SYN Flood Attack Report – Understanding TCP Exploitation

Objective: Analyze how SYN flood exploits the TCP handshake.

Summary: This report explains how attackers can abuse the 3-way handshake process to overload a target system by initiating a flood of SYN requests without completing the connection.

Key Concepts:

- TCP states: SYN → SYN/ACK → ACK
- Victim allocates memory in half-open state

Indicators Observed:

- Server unresponsive during attack spike
- SYN queue backlog full

Recommendations:

- Implement SYN cookies
- Configure rate-limiting firewall rules
- Enable connection timeout thresholds

Tools: Wireshark

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is a DoS attack.The logs show that the web server stop respond since overload of SYN requests. This event could be a DoS attack named SYN flood attack.

Section 2: Explain how the attack is causing the website to malfunction

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:
1. A SYN packet is sent form the source to the destination (in this situation is the web server) request to connect.

2. Then, the destination replies to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect.

3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect.

In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server's available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.

The logs indicate that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message.