Cybersecurity

Module 8 Challenge Submission File

Networking Fundamentals: Rocking your Network

Make a copy of this document to work in, and then 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 `fping` against the IP ranges:

```
Fping 15.199.95.91 15.199.94.91 11.199.158.91 161.35.96.20 11.199.141.91
```

2. Summarize the results of the `fping` command(s):

```
Determined after running that 161.35.96.20 is alive while the others are all
unreachable
```

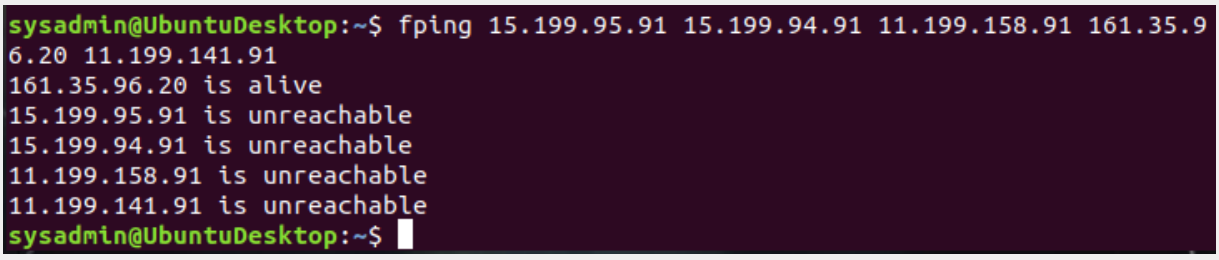
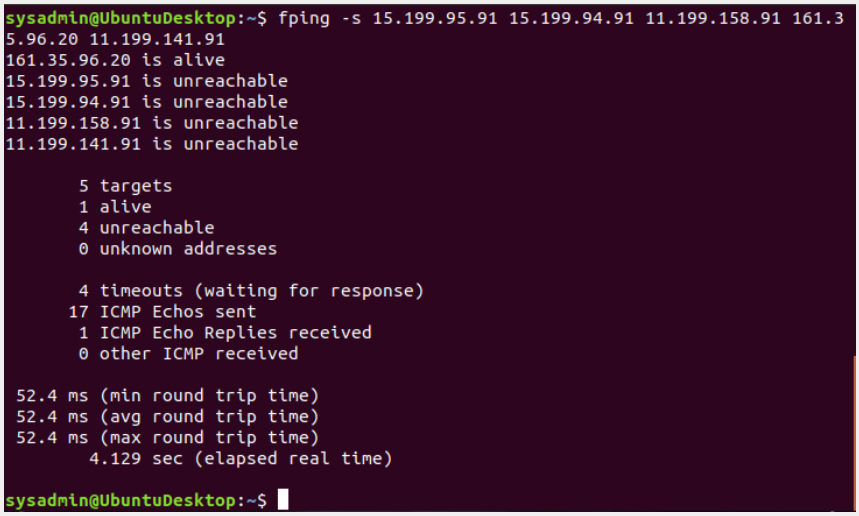


Figure 1.

3. List of IPs responding to echo requests:

```
Ip address: 161.35.96.20
```



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

```
For the reason that we are using ping, it is the network layer 3.
```

