INTERNSHIP REPORT

UNDER GUIDANCE OF

DR.ARUN RAJ KUMAR P.

AT CSED,NITC

BY

MUMMANA SANJAY

BTECH

MAJOR - MECHANICAL ENGINEERING [NITK]

MINOR - COMPUTER SCIENCE [NITK]

TASK 2 ASSIGNED ON 2ND JUNE 2024

1. Task Overview

This report presents a comparative analysis of TCP SYN flood attack traffic samples from three datasets: CIC DDoS 2019, CSE-CIC-IDS2018, and a generated pcap file from task1. The goal is to identify and compare the characteristics of TCP SYN flood attacks across these datasets, focusing on their similarities and differences.

2. Datasets Overview

- CIC DDoS 2019: A dataset containing various types of DDoS attacks, captured in a controlled environment to simulate modern DDoS attack scenarios.
- CSE-CIC-IDS2018: A comprehensive dataset representing a mix of benign and malicious network traffic, collected over several days to emulate real-world network traffic patterns.
- Generated pcap file: A pcap file created by conducting a TCP SYN flood attack in a controlled environment, providing a sample for direct comparison.

3. Methodology

The analysis involved the following steps:

- Loading and filtering each dataset to isolate TCP SYN packets.
- Extracting key features relevant to SYN flood attacks: packet volume, inter-arrival times, source/destination IP addresses, and TCP flags.
- Comparing these features across the three datasets to highlight similarities and differences.

4. Analysis and Findings

4.1 TCP SYN Flood Attack Characteristics

- Common indicators of a TCP SYN flood attack include:
    a) High volume of SYN packets.
    b) Low volume of SYN-ACK and ACK packets.
    c) Short inter-arrival times between SYN packets.
    d) Spoofed source IP addresses to obscure the origin of the attack.

4.2 Generated pcap File Analysis

- **Volume of SYN Packets:** The dataset contains 28,841 SYN packets.
- **Inter-arrival Times:** Typically within milliseconds, indicating a high-rate flood.
- **Source IPs:** A single source IP address (145.127.122.192).
- **TCP Flags:** All packets are SYN packets.
- **Targeting:** All packets target a single destination IP address (192.168.100.4).

4.3 CIC DDoS 2019 Dataset

- **Volume of SYN Packets:** High volume consistent with DDoS attack behavior.
- **Inter-arrival Times:** Extremely short, indicating rapid packet generation typical of SYN flood attacks.
- **Source IPs:** Many spoofed IP addresses.
- **TCP Flags:** Predominantly SYN packets with very few SYN-ACK and ACK packets.
- **Targeting:** Focused on specific target IP addresses and ports.

4.4 CSE-CIC-IDS2018 Dataset

- **Volume of SYN Packets:** High volume, though slightly lower compared to CIC DDoS 2019.
- **Inter-arrival Times:** Short, indicating rapid packet generation.
- **Source IPs:** A mix of real and spoofed IP addresses.
- **TCP Flags:** Primarily SYN packets with occasional SYN-ACK and ACK packets.
- **Targeting:** More variation in target IPs and ports.

5. Comparative Analysis

5.1 Similarities

- **High Volume of SYN Packets:** All datasets exhibit a significant number of SYN packets, characteristic of flood attacks.
- **Short Inter-arrival Times:** Consistently short across all datasets, indicating high packet generation rates typical of SYN flood attacks.
- **Predominantly SYN Flags:** All datasets predominantly contain SYN packets, with very few SYN-ACKs and ACKs, which is indicative of a SYN flood attack.

Feature	Generated pcap File	CIC DDoS 2019	CSE-CIC-IDS2018
Volume of SYN Packets	High volume (28,841 packets)	High volume	High volume
Inter-arrival Times	Short (milliseconds)	Extremely short (milliseconds)	Short (milliseconds)
TCP Flags	Predominantly SYN packets	Predominantly SYN packets	Predominantly SYN packets
Attack Pattern	High-rate SYN flood attack	High-rate SYN flood attack	High-rate SYN flood attack

5.2 Differences

- **Source IP Variability:**

    a) **Generated pcap File:** Utilizes a single source IP address.
    b) **CIC DDoS 2019:** Includes many spoofed IP addresses to obscure the origin of the attack.
    c) **CSE-CIC-IDS2018:** Features a mix of real and spoofed IP addresses, showing more diversity.

- **Target IP Variability:**

    a) **Generated pcap File:** Targets a single destination IP address.
    b) **CIC DDoS 2019:** Focused on specific targets, but generally more concentrated than the generated pcap file.
    c) **CSE-CIC-IDS2018:** Exhibits more variability in target IPs and ports, indicating a broader range of attack vectors.

- **Intensity and Pattern of Attack:**

    a) **Generated pcap File:** Exhibits a highly focused and intense attack with very short inter-arrival times.
    b) **CIC DDoS 2019:** Shows a similar level of intensity but with more source IP variability.
    c) **CSE-CIC-IDS2018:** Slightly less intense with more variation in attack patterns, including some legitimate traffic.

Feature	Generated pcap File	CIC DDoS 2019	CSE-CIC-IDS2018
Source IP Variability	Single source IP	Many spoofed IP addresses	Mix of real and spoofed IPs
Target IP Variability	Single target IP	Focused on specific target Ips	More variation in target IPs
Intensity and Pattern	Highly focused and intense	Similar intensity, more source IP variability	Slightly less intense, more varied patterns
Target Ports	Single target port	Specific target ports	More variation in target ports

Similarities	Differences
High volume of SYN packets.	Source IP variability.
Short inter-arrival times.	Target IP variability.
Predominantly SYN flags.	Intensity and pattern of attack.

6. Conclusion

The analysis reveals that while all three datasets demonstrate the high-intensity nature of TCP SYN flood attacks, there are distinct differences in the source IP variability and targeting strategies. The generated pcap file shows a highly focused attack with a single source and target IP, closely resembling the attack patterns in the CIC DDoS 2019 dataset but differing in its lack of source IP variability. The CSE-CIC-IDS2018 dataset displays more variability in both source and target IPs, suggesting a broader and less focused attack pattern.

---THANK YOU---