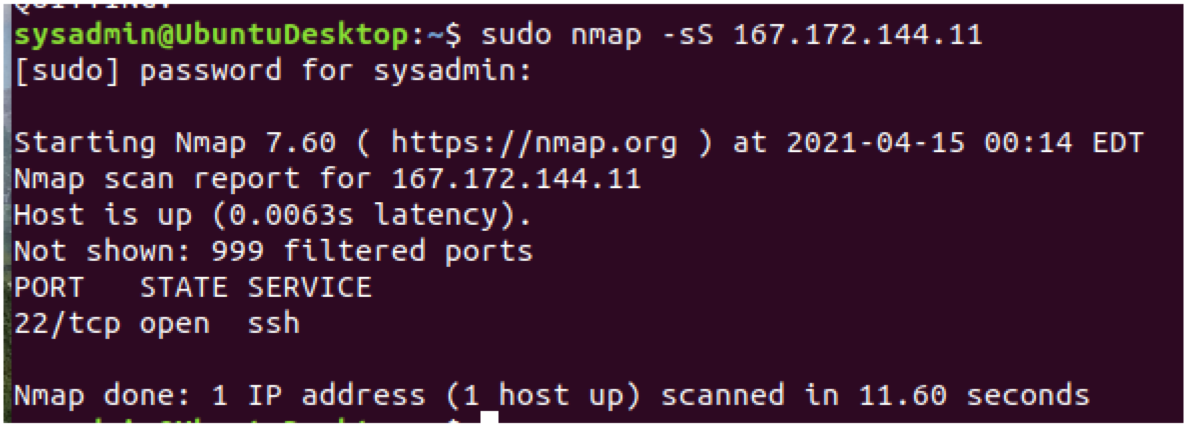
- Determined a potential vulnerability that IP 167.172.144.11 is responding to ping requests.

    - Since RockStar Corp doesn't want to respond to any requests, this is a vulnerability.

- Recommended mitigation strategy is to restrict allowing ICMP echo requests against IP 167.172.144.11 to prevent successful responses from PING requests.

- This occurred on the network layer as Ping uses IP addresses and IPs are used on the network layer (Layer 3).

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

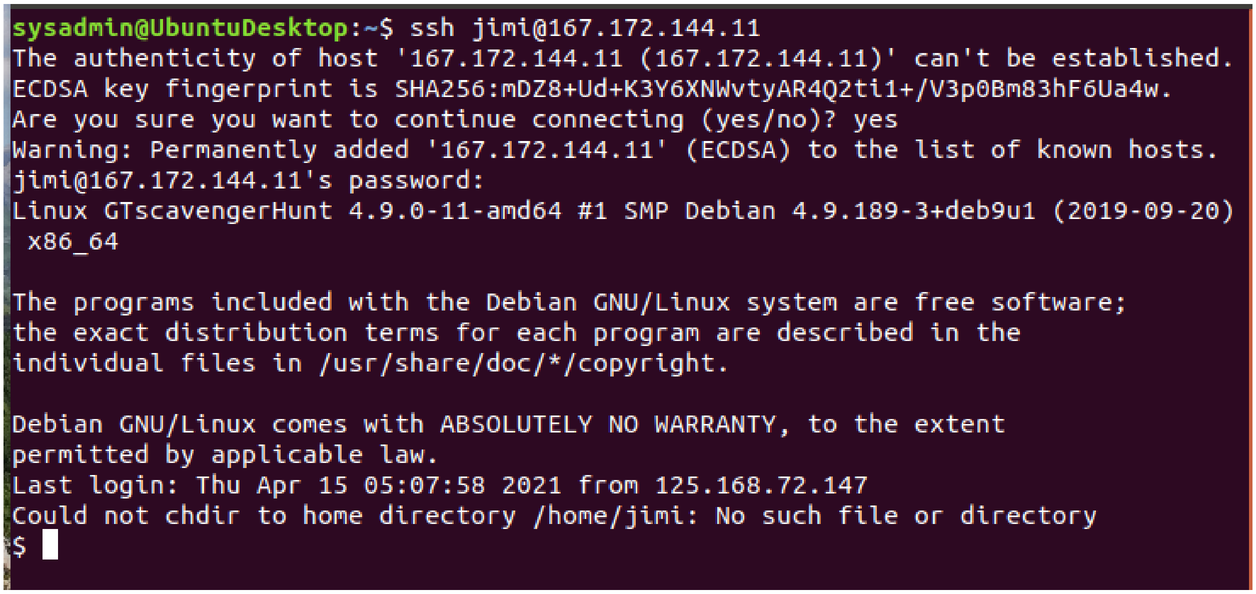


```
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 167.172.144.11
[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2021-04-15 00:14 EDT
Nmap scan report for 167.172.144.11
Host is up (0.0063s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds
```