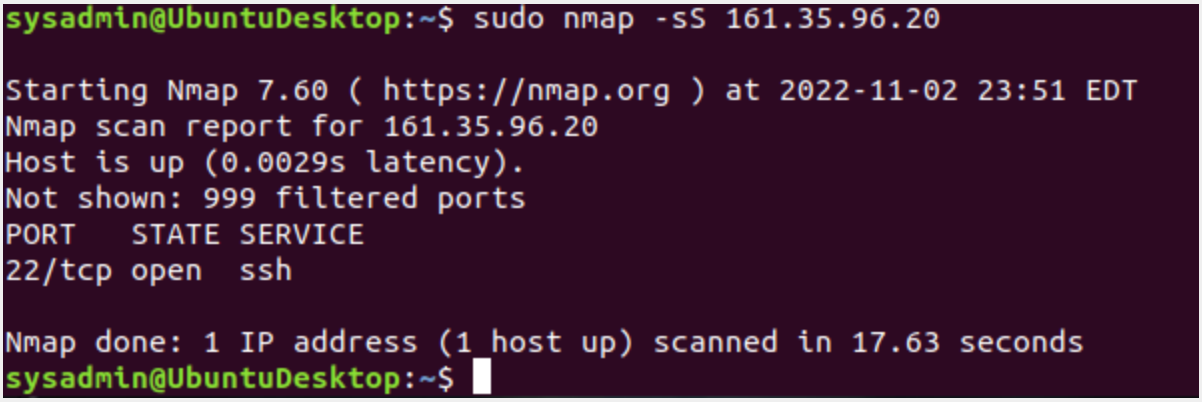
5. Mitigation recommendations (if needed):

```
Recommend to restrict ICMP privileges for 161.35.96.20 because that is a
vulnerable entry point.
```

Phase 2: *“Some SYN for Nothin`”*

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

```
Port 22 is open, the ssh port
```



2. Which OSI layer do SYN scans run on?

    a. OSI Layer:

```
Layer 4 - Transport Layer
```

    b. Explain how you determined which layer:

```
Because SYN is scanning ports, when scanning ports, ports are located in the
transport layer of the OSI model, it determines which ports are open.
```

3. Mitigation suggestions (if needed):

```
Recommend closing the ssh port, as because it is open attackers can easily
enter through.
```

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:

```
Within ssh jimi@161.35.96.20 -22:
Cd /etc
Nano hosts
98.137.246.8 rollingstone.com

Within my own system:
```

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

Non-authoritative answer:
Name:   rollingstone.com
Address: 192.0.66.114

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:~$
```

When using nslookup, we can see that in the Rockstar corp server, the domain name is mapped to a different ip address to where the actual domain server for rollingstone.com is located.

2. Command used to query Domain Name System records:

```
Nslookup -type=ns rollingstone.com

Ns = specifies dns name server for named zone
```

3. Domain name findings:

```
sysadmin@UbuntuDesktop:~$ nslookup -type=ns rollingstone.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
rollingstone.com        nameserver = ns-1426.awsdns-50.org.
rollingstone.com        nameserver = ns-2007.awsdns-58.co.uk.
rollingstone.com        nameserver = ns-416.awsdns-52.com.
rollingstone.com        nameserver = ns-718.awsdns-25.net.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

4. Explain what OSI layer DNS runs on:

```
DNS runs on the Application layer 7 because it runs parallel to HTTP. It is called upon within the layer to aid HTTP in delivering the correct domain to address.
```

