Cybersecurity

Networking Challenge Submission File

Networking Fundamentals: Rocking your Network

Make a copy of this document to work in. 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 `ping` against the IP ranges:

```
sysadmin@UbuntuDesktop:~$ fping 15.199.95.91
15.199.95.91 is unreachable
sysadmin@UbuntuDesktop:~$ fping 15.199.94.91
15.199.94.91 is unreachable
sysadmin@UbuntuDesktop:~$ fping 203.0.113.32
203.0.113.32 is unreachable
sysadmin@UbuntuDesktop:~$ fping 161.35.96.20
161.35.96.20 is alive
sysadmin@UbuntuDesktop:~$ fping 192.0.2.0
192.0.2.0 is unreachable
```

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

```
Used fping against all IPs for the Hollywood office and it returned only one as alive.
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

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

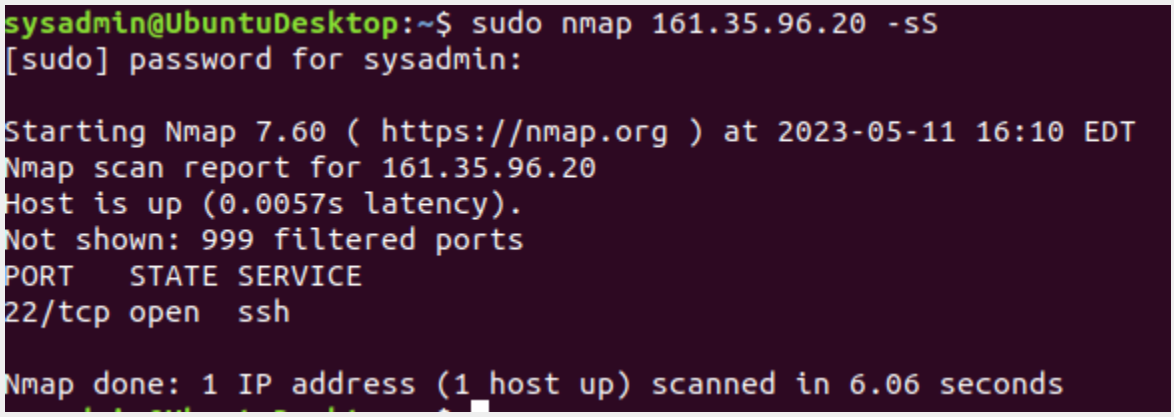
```
Networking layer
```

5. Mitigation recommendations (if needed):

```
Block connections to 161.35.96.20
```

Phase 2: *"Some SYN for Nothin'"*

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



2. Which OSI layer do SYN scans run on?
    a. OSI layer:

```
Transport layer
```

    b. Explain how you determined which layer:

```
Anything dealing with ports will be on the Transport layer.
```

3. Mitigation suggestions (if needed):

```
Suggest to use a filter or close port 22.
```

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:

```
I ssh'd into the RockStar server with the given credentials. Then, I
previewed the /etc/host file to find the IP address associated with
rollingstone.com. Then, I ran an nslookup on IP 98.137.246.8 and can
conclude that RockStar server was redirected to yahoo.com.
```

2. Command used to query Domain Name System records:

```
Nslookup 98.137.246.8
```

3. Domain name findings:

```
sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.

Authoritative answers can be found from:
```

4. Explain what OSI layer DNS runs on:

