Phase 1
- 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
- Findings
- Vulnerabilities and Mitigation Suggestions

Phase 2
- Findings

Phase 3
- Findings

Phase 4
- Suspicious ARP Packet
- Suspicious HTTP Packet

Phase 1

For each IP range for Hollywood networks, the IPs scanned were the IPS for the available hosts. This didn't include the first and last IP -- the network and broadcast addresses -- in the range.

15.199.95.91/28 → Hollywood Database Servers

Used the following command in Bash:

```
fping -g 15.199.95.91/28
```

Received the following output:

```
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
```

15.199.94.91/28 → Hollywood Web Servers

Used the following command in Bash:

```
fping -g 15.199.94.91/28
```

Received the following output:

```
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
```

11.199.158.91/28 → Hollywood Web Servers

Used the following command in Bash:

```
fping -g 11.199.158.91/28
```

Received the following output:

```
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
```

167.172.144.11/32 → Hollywood Application Servers

Used the following command in Bash:

```
fping -g 167.172.144.11/32
```

Received the following output:

```
167.172.144.11 is alive
```

11.199.141.91/28 → Hollywood Application Servers

Used the following command in Bash:

```
fping -g 11.199.141.91/28
```

Received the following output:

```
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
```

Findings

The only IP accepting connections is “167.172.144.11”. My findings are located in layer 3 of the OSI Model.

Mitigation Strategies

- A firewall could disable ICMP so we wouldn’t know if “167.172.144.11” reachable.

Phase 2

I ran the following scan:

```
sudo nmap -sS 167.172.144.11
```

I received the following results:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-11-09 21:58 EST
Nmap scan report for 167.172.144.11
Host is up (0.0039s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 12.10 seconds
```

Findings

Port 22/TCP (SSH) is open. SYN scans are run on layer 4 of the OSI Model.

Mitigation Strategies

- The following article outlines how to block NMAP scans from a given IP address: https://success.trendmicro.com/solution/TP000087920-How-do-I-block-NMAP-port-scans.
- A good firewall should be able to protect against NMAP scans.

Phase 3

I used the following command to connect the “167.172.144.11” machine:

```
ssh jimi@167.172.144.11
```

I found the following entry in the “/etc/hosts” file on the “167.172.144.11” machine:

```
98.137.246.8 rollingstone.com
```

I would attribute the above entry to an attacker. I used the following command to find the actual name that the “98.137.246.8” IP address is tied to:

```
nslookup 98.137.246.8
```

I received the following results:

```
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Name:    unknown.yahoo.com
```

