# Cybersecurity Incident Report

|  |
| --- |
| **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 the server is undergoing a successful Denial of Service attack.  The logs show that the server has been overwhelmed by a large number of SYN packets from an unfamiliar IP address and is no-longer serving web-pages to employees.  This event could be a Denial of Service attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| The three steps of a TCP handshake are:  1. SYN (Synchronize): The client initiates a connection with the server by sending a SYN packet to the server  2. SYN-ACK (Synchronize-Acknowledge): The server responds with a SYN-ACK packet, indicating that it has set aside resources for the connection.  3. ACK (Acknowledge): The client acknowledges server’s response by sending a ACK packet, at this point the connection is established.  When a malicious actor sends a large number of SYN packets all at once, the target server upon receiving each request allocates resources for each connection. However since the attacker is initiating a large number of connections all at once and not completing them, the server now has a large amount of computing resources allocated to these connections that are not being freed. If the number of these requests is large enough the server will quickly run out of connection slots and memory. The server will begin to slow down until it eventually crashes if attack continues. In this event legitimate users of the server will find it increasingly challenging to communicate with the server or the server will become completely unreachable. This is called a Denial of Service attack.  The logs indicate that the serve was functioning properly responding to requests from visitors. However, a user with an unfamiliar IP address began initiating a large number of connections with server, sending many SYN packets to the server. This was the start of a DoS attack. At the start of the attack the server was still able to serve web-pages to company employees as well as respond to the attacker, however as the number of connection requests from the attacker increased, the server began taking too long to respond to requests for web-pages and as result these request were generating time out errors. Eventually server become completely unresponsive to all legitimate requests and the logs show the attacker overwhelming an unresponsive server with SYN packets. |