# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| Based on the logs we reviewed in the wireshark data forms we can come to the understanding that this was a decisive Synchronize (SYN) Flood Attack causing a DoS. The log entries are business as usual apart from a few gateway timeouts until the mid-late #70’s. This is where we started to get more gateway timeouts as well as more Synchronize Resets. The resets were consistently showing up every 5 log entries on average until log #125 where we started to receive a massive influx of SYN log entries without SYN acknowledge entries in a very short period of time until we decided to shut the system down manually after log #214. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| Due to the massive influx of SYN messages to our server, this caused an overload of information that overwhelmed the server’s resources and depleted its ability to process further TCP requests. This in turn caused visitors to be unable to connect to the website and gave them an error message. |