```
Application layer
```

5. Mitigation suggestions (if needed):

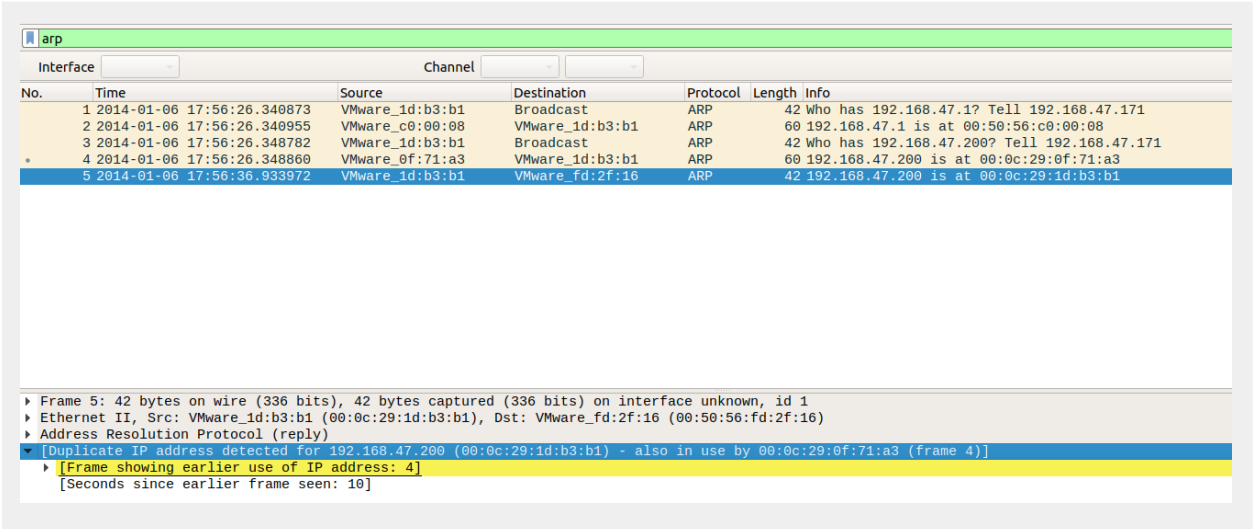
```
They need unique usernames and passwords for each server. Also, the host
file should only be accessible to those with clearance.
```

Phase 4: *"ShARP Dressed Man"*

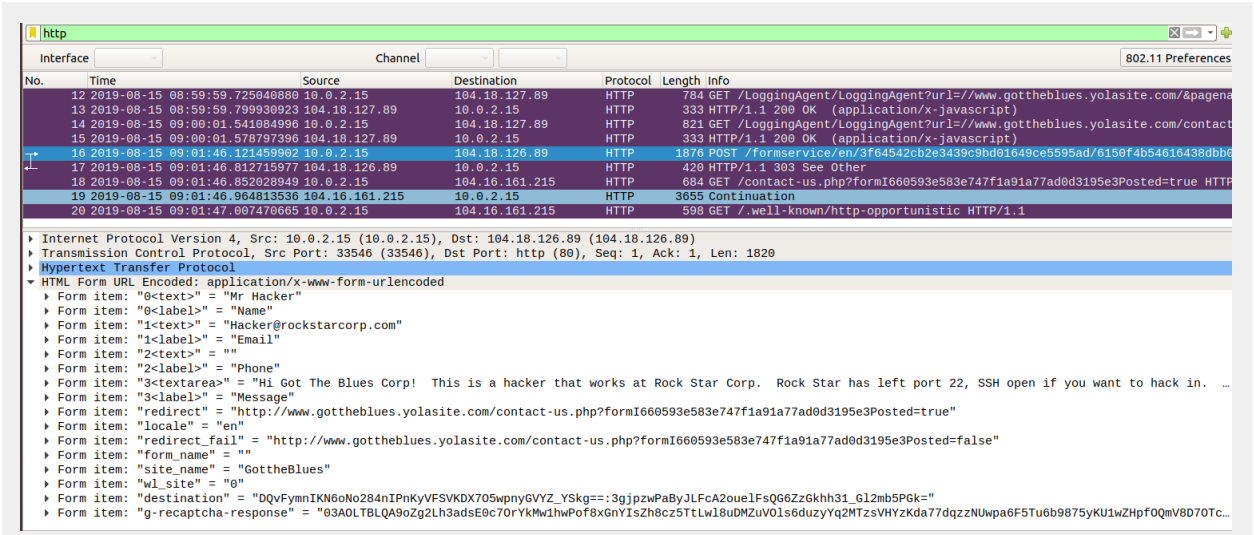
1. Name of file containing packets:

```
Inside /etc, there was a file called packetcaptureinfo.txt that contained
the link to download the packet capture called secretlogs.pcapng.
```

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



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



4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

```
Application layer
```

    b. Layer used for ARP:

```
DataLink layer
```

5. Mitigation suggestions (if needed):

```
They can start an investigation on the hacker’s MAC Address.
```