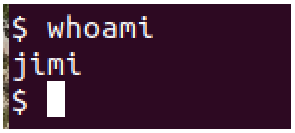
Summary:

- Used the following command to SYN SCAN the vulnerable IP address
  - `sudo nmap -sS 167.172.144.11`
- Any network vulnerabilities discovered.
  - A vulnerability from the SYN SCAN was discovered. The SSH service on port 22 is open.
- Findings associated with a hacker.
  - A hacker could infiltrate the network on this port.
- Recommended mitigation strategy
  - It is recommended to close the port or shutdown the SSH service if not in use.
- Document the OSI layer where the findings were found.
  - The open TCP port was discovered on the transport layer (layer 4) of the OSI model.

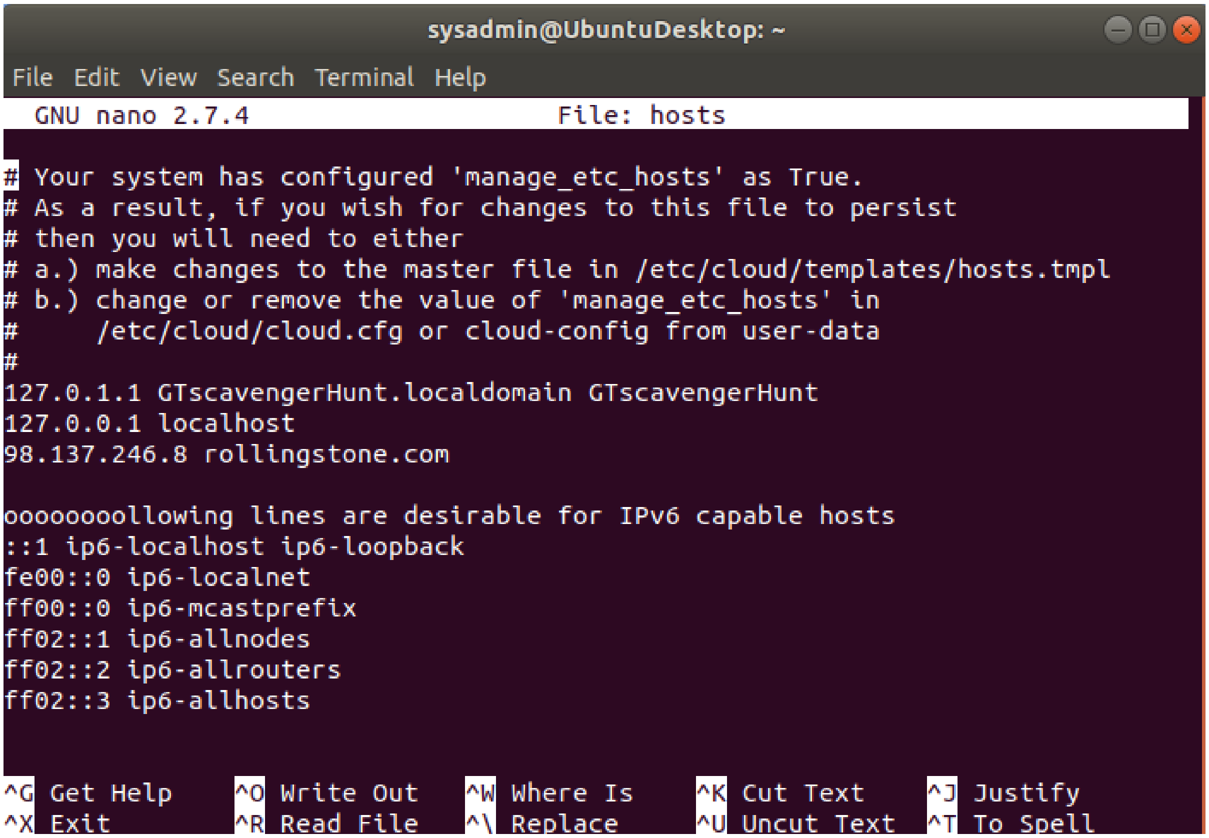
Phase 3: *"I Feel a DNS Change Comin' On"*