5. Mitigation suggestions (if needed):

```
[Enter text here]
```

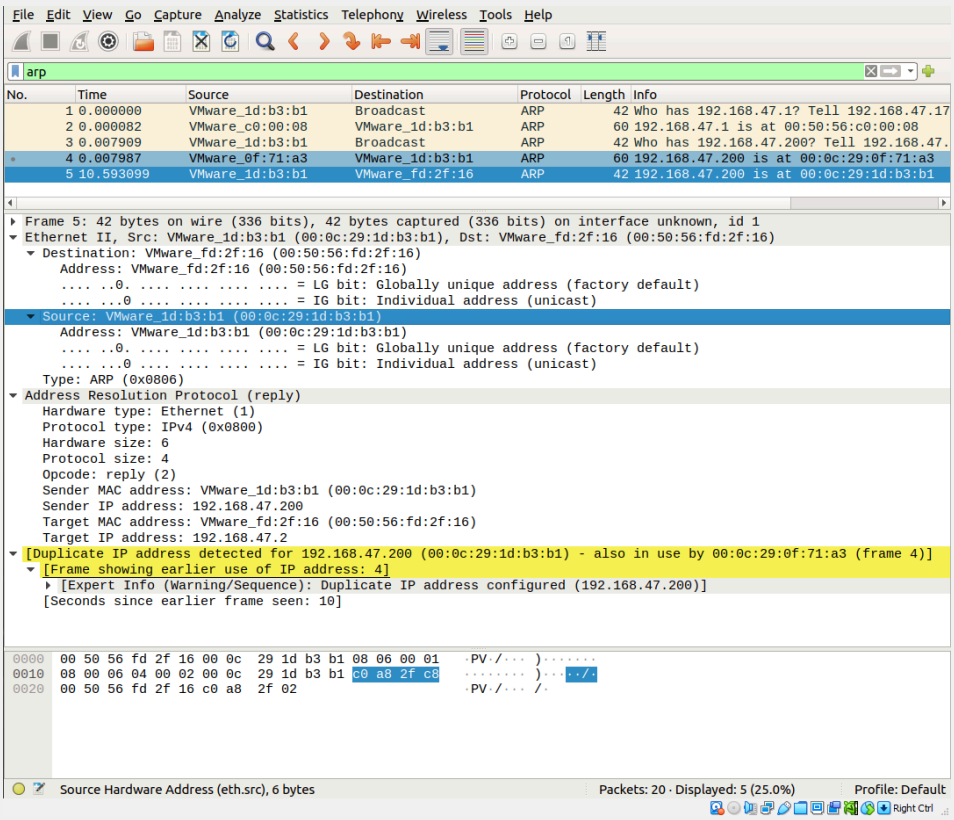
Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

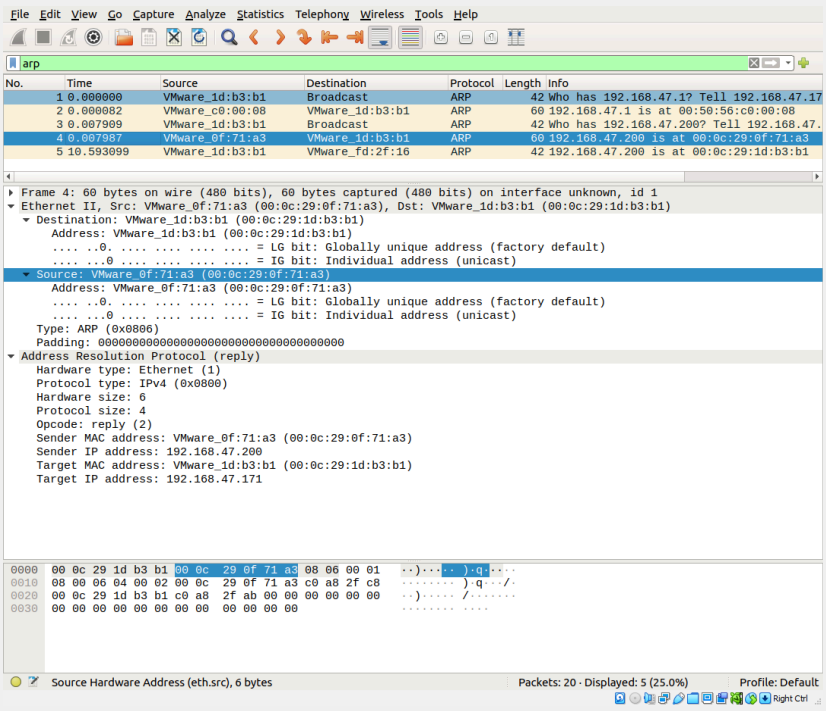
```
Cd etc
Cat packetcaptureinfo.txt
Open in google
file name : secretlogs.pcapng
```

