# DoS Attack Detection Report Using Wireshark

Maya Lotfy

## 1. Introduction

This report presents the findings of a Denial of Service (DoS) attack, specifically a SYN flood attack, detected using Wireshark. The analysis was performed on a PCAP file, which captured the network traffic during the attack. The goal was to identify the attack's characteristics, analyze the traffic patterns, and present the relevant findings.

## 2. Objective

The objectives of this analysis were to:

- Detect and identify the SYN flood attack in the captured network traffic.
- Analyze the network conversations and endpoints involved in the attack.
- Present visual evidence of the attack using I/O graphs.

## 3. Tools and Techniques Used

- **Tool**: Wireshark
- **PCAP File**: pkt.TCP.synflood.spoofed.pcap
- **Version**: 4.2.6 (v4.2.6-0-g2acd1a854bab).

**Command Executed**: The PCAP file was analyzed using Wireshark's graphical user interface.

## 4. Methodology

### 4.1. Loading the PCAP File

1. Open Wireshark.
2. Load the PCAP file by navigating to `File` > `Open` and selecting `[file.pcap]`.

### 4.2. Identifying SYN Flood Attack

A SYN flood attack can be identified by:

- **High Volume of SYN Packets**: An abnormal number of TCP SYN packets sent to a specific port or IP address.
- **Uncompleted Handshakes**: A large number of half-open TCP connections with no corresponding ACK packets.

### 4.3. Analyzing Conversations and Endpoints

1. **Conversations**:
    - Go to `Statistics` > `Conversations`.
    - Analyze the TCP conversation statistics to identify abnormal patterns or a high volume of connections.
2. **Endpoints**:
    - Go to `Statistics` > `Endpoints`.
    - Analyze the endpoints involved to determine which IP addresses are primarily targeted and which ones are sending the attack traffic.

## 5. Findings

### 5.1. SYN Flood Detection

- **Traffic Analysis**:
    - **Number of SYN Packets**: 37841
- **Traffic Pattern**:
    - The SYN flood attack was characterized by a high frequency of SYN packets directed towards a specific port, causing the target server to allocate resources for incomplete connections.

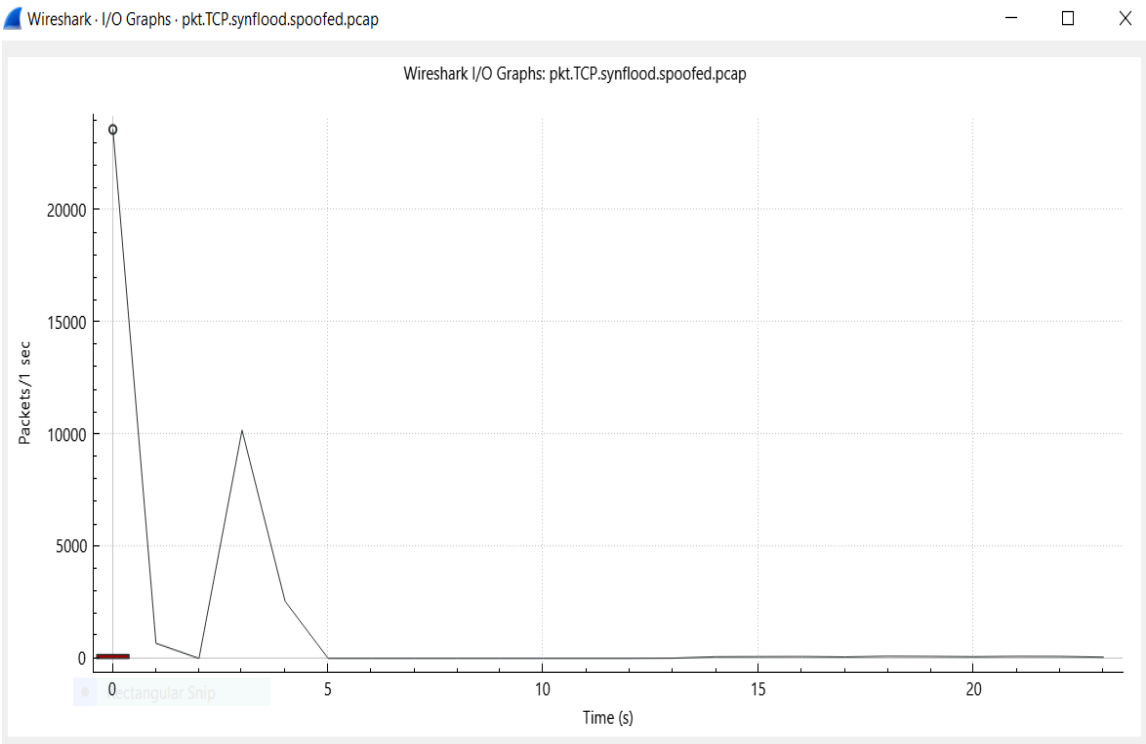
### 5.2. Conversations and Endpoints

- conversation exhibited a high volume of packets and data, which is significantly above the normal traffic levels. This high traffic volume suggests a potential DoS attack, where either the source IP is generating excessive traffic or the destination IP is being overwhelmed.

- Endpoints analysis revealed several IP addresses with abnormally high traffic volumes, both in terms of packets and bytes. These endpoints are potentially involved in or targeted by a DoS attack. Specifically, high-traffic source IPs could be either attackers or compromised hosts, while high-traffic target IPs are likely victims of the attack.

## 6. I/O Graphs

- **Description**: The I/O graph below shows the spike in SYN packets over time, indicative of the SYN flood attack.




## 7. Recommendations

1. **Mitigation Strategies**:
    - Implement rate limiting and SYN cookies on the affected server to handle SYN flood attacks.
    - Configure firewalls and intrusion prevention systems to detect and block high volumes of SYN packets.
2. **Network Monitoring**:
    - Enhance network monitoring to detect and respond to abnormal traffic patterns promptly.
3. **Incident Response**:
    - Develop and test an incident response plan for DoS attacks, including communication protocols and mitigation measures.