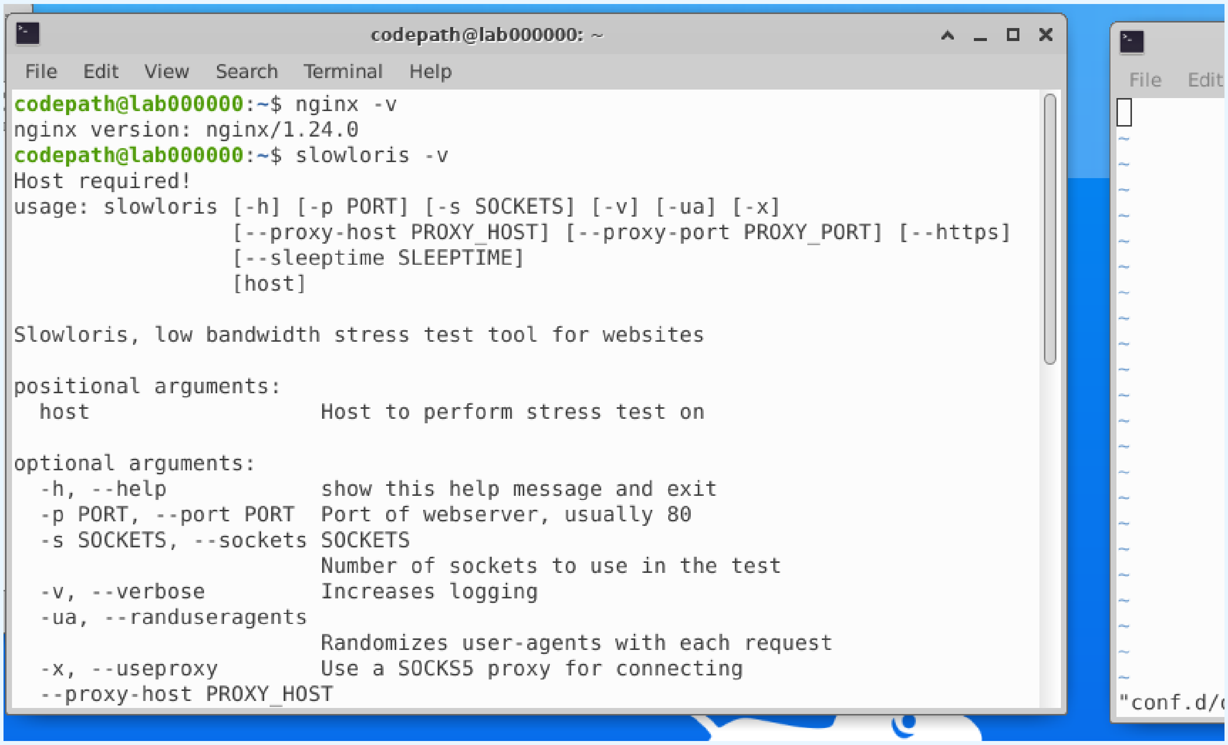
Project 4

Gerrell Bones
01 NOV 2023
CNT 4403
Project 4

Required Challenges (Required)

> **Item #1:** A screenshot of your `/etc/nginx/conf.d/default.conf` file with your DoS mitigation rules implemented:
>
> 
>
>
> ```
> codepath@lab000000:~$ nginx -v
> nginx version: nginx/1.24.0
> codepath@lab000000:~$ slowloris -v
> Host required!
> usage: slowloris [-h] [-p PORT] [-s SOCKETS] [-v] [-ua] [-x]
>                  [--proxy-host PROXY_HOST] [--proxy-port PROXY_PORT] [--https]
>                  [--sleeptime SLEEPTIME]
>                  [host]
>
> Slowloris, low bandwidth stress test tool for websites
>
> positional arguments:
>   host                  Host to perform stress test on
>
> optional arguments:
>   -h, --help            show this help message and exit
>   -p PORT, --port PORT  Port of webserver, usually 80
>   -s SOCKETS, --sockets SOCKETS
>                         Number of sockets to use in the test
>   -v, --verbose         Increases logging
>   -ua, --randuseragents
>                         Randomizes user-agents with each request
>   -x, --useproxy        Use a SOCKS5 proxy for connecting
>   --proxy-host PROXY_HOST
> ```

> **Item #2:** A detailed explanation (two sentences minimum) of how you know that your DoS mitigation rules are working:
>
> **To ascertain the effectiveness of DoS mitigation rules, organizations employ several monitoring and evaluation techniques. One crucial method involves analyzing network traffic patterns in real-time or through historical data. If the**

implemented rules are working as intended, the system should be able to distinguish between normal and malicious traffic, promptly identifying and mitigating any disruptive activities. Additionally, organizations often conduct simulated or controlled DoS attacks to test the responsiveness of their mitigation strategies, ensuring that the rules effectively prevent service disruptions and maintain system availability. Regular audits, incident response drills, and ongoing analysis of security logs contribute to a comprehensive understanding of the DoS mitigation rules' functionality and their ability to protect against potential threats.

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:

To distinguish between a .pcap file from a vulnerable server and one from a DoS mitigation setup, you would typically look at the content and characteristics of the network traffic captured in each file.

For the vulnerable server .pcap file, you might observe patterns indicative of a system under stress or attack. This could include an unusually high volume of requests from a limited set of IP addresses, a spike in traffic to specific ports, or other irregularities that suggest an attempt to overwhelm or exploit vulnerabilities in the server.

On the other hand, the .pcap file from the DoS mitigation setup would ideally demonstrate the effectiveness of the mitigation rules. You would look for signs of traffic normalization, the blocking or rate-limiting of malicious requests, or any other measures that indicate the mitigation system is successfully identifying and mitigating the attack.

Comparing the two .pcap files side by side, you can analyze the differences in traffic patterns to determine how well the DoS mitigation rules are working to protect the server. This analysis may involve examining packet headers, payload content, source and destination IP addresses, and other relevant information to differentiate between normal and potentially malicious traffic.