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

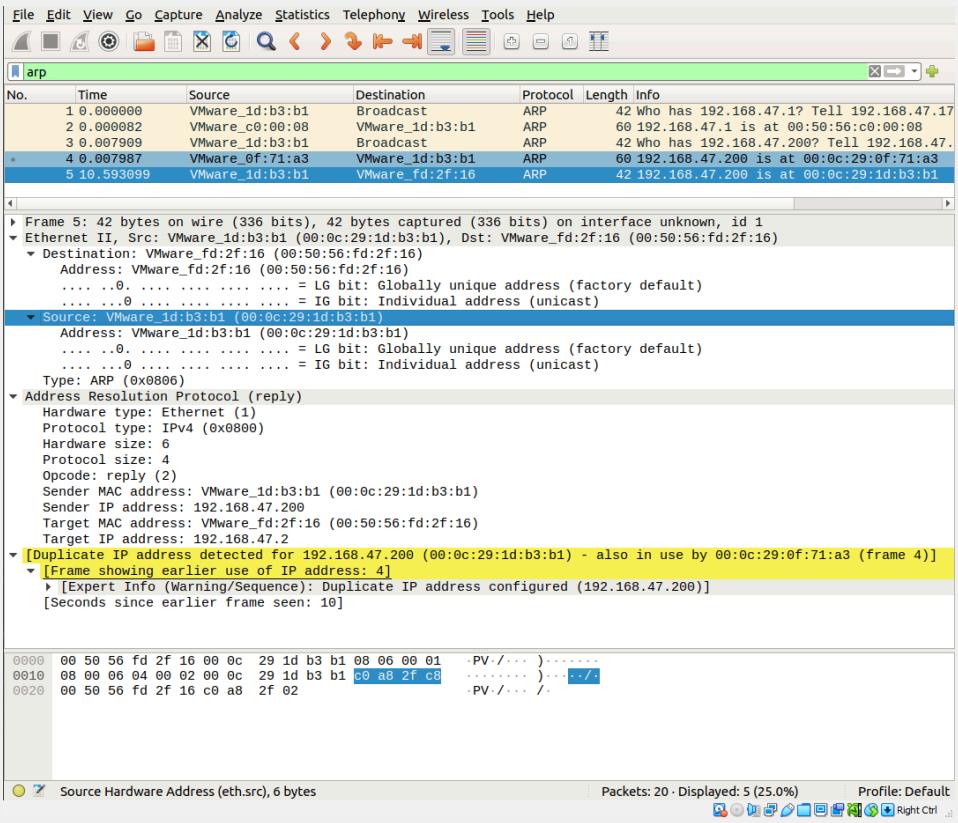
```
In the first arp on line 1, it shows the actual ip address and mac address to the rollingstone.com address being requested.
```



In line 4 of the first arp, we can see that the response back to the one who requested the arp is the rollingstone.com address, the mac and ip address originally linked to it.



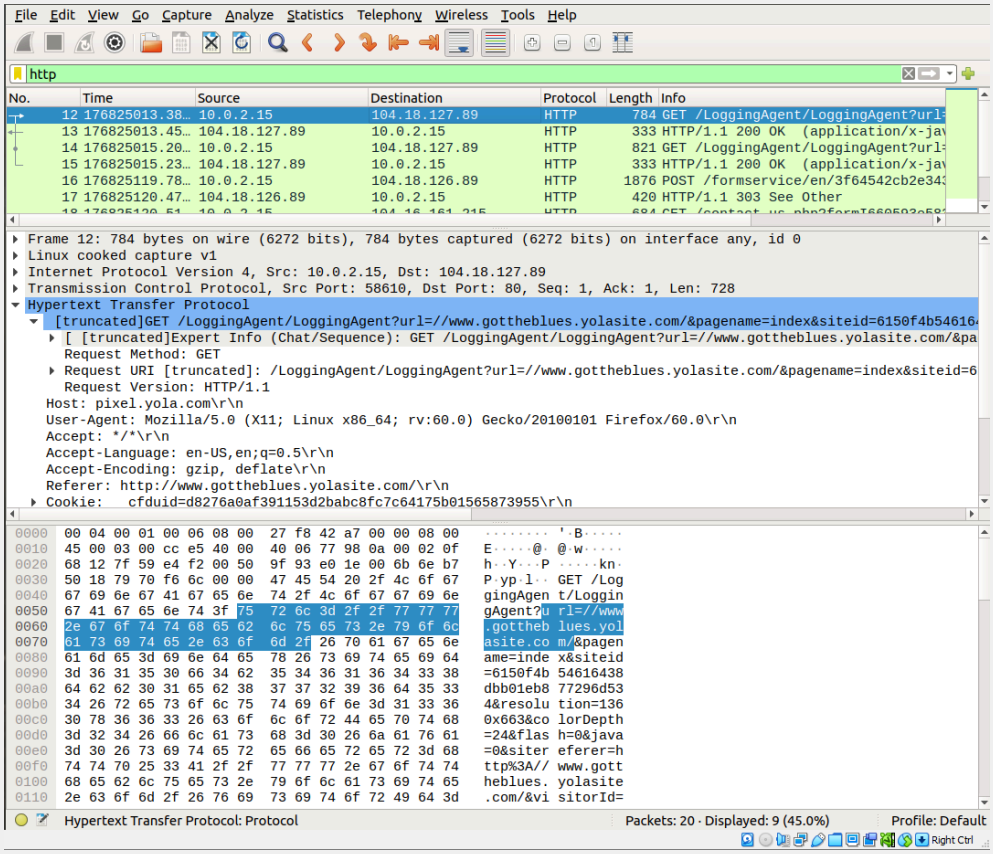
In line 5, that is where the hacker is spoofing their ip and mac address so that when you search rollingstone.com, you will end up on their site.