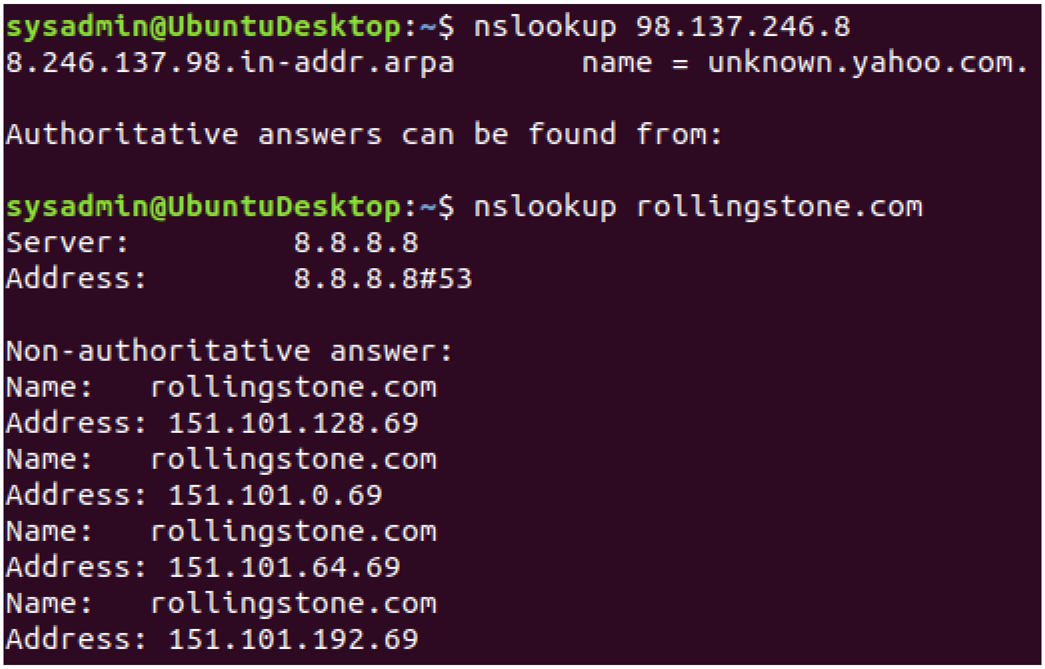
```
sysadmin@UbuntuDesktop:~$ ssh jimi@167.172.144.11
The authenticity of host '167.172.144.11 (167.172.144.11)' can't be established.
ECDSA key fingerprint is SHA256:mDZ8+Ud+K3Y6XNWvtyAR4Q2ti1+/V3p0Bm83hF6Ua4w.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '167.172.144.11' (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: Thu Apr 15 05:07:58 2021 from 125.168.72.147
Could not chdir to home directory /home/jimi: No such file or directory
$ 
```



```
$ whoami
jimi
$ 
```


sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
  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


^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell
```



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

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

Summary:

- Used the following commands to determine why employees cannot access rollingstone.com.

    - `ssh jimi@167.172.144.11`
    - `cd/etc`
    - `nano hosts`
    - `nslookup 98.137.246.8`

- Any network vulnerabilities discovered.
    - **DNS cache poisoning**
    - IP address 98.137.246.8 is being used for rollingstone.com
- Findings associated with a hacker.
    - A hacker is redirecting traffic from the rollingstone.com IP address 151.101.128.69 to an unknown.yahoo.com IP address 98.137.246.8
- Recommended mitigation strategy
    - It is recommended to use Public Key Infrastructure (PKI) on the server to ensure that digital certificates will be used to authenticate your ssh sessions. Additionally, you could implement file monitoring on /etc/hosts to identify any changes.
- Document the OSI layer where the findings were found.
    - This DNS attack occurs at the **application layer (layer 7)** of the OSI model.

An instance of DNS cache poisoning found on the Hollywood server. A fake IP address was configured in the /etc/hosts file, which is redirecting traffic to unknown.yahoo.com *instead* of to rollingstone.com. This attack occurs at the application layer (layer 7) of the OSI model.

Phase 4: *"ShARP Dressed Man"*

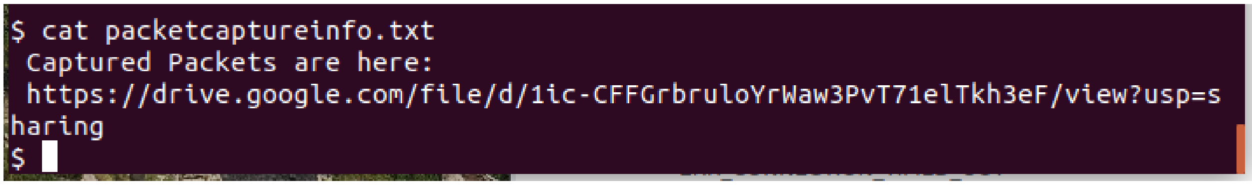
Steps & Commands:
Locate secretlogs.pcapng file:

