# Cybersecurity Incident Report

|  |
| --- |
| **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 web server is overwhelmed with network traffic coming externally into the internal network with SYN rquests flooding the server causing it to be unresponsive which is the reason why we see timeout messages in the logs and the reason why the websrver cannot service clients.**  The logs show that: **there is abnormal activity ocurring on the network the public ip address 203.0.113.0 is constantly targets the web server with SYN data packets overwhelming the system causing timeouts which impacts business users from sending HTTPS rquests.**  This event could be: **an attempt of a Network Level DOS attack inpersonating the internal network in thinking that the outsider is part of the internal network. During the SYN attack the attacker transmits ICMP packets which halts communications from the web server.** |
|

|  |
| --- |
| **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. **The requestors send a SYN data packet to the web server using the TCP protocol to gain access to the website via HTTPS.**  2. **The web server acknowledges this rquest from the client and attempts to fulfill this request in responding with a SYN/ ACK packet back to the client machine.**  3. **The client establishes a TCP connection with an ACK packet allowing them authorization to gain acess to the website.**  Explain what happens when a malicious actor sends a large number of SYN packets all at once: **When the attacker sends large and consistent SYN packets to the destination it ovrwhelms the server which restricts its functionality of servicing clients with access to its website.**  Explain what the logs indicate and how that affects the server: **This is an indication of an outside public ip address attacking the server with SYN flooding. By configuring the firewall to accept only ip addresses in a particular range would mitigate this risk. A future recommendation would be Implementing a NGFW firewall would be the ideal solution as this has more advanced capabilities than stateful / stateless firewalls which provides deep packet inspection which also performs threat intelligence getting its updates from the cloud.**  **Alternatively we should encrypt our network traffic using a VPN where a tunnel is created between requestor and servic provider, by encypting data packets would be encapsulated in other packets making it unreadable for any potential attackers.** |