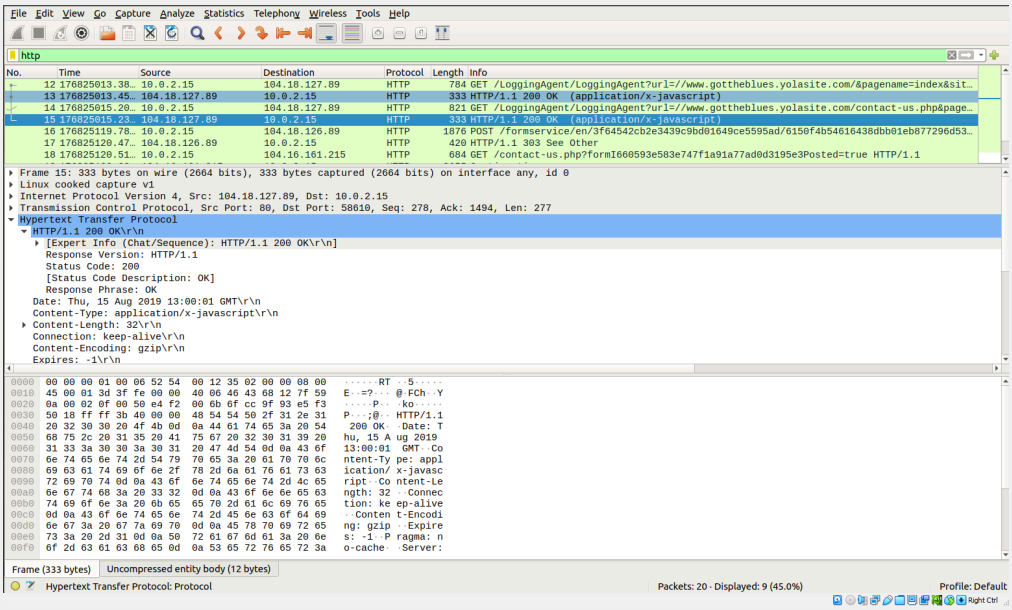


The hacker's MAC address is: 00:0c:29:1d:b3:b1

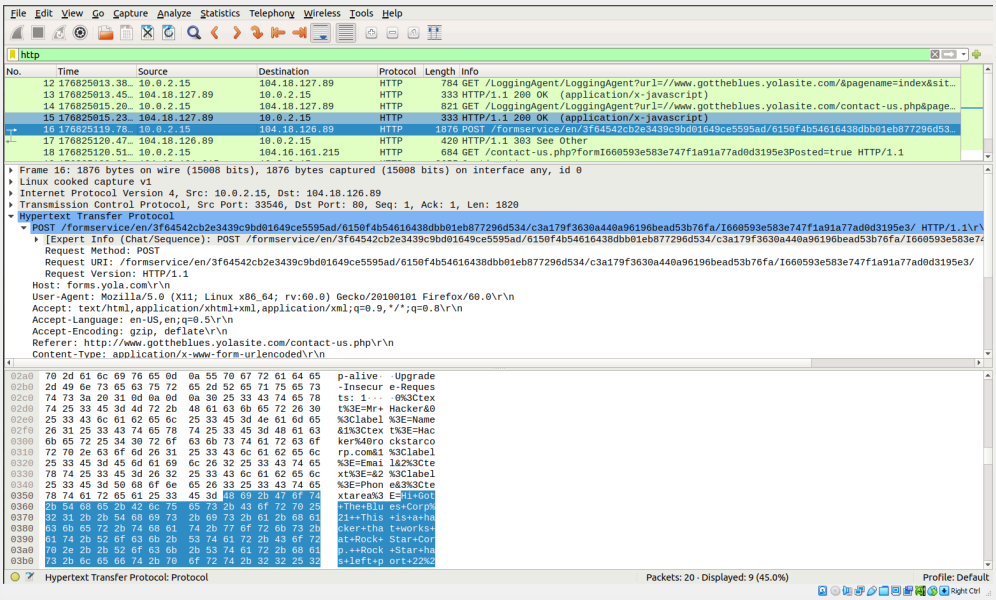
3. HTTP findings, including the message from the hacker:

After looking through lines 12 - 15 the information looks normal and is what you would get from http request and response from the server.



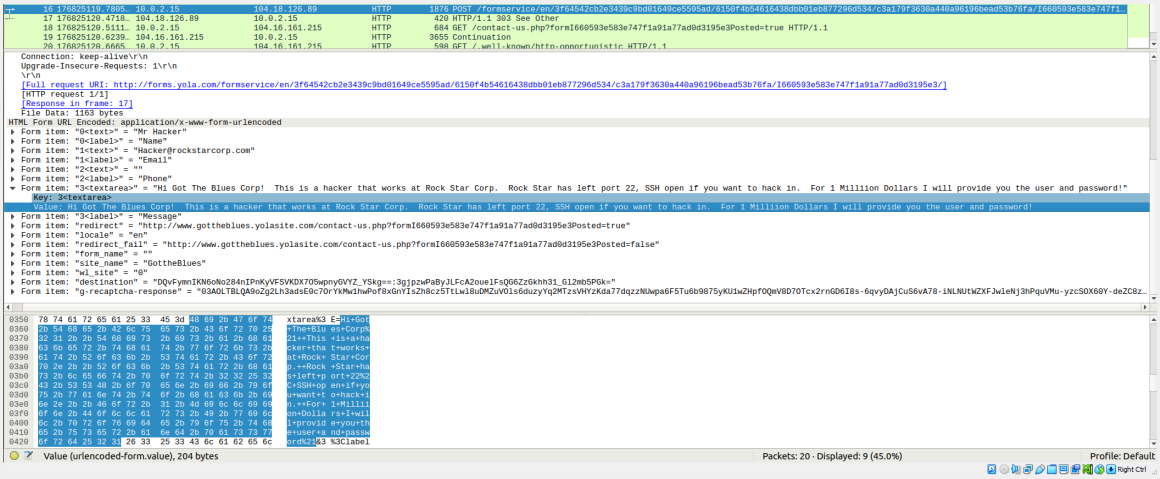


At line 16, I can see that this is where the hacker has spoofed the ip so that when searching rollingstone.com, you end up on this site.



The hacker's message is:

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 password!



4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

HTTP uses the application layer 7 because the input to receive the information utilizes the application layer

b. Layer used for ARP:

```
ARP uses the data link layer 2 because it is used to map IP network
addresses to the MAC address that is used by layer 2. MAC addresses are
layer 2.
```

5. Mitigation suggestions (if needed):

```
Close port 22
```