# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 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: All the ports are full and only the first part of the SYN/ACK handshake is happening. Since ports are full, the server is unable to function.  The logs show that: There is initially successful connection but the server stops responding due to being overwhelmed by SYN requests.  This event could be: A DoS SYN flood attack. |
|

|  |
| --- |
| Part 2: Explain how the attack is causing the website to malfunction |
| Three steps of the handshake:   1. The device sends a SYN (synchronise) packet request to the server to connect; 2. The server responds with a SYN/ACK packet to acknowledge receipt of the device’s request. It then leaves a port open for the final step of the handshake. 3. The server receives the final ACK packet from the device and a TCP connection is established.   The incident occurred in the afternoon. The IT Team became aware of the issue because of an automated alert indicating that there was a problem with the web server. The IT department also attempted to visit the company website and received the same error. To investigate the issue further we used a packet sniffer to investigate the activity.  In the beginning there were several requests that proceeded through the complete SYN/ACK handshake and resulted in an HTTP request (indicating connection to the server). Later, the SYN/ACK request was no longer being sent back by the server indicating that the ports were full. This can be seen in several lines where the server sent an RST/ACK packet instead of a SYN/ACK packet and eventually was unable to send any reply due to being overwhlemed.  The issue is most likely a DoS SYN flood attack given the high volume of SYN requests from a single IP address, and also the fact that the later requests do not proceed to the later parts of the handshake. This is supported by there only being one IP address sending requests starting at about 21.13 with no response from the server.  We can set up a firewall to stop this IP address from attacking; however, the attacker can use IP spoofing to attack again. To prevent this issue from happening again in the future, we could configure a firewall to prevent IP spoofing—create a rule to reject all incoming traffic that have the same IP address as local network |