CYB102 Project 4

(🔗 Instructions Page)

👤 Student Name: Weicong Xie
✉️ Student Email: Weicong.wx@gmail.com

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?

Slowloris, SYN flood, Smurf attacks

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

Required Challenges (Required)

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

```
codepath@lab000000:/etc/nginx/conf.d$ cat default.conf
server {
    listen       80;
    server_name  localhost;

    #DoS mitigation rules
    limit_conn addr 10;
    limit_req zone=one;
    client_body_timeout 10s;
    client_header_timeout 10s;
    keepalive_timeout 10s;

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

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

    #error_page  404              /404.html;

    # redirect server error pages to the static page /50x.html
    #
    error_page   500 502 503 504  /50x.html;
    location = /50x.html {
        root   /usr/share/nginx/html;
    }

    # proxy the PHP scripts to Apache listening on 127.0.0.1:80
    #
    #location ~ \.php$ {
    #    proxy_pass   http://127.0.0.1;
    #}

    # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
    #
    #location ~ \.php$ {
    #    root           html;
    #    fastcgi_pass   127.0.0.1:9000;
    #    fastcgi_index  index.php;
    #    fastcgi_param  SCRIPT_FILENAME  /scripts$fastcgi_script_name;
    #    include        fastcgi_params;
    #}

    # deny access to .htaccess files, if Apache's document root
    # concurs with nginx's one
    #
    #location ~ /\.ht {
    #    deny  all;
    #}
}
```

Note (Optional):

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

The graphs are spikier meaning they are being dropped more frequently. The errors are also more spaced out, instead of a constant 150, it's: 150 150 150 break 150 150 150.

Screenshot (Optional):

> **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:
>
> **File A is the protected server because it has a pattern of RST flags, meaning TCP connections are constantly being forcibly closed.**

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~~