# Distributed Denial of Service (DDoS) Attack Simulation and Mitigation

## Project Overview

This document outlines a cybersecurity project where a Distributed Denial of Service (DDoS) attack was simulated using a Kali Linux virtual machine, targeting a Raspberry Pi 5 with Kali Linux. The project aimed to demonstrate practical offensive and defensive security skills, including the detection and mitigation of a SYN flood attack.

## Technical Details

**Attacker Machine:** Kali Linux VM on PC (used hping3 for the SYN flood attack)
**Target Machine:** Raspberry Pi 5 with Kali Linux
**Network Setup:** Both machines connected via the same WIFI network
**Tools Used:**

- **Hping3:** For simulating a SYN flood attack.
- **Wireshark:** For capturing and analyzing network traffic
- **Iptables:** For creating firewall rules to mitigate the attack

## Attack Process

**SYN Flood Attack:**

- The attacker machine used hping3 to flood port 80 of the Raspberry Pi with SYN packets.
- Wireshark was used to capture the traffic and identify the incoming SYN flood.

**Traffic Analysis:**

- Wireshark filters were applied to focus on the SYN packets (tcp.flags.syn==1), revealing thousands of incoming packets targeting port 80.

## Mitigation Process

**Firewall Rule:**

- On the Raspberry Pi, iptables was used to block incoming SYN packets while allowing legitimate traffic to pass through.

**Verification:**

- After applying the firewall rule, Wireshark was used again to confirm that the malicious traffic had stopped, and legitimate network connections were unaffected.

## Conclusion

This project showcased my ability to execute and defend against a real-world cybersecurity threat in a controlled environment. By successfully simulating a SYN flood DDoS attack, I gained experience in analyzing malicious network traffic using Wireshark and implementing defensive strategies through iptables firewall rules. The hands-on nature of the project strengthened my skills in both offensive and defensive cybersecurity, demonstrating my capability to not only identify and understand complex network attacks but also to mitigate them effectively. These procedures are essential for safeguarding systems in today's increasingly hostile digital world, making this experience a valuable addition to my cybersecurity skill set.