# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| The problem that is coming up frequently is the inability to establish or maintain a connection. This seems to be due to the number of requests the server is receiving in establishing a connection. In the log, there are valid requests that come from IP addresses in a normal volume requesting sales activity. There is a recurring SYN request that is establishing a connection coming from an IP address. This is resolved by the server and a connection is established. This request is then repeated multiple times, in addition to valid requests. This indicates to me that this is a SYN flood attack, a type of DOS attack. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| When trying to establish a connection, there is a three way handshake process that occurs. In this case of the IP address that is performing the suspected attack, a SYN request is sent from the attacker’s IP address to establish a connection. The server then responds by acknowledging their request and giving them the proper authorization.  The attacker’s system then sends an ACK, or acknowledgement, back to the server and a connection is established. Once the attacker has done this once, the request is conducted multiple times in high frequency among other valid requests. This means the server attempts to respond to the requests. A high volume of requests can slow the server down, causing valid requests to slow down or time out completely, as it attempts to resolve the attacker’s requests. Eventually, the server shuts down completely, as too many requests are made from the attacker. The logs indicate that the attacker has sent the TCP SYN requests multiple times in high frequency. As the request is being resolved, another request is sent and so on. Eventually, valid requests were completely shut out until only the attacker’s requests were being evaluated. Even the attacker’s requests were not concluding, indicating that the server has stopped responding.  My recommendation in preventing this in the future is to implement a SYN request timer that spaces the requests an IP address can make at a time. For valid users, this will likely show no change in usage. But for an attacker, this will prevent them from using the same IP address to send a request. In the event of a DDOS, the attacker will be forced to use many IP addresses, which is very difficult to coordinate and very costly to establish. |