Cybersecurity Incident Report

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

After reviewing the TCP/HTTP log it seems that the server is under a DoS attack as there is a high volume of incoming traffic sent to the server. The logs show that an attacker with the IP address of 203.0.113.0 is sending consistent SYN traffic to the server which is causing an overload. This event could be a DoS attack on the server, specifically “SYN flooding”.

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.

1. The SYN request from source is sent to the web server requesting a connection
2. Followed by SYN, ACK packet response to the visitor's response allowing the connection.
3. Followed by the ACK packet from the source machine acknowledging the permission to connect.

When malicious actors send a large number of SYN packets all at once, it slows down the servers and eventually crashes the servers which halts normal server operation for visitors and employees. The log indicates a numerous number of SYN packets being sent to the server by the attacker with an IP address of 203.0.113.0 which is an act of DoS attack. This is slowing down the server and got to the point where the server is no longer granting access to the employees who have the right to access the server because there are no server resources left for legitimate TCP connection requests.