# CYB102 Project 4

(🔗 Instructions Page)

👤 Student Name: [ ]
✉️ Student Email: [ ]

## Reflection (Required)

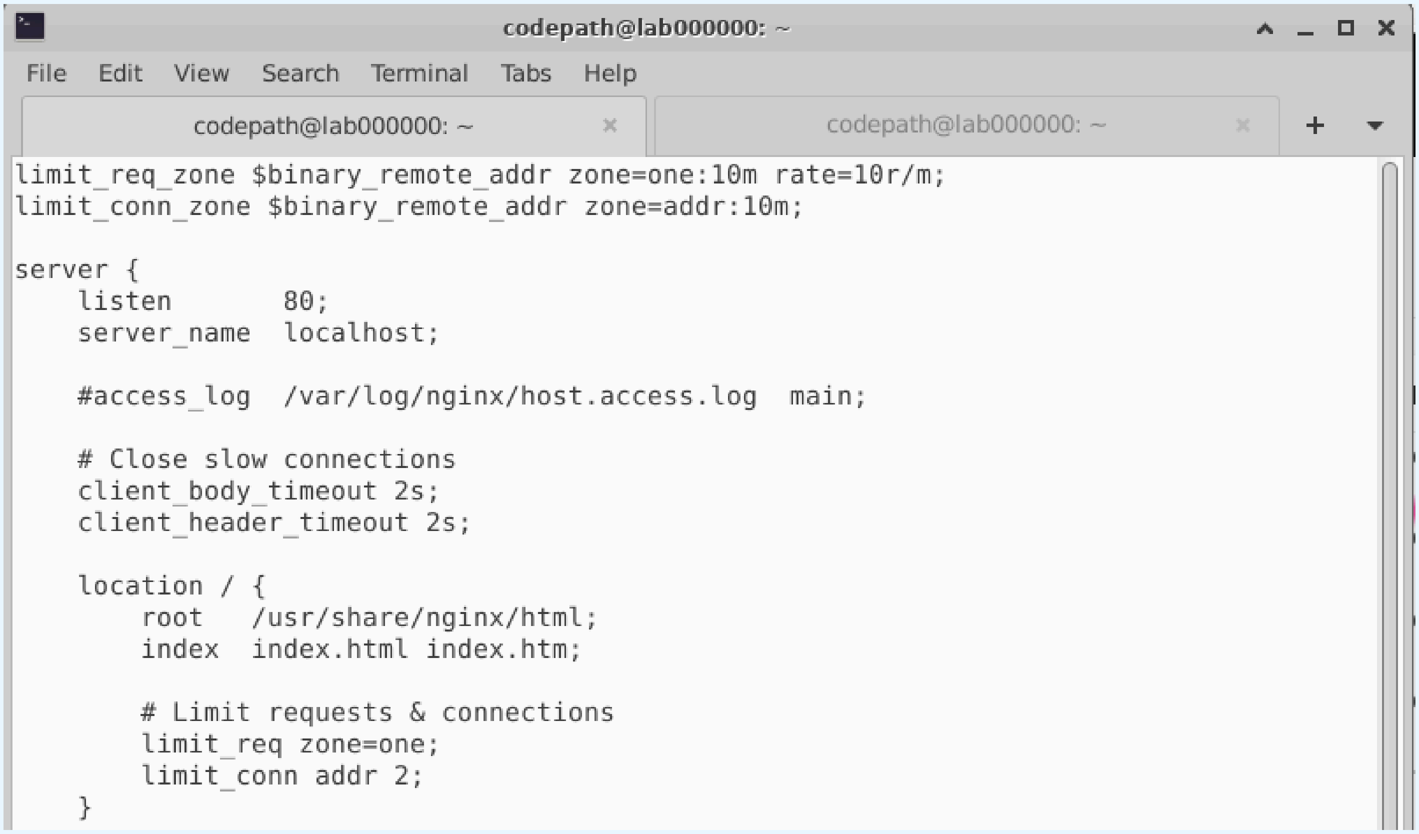
> 🤔 **Reflection Question #1:** If I had to **explain "what is a proxy server" in 3 emojis,** they would be…
> (Feel free to put other comments about your experience in this unit here, too!)
>
> 🌐🛡️💻

> 🧠**Reflection Question #2:** What are some different types of DoS/DDoS attacks?
>
> There are volume attacks to take up a server's bandwidth, protocol attacks to disrupt infrastructure like the TCP handshake, and application layer attacks like Slowloris to keep connections open for as long as possible.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!
>
> Shout out to the Slack homework bot for the reminder!

