**Cybersecurity Incident Report: Analyse Network Attacks**

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

**Name of the network intrusion attack:** DoS Attack - SYN Flood

**Description of the attack:** One potential explanation for the website’s connection timeout error message is a DoS attack. The logs indicate that the web server ceased responding after being inundated with SYN packet requests. This event aligns with characteristics of a DoS attack specifically known as SYN flooding.

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

**Explanation of the TCP three-way handshake:** When website visitors attempt to connect to the web server, a TCP three-way handshake occurs:

1. **SYN:** The client sends a SYN packet to the server, requesting to establish a connection.
2. **SYN-ACK:** The server responds with a SYN-ACK packet, acknowledging the request and allocating resources.
3. **ACK:** The client sends an ACK packet back, finalizing the handshake and establishing the connection.

**Impact of a SYN Flood Attack:** During a SYN flood attack, a malicious actor floods the server with a high volume of SYN packets simultaneously, overwhelming its capacity to allocate resources for legitimate connection requests. This flood exhausts the server’s available connection resources, preventing it from responding to genuine connection attempts.

**Log Analysis:** The logs clearly indicate a sharp increase in SYN packets from a single, unfamiliar IP address. This flood of SYN packets saturated the server’s resources, leading to its inability to process legitimate connection requests. Consequently, legitimate users experienced connection timeouts when trying to access the website.

**Conclusion:** The SYN flood attack severely disrupted the functionality of the company’s website by overwhelming its server with excessive SYN packets. Immediate measures were taken to mitigate the attack, including temporarily taking the server offline and implementing IP blocking. Moving forward, enhanced network defences, such as rate limiting and more robust firewall configurations, are recommended to mitigate future attacks.