```
ssh jimi@167.172.144.11
```

```
cd etc
```

```
cat packetcaptureinfo.txt
```

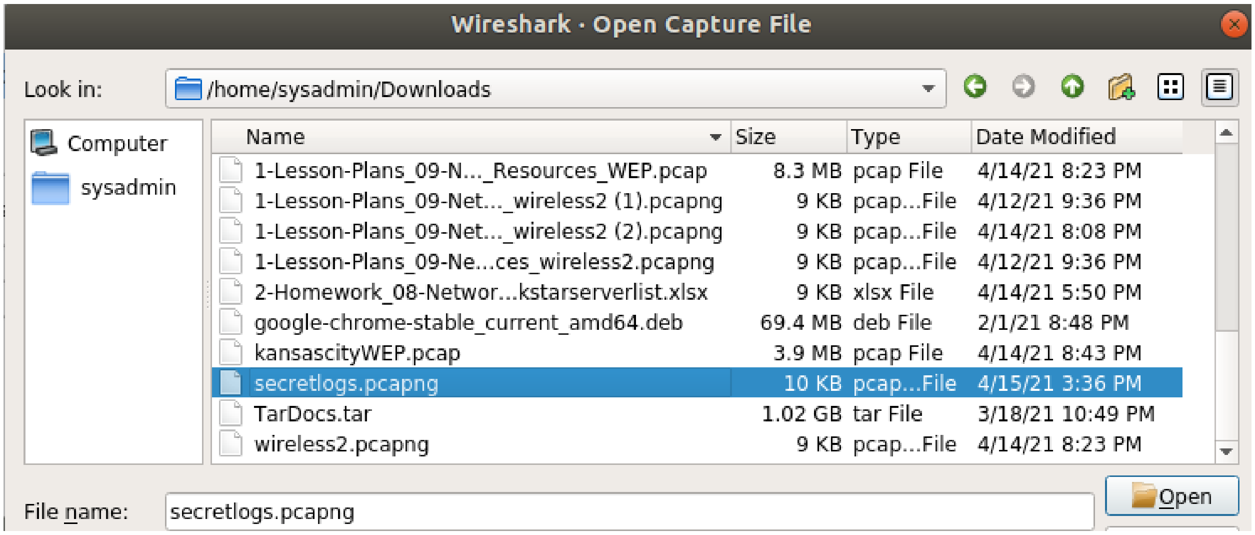
Visited this website and downloaded the secretlogs.pcap file.



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

secretlogs.pcapng

Import the secretlogs.pcapng file into Wireshark



Wireshark · Open Capture File

Look in: /home/sysadmin/Downloads

Name	Size	Type	Date Modified
1-Lesson-Plans_09-N..._Resources_WEP.pcap	8.3 MB	pcap File	4/14/21 8:23 PM
1-Lesson-Plans_09-Net..._wireless2 (1).pcapng	9 KB	pcap...File	4/12/21 9:36 PM
1-Lesson-Plans_09-Net..._wireless2 (2).pcapng	9 KB	pcap...File	4/14/21 8:08 PM
1-Lesson-Plans_09-Ne...ces_wireless2.pcapng	9 KB	pcap...File	4/12/21 9:36 PM
2-Homework_08-Networ...kstarserverlist.xlsx	9 KB	xlsx File	4/14/21 5:50 PM
google-chrome-stable_current_amd64.deb	69.4 MB	deb File	2/1/21 8:48 PM
kansascityWEP.pcap	3.9 MB	pcap File	4/14/21 8:43 PM
secretlogs.pcapng	10 KB	pcap...File	4/15/21 3:36 PM
TarDocs.tar	1.02 GB	tar File	3/18/21 10:49 PM
wireless2.pcapng	9 KB	pcap...File	4/14/21 8:23 PM

File name: secretlogs.pcapng

Utilized the arp filter to discover a possible ARP spoofing attack and utilized the http.request.method == “POST” filter and discovered a suspicious message.

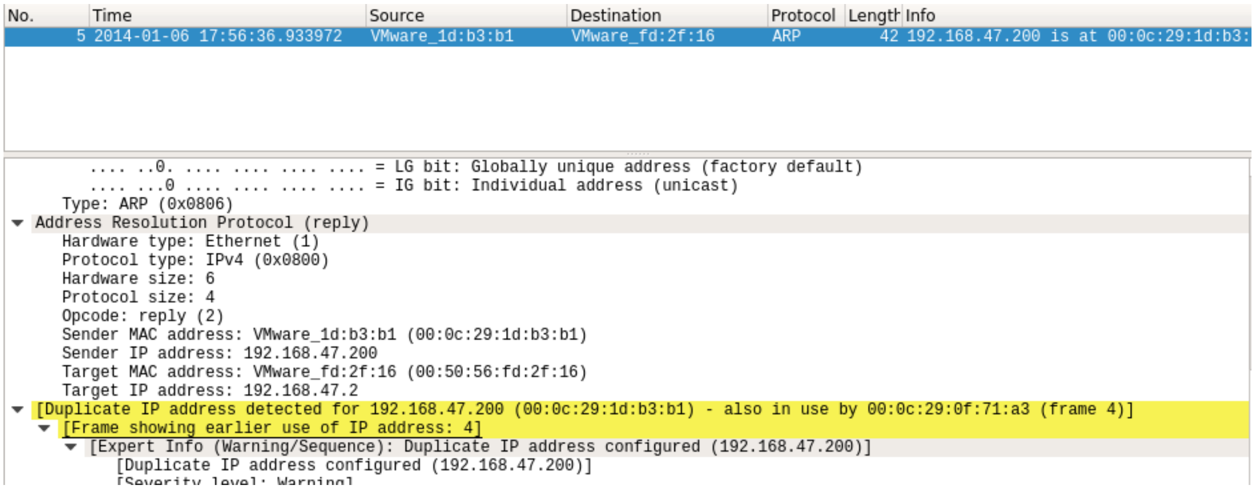
Summary (ARP):

The filter used in Wireshark after importing the packetcaptureinfo.txt file was *arp*. A potential vulnerability: address resolution protocol (ARP) spoofing was found.

After locating and analyzing the suspicious pcap file on wireshark, a duplicate IP address was found after filtering through the ARP packets. Duplicate IP addresses can be a vulnerability known as address resolution protocol (ARP) spoofing.
The duplicate IP is 192.168.47.200. The Hollywood server is utilizing this IP with the following MAC address (00:0c:29:1d:b3:b1). A hacker is utilizing this IP with a different MAC address (00:0c:29:0f:71:a3).

- Security risk of ARP spoofing is that an attacker can intercept messages and gain access to confidential information.
- **Mitigation strategies for ARP poisoning attack**
  - Create static ARP entries
  - Implement ARP spoofing detection software
- **ARP Spoofing occurs at the Data Link Layer (Layer 2).**

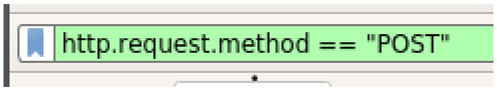
Screenshot of Wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
5	2014-01-06 17:56:36.933972	VMware_1d:b3:b1	VMware_fd:2f:16	ARP	42	192.168.47.200 is at 00:0c:29:1d:b3:

