# Cybersecurity Incident Report

Scenario:

This issue involves with a website needing help with a potential cyber-attack activity that infected a company’s website security infrastructure. This documentation explains the details behind the issue of what happened in this manner.

|  |
| --- |
| **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 logs show that: A large number of TCP SYN requests were shown to overwhelm the network incoming traffic to cause the inability to respond to the SYN requests for the system for the website to function accordingly.  This event could be: DOS attack that is initiated by an attacker using a SYN flood method to overwhelm the system capacity of a website to get it shut down for hackers to exploit it to gain unauthorized control of the security framework. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:  1. **a connection between server and client is established, so the target server must have open ports that can accept and initiate new connections. The client node sends a SYN (Synchronize Sequence Number) data packet over an IP network to a server on the same or an external network. The SYN packet is a random sequence number that the client wants to use for the communication (for example, X). The objective of this packet is to ask/infer if the server is open for new connections.**  2. **When the server receives the SYN packet from the client node, it responds and returns a confirmation receipt – the ACK (Acknowledgement Sequence Number) packet or SYN/ACK packet. This packet includes two sequence numbers.**  **The first one is ACK one, which is set by the server to one more than the sequence number it received from the client (e.g. X+1).**  **The second one is the SYN sent by the server, which is another random sequence number (for example, Y).**  **This sequence indicates that the server correctly acknowledged the client’s packet, and that is sending its own to be acknowledged as well.**  3. **The client node receives the SYN/ACK from the server and responds with an ACK packet. Once again, each side must acknowledge the sequence number received by incrementing it by one.**  **So now it’s the turn of the client to acknowledge the server’s packet by adding one to the sequence number (in this case, Y+1), and resend it to the server.**  **Upon completion of this process, the connection is created and the host and server can communicate.**  **All these steps are necessary to verify the serial numbers originated by both sides, guaranteeing the stability of the connection.**  **Since both hosts must acknowledge the connection parameters of the other side, a missing or out-of-order segment can be quickly detected before the actual data transfer process is initiated.**  Explain what happens when a malicious actor sends a large number of SYN packets all at once: The attacker is able to overwhelm all available ports on a targeted server machine. This causes the targeted device to respond to legitimate traffic poorly or not at all. This gives hackers the ability to exploit your computer where you have little control to fix in this manner while files are being overwhelmed to infect the system more to fail massively.  Explain what the logs indicate and how that affects the server:  Logs files include information about system performance that can be used to determine when additional capacity is needed to optimize the user experience. Log files can help cybersecurity SOC analysts identify slow queries, errors that are causing transactions to take too long or bugs that impact website or application performance on a computer. |