# 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:

```
ping 15.199.95.91
```

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

```
The only server that didnt request a timeout was the Hollywood Application
Server 1
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

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

```
Network layer, layer 3
```

5. Mitigation recommendations (if needed):

```
Disable echo requests for Hollywood Application Server 1
```

## Phase 2: *“Some SYN for Nothin’”*

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

```
22, 113
```

2. Which OSI layer do SYN scans run on?

    a. OSI layer:

```
I believe they run in multiple layers but primarily layer 3 network and
layer 4 transport
```

    b. Explain how you determined which layer:

```
It involves ip packets and tcp protocols
```

3. Mitigation suggestions (if needed):

```
Not sure
```

## 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:

```
The issue seems to be with the DNS server being used.
```

2. Command used to query Domain Name System records:

```
nslookup rollingstone.com
```

3. Domain name findings:

```
Server:           8.8.8.8
Address:    8.8.8.8#53
```

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

4. Explain what OSI layer DNS runs on:

```
Layer 7, application layer
```

5. Mitigation suggestions (if needed):

```
If the office's internet filter is blocking access then it can be unblocked
by being whitelisted. The office’s IP could be block by the domain.
```

## Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

```
packetcaptureinfo.txt
secretlogs.pcapng
```

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

```
00:0c:29:1d:b3:b1 also in use by 00:0c:29:0f:71:a3
I found both of these next to the duplicate ip in wireshark
```

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

```
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 the user and
password!"
    Form item: "3<label>" = "Message"
    Form item: "redirect" =
"http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91
a77ad0d3195e3Posted=true"
    Form item: "locale" = "en"
    Form item: "redirect_fail" =
"http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91
a77ad0d3195e3Posted=false"
    Form item: "form_name" = ""
    Form item: "site_name" = "GottheBlues"
    Form item: "wl_site" = "0"
    Form item: "destination" =
"DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6Z
zGkhh31_Gl2mb5PGk="
    Form item: "g-recaptcha-response" =
"03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MT
zsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78
-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u
```

4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

```
Application layer, layer 7
```

    b. Layer used for ARP:

```
Data link layer, layer 2
```

5. Mitigation suggestions (if needed):

```
Some things were securing the network and upgrading security measures
```