



# 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 -s 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):

```
161.35.96.20 is alive and the other 4 are unreachable
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

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

```
Network Layer
```

5. Mitigation recommendations (if needed):

```
The corporation doesn't want any ip addresses to be reachable so we would have to block that ip using the firewall
```

## Phase 2: “Some SYN for Nothin`”

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

Port 22 is open

2. Which OSI layer do SYN scans run on?

- a. OSI Layer:

Transport Layer

- b. Explain how you determined which layer:

Port 22 is the transport layer on the TCP model

3. Mitigation suggestions (if needed):

I don't think there is any mitigation needed

## Phase 3: “I Feel a DNS Change Comin’ On”

1. Summarize your findings about why access to [rollingstone.com](http://rollingstone.com) is not working as expected from the RockStar Corp Hollywood office:

I believe the wrong ip address is associated with the website

2. Command used to query Domain Name System records:

nslookup [www.rollingstones.com](http://www.rollingstones.com)

3. Domain name findings:

The Ip address for [rollingstones.com](http://rollingstones.com) is 18.190.122.157  
The other address is 2607:f8b0:4009:818::2004

#### 4. Explain what OSI layer DNS runs on:

Application layer

#### 5. Mitigation suggestions (if needed):

Change the ip route to run off of the 161.35.96.20 address

### Phase 4: “ShARP Dressed Man”

#### 1. Name of file containing packets:

secretlogs.pcapng

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

There is a duplicate ip address for 192.168.47.200

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

The image shows a Wireshark packet capture of an HTTP POST request. The packet list on the left shows a packet from 192.168.47.200 to 104.16.127.89. The packet details pane shows the following information:

- Cookie: \_\_cfduid=d8276a0af391153d2babc8fc7c64175b01565873955v\r\n
- Cookie pair: \_\_cfduid=d8276a0af391153d2babc8fc7c64175b01565873955
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n
- Full request URI: http://forms.yola.com/formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bead53b76f/I660593e583e747f1a91a77ad8d3195e3/
- HTTP request 1/1
- Response in frame: 17
- File Data: 1163 bytes
- HTML Form URL Encoded: application/x-www-form-urlencoded
- Form items:
  - 0<label> = "Name"
  - 1<text> = "Hacker@rockstarcorp.com"
  - 1<label> = "Email"
  - 2<text> = ""
  - 2<label> = "Phone"
  - 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 Million Dollars I will pro"
  - 3<label> = "Message"
  - redirect = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad8d3195e3Posted=true"
  - locale = "en"
  - redirect\_fail = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad8d3195e3Posted=false"
  - form\_name = ""
  - site\_name = "GotTheBlues"
  - wl\_site = "g"
  - destination = "DQvFymnIKN6No284nIPnKyVFSVKDX705wpyGVYZ\_YSkG==:3gjpwPaByJLFCa2oue1fSg6GZgkhh31\_g12mb5Pgk="
  - g-recaptcha-response = "83AOLTLBQA9ozg2Lh3adsE8c70rYkMw1hwPof8xGnYIsZh8cZ5TLwL8UDM2uV01s6duzyq2MTzsVHYzKda77dqzZUwpa6F5Tu6b9875yKU1wZHpQmV8D70Tcx2rn6D6I8s-6qvYDAjCuS6vA78-INLNUt"

4. Explain the OSI layers for HTTP and ARP.

a. Layer used for HTTP:

Application layer

b. Layer used for ARP:

Data Link layer

5. Mitigation suggestions (if needed):

Change the ip address so they won't be duplicated