

# Cybersecurity Incident Report

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

The type of attack that caused the network interruption is a **TCP SYN Flood Attack**.

- **What it is:** This is a type of Denial of Service (**DoS**) attack that exploits the TCP protocol connection process, known as the "three-way handshake."
- **How it occurred in the scenario:** The attacker sent a massive volume of connection requests (**SYN**) to the web server. However, the attacker never finalized the connections. This forced the server to keep these connections "half-open," consuming all available memory and resources (CPU/RAM).
- **Consequence:** Because the server exhausted its capacity to process new connections, it stopped responding to legitimate employees, resulting in the "Connection timed out" error.

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

The **SYN Flood** attack causes the website to malfunction by paralyzing the server's communication process through resource exhaustion.

1. **Abuse of the Three-way Handshake:** Normally, a TCP connection requires three steps: the client sends a **SYN** signal, the server responds with a **SYN-ACK**, and the client confirms with an **ACK**. The website functions when these steps are successfully completed.
2. **Creation of "Half-Open" Connections:** During the attack, the intruder sends thousands of SYN signals but ignores the server's SYN-ACK responses. This leaves the server in a state of perpetual waiting, looking for the final step (the ACK) that never arrives.
3. **Memory Exhaustion (Backlog Queue):** The server has a limited table to store these pending connections. When this table becomes filled with fake "half-open" connections, the server can no longer accept any new requests.
4. **Failure for Legitimate Users:** When an employee tries to access the website, the server has no "space" left in its memory to process that new legitimate request,

resulting in the "Connection timed out" error message.

r: