Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The website is overloaded due to a high number of SYN requests, which is hampering response times for visitors.

In record 52 from the IP 203.0.113.0 a SYN request is sent to which the Web server responds to the requester in record 53 with the SYN, ACK packet, where the visitor then acknowledges the connection permission with an ACK packet, however the attacker continues sending SYN packets, when the connection has already been established.

This event could be a direct denial of service (DoS) attack, where the attacker, after establishing a connection with the server, sends approximately three SYN requests per second to the server, a SYN Flood type 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. SYN: It is the initial request that a visitor tries to connect to the web server.

2. SYN, ACK: It is the response from the server indicating that the connection is accepted

3. ACK: It is a packet from the visitor indicating that he recognizes the connection permission.

When an attacker sends a large number of SYN packets at once, it overloads the server, which, when saturated, stops responding appropriately to requests from other visitors, making it impossible to access the service.

Logs indicate that an attacker with IP address 203.0.113.0, after establishing contact with the WEB server, continues to send SYN requests simultaneously, making it impossible for other visitors to access the server.