```
Address:  98.137.246.8
```

Findings

In the Hollywood office, “rollingstone.com” was resolving to “98.137.246.8”. “98.137.246.8” is actually tied to “unknown.yahoo.com”. DNS operates on layer 7 of the OSI Model.

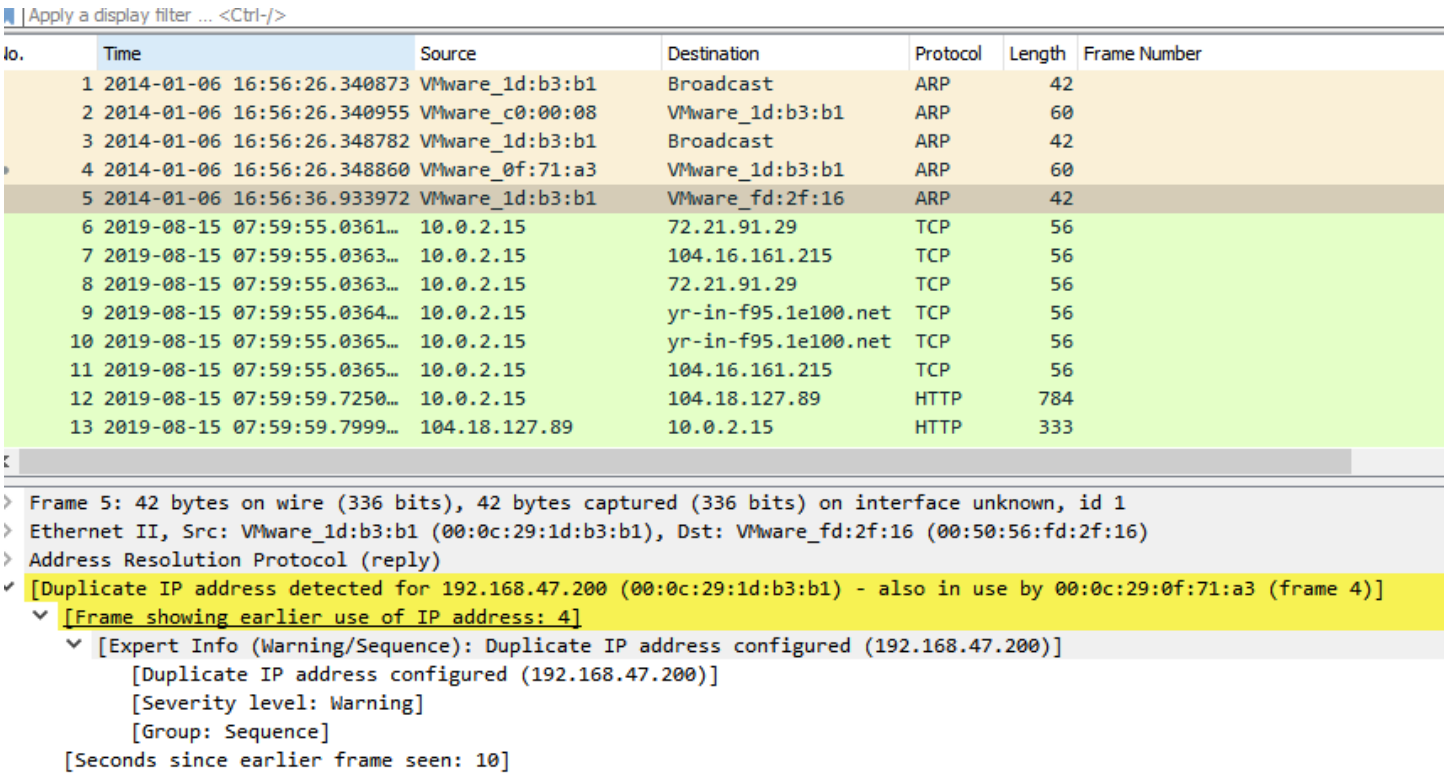
Mitigation Strategies

- User Education
    - Instruct users on how to spot potential DNS poisoning. This would include making sure they don’t ignore the SSL warning that could appear or making sure they visually confirm the website they’re visiting is indeed what they’re intending on visiting.
- The company could prevent any and all external Internet traffic.
- An alert should be generated anytime the “/etc/hosts” file is edited. This is most likely a malware indicator. Got this from this website: https://followcybersecurity.com/2018/12/06/cybersecurity-security-importance-of-etc-host-file/
- The fact that it’s a known fact that the company uses an “initial” username and password combination is really bad practice. The company should generate secure passwords for any SSH user.
- The company could require public/private key access for SSH instead of username/password.

Phase 4

Suspicious ARP Packet

We can attribute the following ARP packet to a hacker:



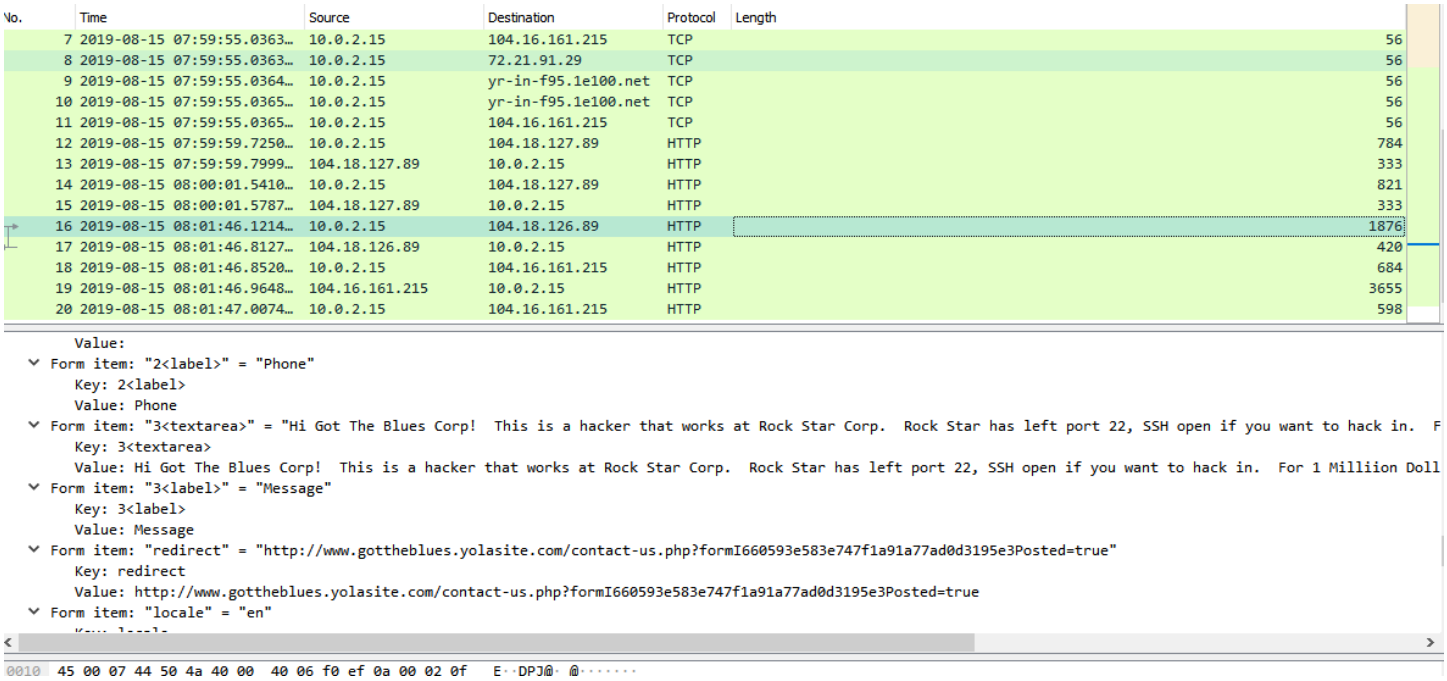
That is most likely a hacker attempting to spoof a MAC address. ARP operates between layer 2 and layer 3 of the OSI model.

Mitigation Strategies

- Static ARP'ing
- Set up a VPN that users must connect to in order to access the network
- There are many other things that can be done. I found numerous on the following website: https://www.indusface.com/blog/protect-arp-poisoning/.

Suspicious HTTP Packet

We can attribute the following packet to a hacker:



No.	Time	Source	Destination	Protocol	Length