## Required Challenges (Required)

> **Item #1:** A screenshot of your `/etc/nginx/conf.d/default.conf` file with your DoS mitigation rules implemented:



```
limit_req_zone $binary_remote_addr zone=one:10m rate=10r/m;
limit_conn_zone $binary_remote_addr zone=addr:10m;

server {
    listen       80;
    server_name  localhost;

    #access_log  /var/log/nginx/host.access.log  main;

    # Close slow connections
    client_body_timeout 2s;
    client_header_timeout 2s;

    location / {
        root   /usr/share/nginx/html;
        index  index.html index.htm;

        # Limit requests & connections
        limit_req zone=one;
        limit_conn addr 2;
    }
```

**Item #2:** A detailed explanation (two sentences minimum) of how you know that your DoS mitigation rules are working:

**My first line defines a zone to limit the number of requests per client IP to 10 per minute. My second line defines another zone to limit the number of concurrent connections per client IP. Within my server block, I close connections that take longer than 2 seconds to send headers or a body. Lastly, within the location block, I enforce the request zone and the connection zone to 2 connections per client IP.**

**Item #3:** A detailed explanation of how you know which `.pcap` file is from the vulnerable server, and which is from the server with DoS mitigation set up:

**A is the DoS-mitigated server, and B is the vulnerable server. In file A, the text "[TCP Port numbers reused]" appears in the info field of some packets, which indicates that the server has detected a single client repeatedly attempting to connect. Another detail to note is the presence of the reset flag in the server's response packets to the client. When the reset flag is set, it means the server is abruptly terminating the connection, which typically occurs when mitigation rules are active. File B does not contain packets that indicate malicious connections or requests. The B server in this case is responding to all incoming traffic.**

---

## Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

**Required Challenges**

☑ ~~Item #1~~

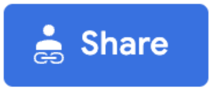
☑ ~~Item #2~~

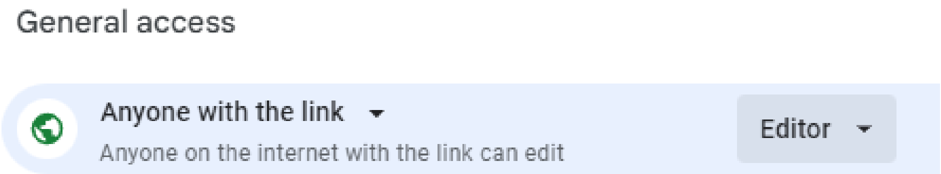
☑ ~~Item #3~~

💡***Tip: You can see specific grading information, including points breakdown, by going to 🔗 the grading page on the course portal.***

**Submit your work!**

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.