```
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
    Sender IP address: 192.168.47.200
    Target MAC address: VMware_fd:2f:16 (00:50:56:fd:2f:16)
    Target IP address: 192.168.47.2
▼ [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)]
  ▼ [Frame showing earlier use of IP address: 4]
    ▼ [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.47.200)]
        [Duplicate IP address configured (192.168.47.200)]
        [Severity level: Warning]
```

Summary (HTTP):



```
http.request.method == "POST"
```

After filtering for http.request.method == “POST” on Wireshark, the following source IP 10.0.2.15 and Destination IP 104.18.126.89 were corresponding using forms.yola.com.

A suspicious message was sent to the following location:

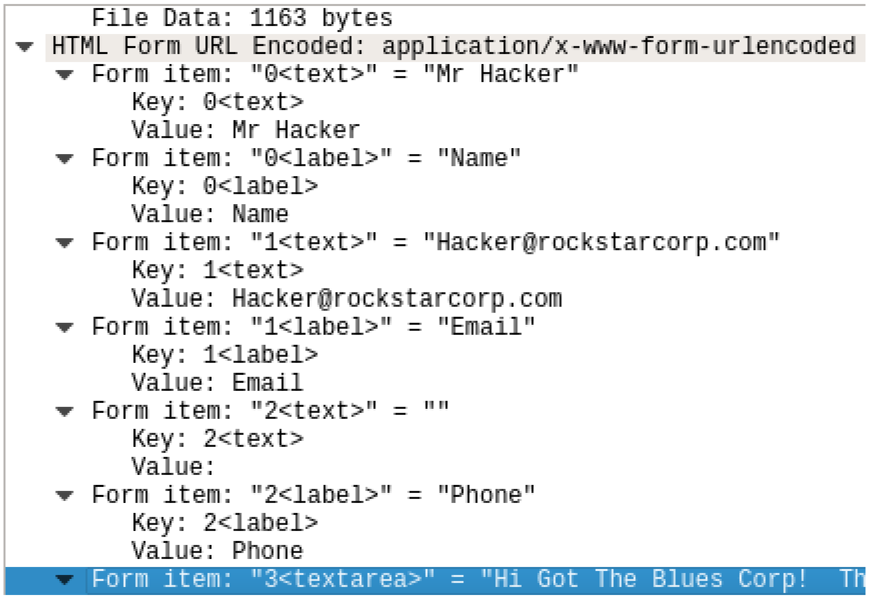
http://www.gottheblues.yolasite.com/contact-us.php on Thursday, August 2019 at 13:01:47 GMT.

The contact details of the hacker from the form:

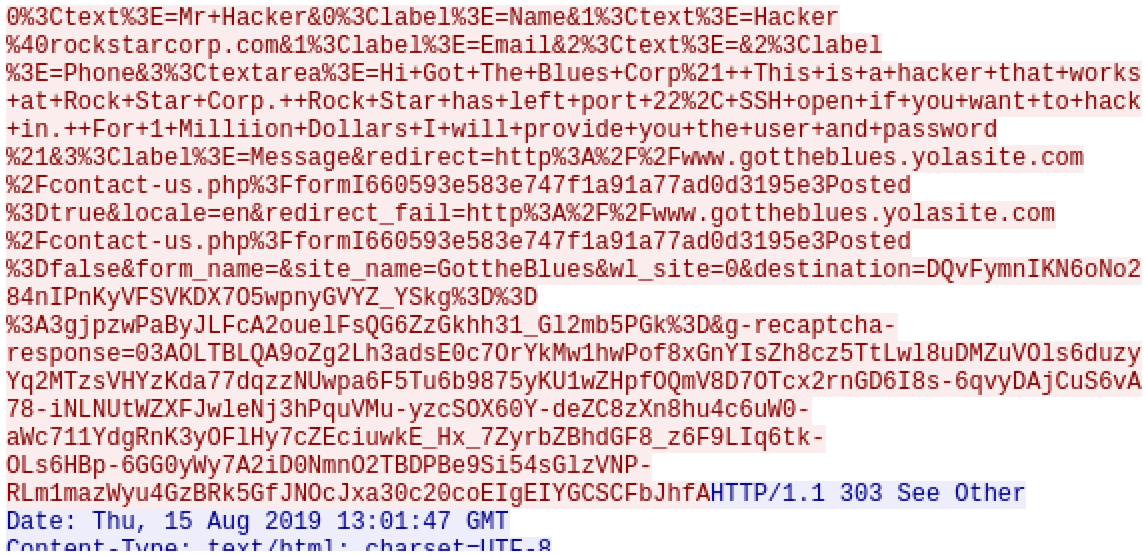
Name: Mr. Hacker

Email: Hacker@rockstarcorp.com

Message: 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!