7	2019-08-15 07:59:55.0363…	10.0.2.15	104.16.161.215	TCP	56
8	2019-08-15 07:59:55.0363…	10.0.2.15	72.21.91.29	TCP	56
9	2019-08-15 07:59:55.0364…	10.0.2.15	yr-in-f95.1e100.net	TCP	56
10	2019-08-15 07:59:55.0365…	10.0.2.15	yr-in-f95.1e100.net	TCP	56
11	2019-08-15 07:59:55.0365…	10.0.2.15	104.16.161.215	TCP	56
12	2019-08-15 07:59:59.7250…	10.0.2.15	104.18.127.89	HTTP	784
13	2019-08-15 07:59:59.7999…	104.18.127.89	10.0.2.15	HTTP	333
14	2019-08-15 08:00:01.5410…	10.0.2.15	104.18.127.89	HTTP	821
15	2019-08-15 08:00:01.5787…	104.18.127.89	10.0.2.15	HTTP	333
16	2019-08-15 08:01:46.1214…	10.0.2.15	104.18.126.89	HTTP	1876
17	2019-08-15 08:01:46.8127…	104.18.126.89	10.0.2.15	HTTP	420
18	2019-08-15 08:01:46.8520…	10.0.2.15	104.16.161.215	HTTP	684
19	2019-08-15 08:01:46.9648…	104.16.161.215	10.0.2.15	HTTP	3655
20	2019-08-15 08:01:47.0074…	10.0.2.15	104.16.161.215	HTTP	598

```
    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 port 22, SSH open if you want to hack in.  F
    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 Doll
  Form item: "3<label>" = "Message"
    Key: 3<label>
    Value: Message
  Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"
    Key: redirect
    Value: http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true
  Form item: "locale" = "en"
```

```
0010  45 00 07 44 50 4a 40 00  40 06 f0 ef 0a 00 02 0f   E··DPJ@· @·····
```

This was found in an HTTP packet which is at the application layer of the OSI model.

Mitigation Strategies

I don’t know that you can mitigate against the above issue. The hacker is offering to sell the company’s information but it’s sending this information from inside the network. I think you’d have to prevent the ARP spoof attack and the SSH vulnerability in order to prevent the above.