**CYB102 Project 4 (🔗** [**Instructions Page**](https://courses.codepath.org/courses/cyb102-dev/unit/1#!projects)**)**

👤 Student Name: Nickodemus Konde

✉️ Student Email: Ntkonde88@gmail.com

**Reflection (Required)**

| **🤔 Reflection Question #1:** If I had to **explain “what is a DoS attack” 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? |
| --- |
| SYN flood, UDP flood, ICMP/ping flood |

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

**Required Challenges (Required)**

| **Nginx screenshot:** A screenshot of your **nginx** config file(s) with your DoS mitigation rules implemented: |
| --- |
| **Note** (Optional): |

#### 

| **Unprotected screenshot:** A screenshot of your Netdata TCP connections graph during the **unprotected** Slowloris attack: |
| --- |
| **Note** (Optional): |

#### 

| **Protected screenshot:** A screenshot of your Netdata TCP connections graph during the **protected** Slowloris attack |
| --- |
| **Note** (Optional): |

#### 

| **Explanation of Differences:** An explanation of the differences between the unprotected and protected Slowloris attacks, in your own words: |
| --- |
| **During the unprotected Slowloris attack, nginx held hundreds of half-open HTTP connections. The TCP Connections graph of Netdata exhibited high, long-duration spikes, showing that sockets were never being closed. After adding mitigation rules — lowered client\_header\_timeout and client\_body\_timeout, decreased keepalive\_timeout, and per-IP limits via limit\_conn and limit\_req - nginx began closing idle or abusive connections in a timely manner. The graph behind protection shows much smaller, short-duration spikes, illustrating that the DoS mitigation was effective and the server remained stable.** |

#### 

**Stretch Challenge (Optional)**

| **Stretch Question:** 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: |
| --- |
| **I loaded both .pcap files into Wireshark and contrasted them. The vulnerable server capture had many long-lived, low-payload TCP connections from one IP with extremely slow header transmits. The protected server capture had far fewer connections with many RST or FIN flags, showing the server was closing abusive sessions early. This is characteristic of a hardened nginx setup with DoS mitigation enabled.** |

**Submission Checklist**

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

**Required Challenges**

* ~~Nginx Screenshot~~
* ~~Unprotected Screenshot~~
* ~~Protected Screenshot~~
* ~~Explanation of Differences~~

**Stretch Challenge**

* ~~Stretch Question~~

***💡Tip: You can see specific grading information, including points breakdown, by going to 🔗*** [***the grading page***](https://courses.codepath.org/courses/cyb102/pages/grading) ***on the course portal.***