```
      File Data: 1163 bytes
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▼ Form item: "0<text>" = "Mr Hacker"
      Key: 0<text>
      Value: Mr Hacker
  ▼ Form item: "0<label>" = "Name"
      Key: 0<label>
      Value: Name
  ▼ Form item: "1<text>" = "Hacker@rockstarcorp.com"
      Key: 1<text>
      Value: Hacker@rockstarcorp.com
  ▼ Form item: "1<label>" = "Email"
      Key: 1<label>
      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!  Th
```



```
0%3Ctext%3E=Mr+Hacker&0%3Clabel%3E=Name&1%3Ctext%3E=Hacker
%40rockstarcorp.com&1%3Clabel%3E=Email&2%3Ctext%3E=&2%3Clabel
%3E=Phone&3%3Ctextarea%3E=Hi+Got+The+Blues+Corp%21++This+is+a+hacker+that+works
+at+Rock+Star+Corp.++Rock+Star+has+left+port+22%2C+SSH+open+if+you+want+to+hack
+in.++For+1+Milliion+Dollars+I+will+provide+you+the+user+and+password
%21&3%3Clabel%3E=Message&redirect=http%3A%2F%2Fwww.gottheblues.yolasite.com
%2Fcontact-us.php%3FformI660593e583e747f1a91a77ad0d3195e3Posted
%3Dtrue&locale=en&redirect_fail=http%3A%2F%2Fwww.gottheblues.yolasite.com
%2Fcontact-us.php%3FformI660593e583e747f1a91a77ad0d3195e3Posted
%3Dfalse&form_name=&site_name=GottheBlues&wl_site=0&destination=DQvFymnIKN6oNo2
84nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg%3D%3D
%3A3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31_Gl2mb5PGk%3D&g-recaptcha-
response=03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzy
Yq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA
78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6uW0-
aWc711YdgRnK3yOFlHy7cZEciuwkE_Hx_7ZyrbZBhdGF8_z6F9LIq6tk-
OLs6HBp-6GG0yWy7A2iD0NmnO2TBDPBe9Si54sGlzVNP-
RLm1mazWyu4GzBRk5GfJNOcJxa30c20coEIgEIYGCSCFbJhfAHTTP/1.1 303 See Other
Date: Thu, 15 Aug 2019 13:01:47 GMT
Content-Type: text/html; charset=UTF-8
```

- Recommended mitigation strategy
    - Restrict permissions to the ssh configuration files
    - Conduct SSH audits and monitor SSH audit logs for suspicious activity
    - Fire Mr. Hacker, change usernames and passwords for the ssh

- Document the OSI layer where the findings were found.
    - This HTTP vulnerability occurs at the **application layer (layer 7)** of the OSI model.