# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| At 03:39 AM this morning the first indication of the incident took place. This is a SYN Flood Attack, a type of Denial of Service Attack. This attack works through the TCP/IP. it works by flooding the network with requests, which I have gone into detail on below. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| Under normal circumstances, a user PC will send a SYN (Synchronize) packet to the PC or server it wants to connect to. The server then acknowledges the connection and sends through a SYN/ACK packet back to the initializing PC. The target PC then sends through a ACK packet of its own and a connection is established. This connection requires a 3-way handshake of sorts to work. If you flood a network with SYN requests, the server may not be able to handle them all and start to slow down or even crash. This is because each SYN request requires memory and bandwidth to be dealt with and too much at one time may cause the server to crash This has ultimately affected subsequent legitimate connections from employees and customers. The first indication of this is at 06:23AM. |