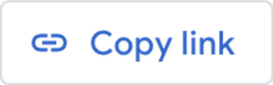

General access

Anyone with the link

Anyone on the internet with the link can edit

Editor

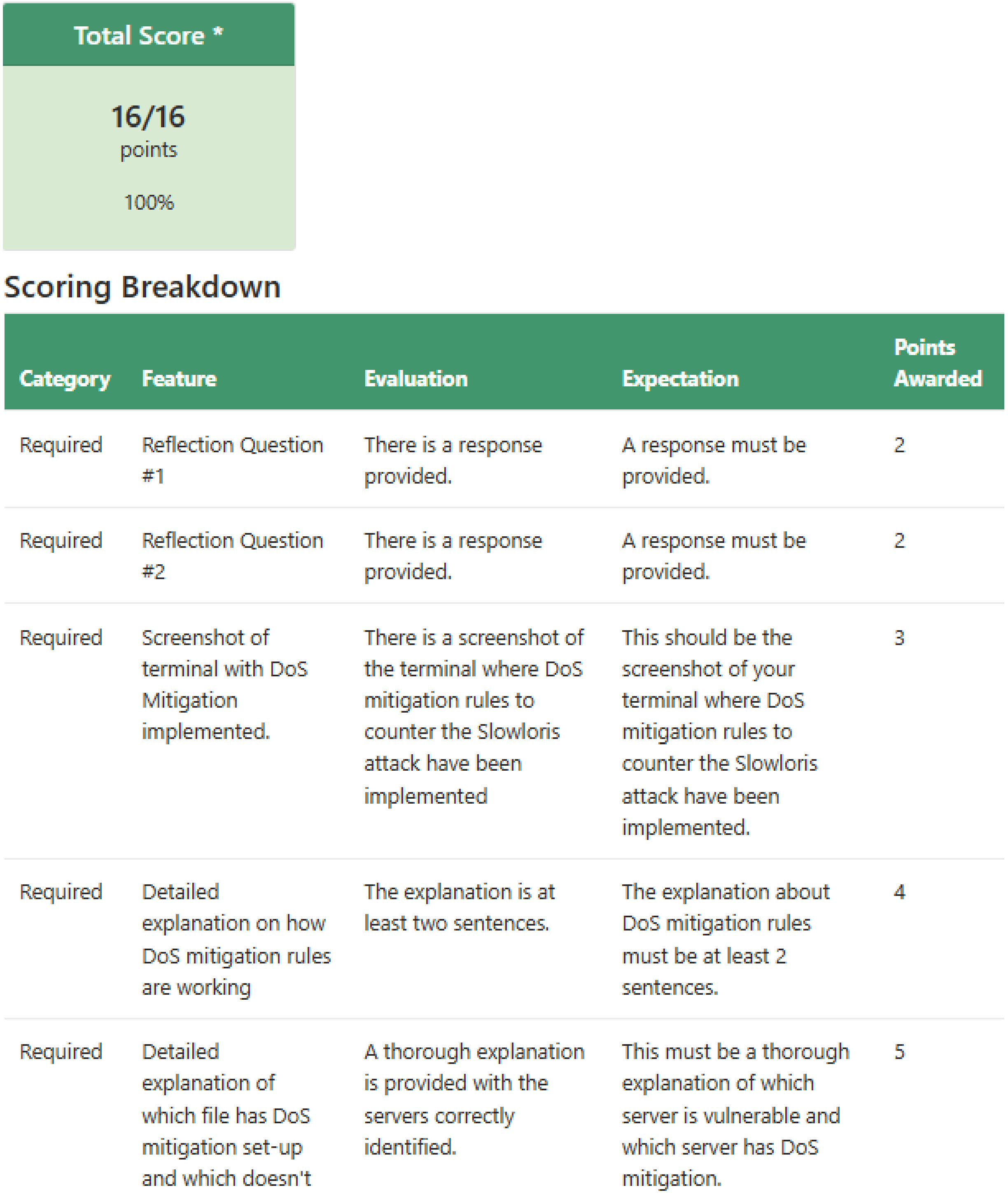
Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.

---

# Grading



Total Score *

16/16
points

100%

## Scoring Breakdown

| Category | Feature | Evaluation | Expectation | Points Awarded |
|---|---|---|---|---|
| Required | Reflection Question #1 | There is a response provided. | A response must be provided. | 2 |
| Required | Reflection Question #2 | There is a response provided. | A response must be provided. | 2 |
| Required | Screenshot of terminal with DoS Mitigation implemented. | There is a screenshot of the terminal where DoS mitigation rules to counter the Slowloris attack have been implemented | This should be the screenshot of your terminal where DoS mitigation rules to counter the Slowloris attack have been implemented. | 3 |
| Required | Detailed explanation on how DoS mitigation rules are working | The explanation is at least two sentences. | The explanation about DoS mitigation rules must be at least 2 sentences. | 4 |
| Required | Detailed explanation of which file has DoS mitigation set-up and which doesn't | A thorough explanation is provided with the servers correctly identified. | This must be a thorough explanation of which server is vulnerable and which server has DoS mitigation. | 5 |