# SYN Flood: Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| This SYN Flood attack was discovered and notified via automated alert from our monitoring system, which indicated a problem within the web server. Upon attempting to visit the company’s website, the user will be prompted with a connection timeout error.  While reviewing Wireshark TCP\_HTTP log entries, a network protocol analyzer, the cyber security analyst found multiple rapid TCP SYN requests being sent by an unfamiliar IP address. Initially, the server responded to the first TCP handshake, as volume of attacks increased the server quickly because overwhelmed and unable to respond to legitimate client requests.  The attack resembles a Denial of Service (DoS) SYN Flood attack. The attacker initiated a flood of SYN requests from a single IP, eliminating the possibility of a DDoS attack which would come from multiple IPs. As the attacker continued to flood the webserver with SYN requests, the number of requests became greater than the number of ports the web server could handle, resulting in the inability to fill requests for legitimate traffic. Ultimately resulting in legitimate users receiving a connection timeout error. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| A SYN flood attack is when a malicious attacker manipulates and abuses the TCP handshake process, repeatedly sending SYN requests to the webserver. The webserver will attempt to respond to each SYN request but quickly becomes overwhelmed due to the limited number of ports available to process the requests. The attacker’s goal is to “flood” the server with rapid synchronize (SYN) requests, to over burden the server’s ability to process legitimate requests.  During a legitimate TCP handshake, the source IP will send a synchronize (SYN) request to the webserver. The webserver will in return send back a synchronize acknowledge [SYN,ACK] packet, which identifies the server has recognized and acknowledged the source IP request, last the source IP will send back an acknowledge [ACK] packet, finalizing the three-steps to the TCP handshake.  Initially, the attack will slow down network operations and functionality, users will experience longer loading times while using the website, eventually as the SYN flood attack continues, the server will become overwhelmed, and users will lose complete functionality of the website.  The consequences of a SYN flood attack can result in financial damage, inability to operate during normal business hours, loss of customer trust and potentially damage to the server and data within the organization.  There are many ways to prevent future attacks such as:   1. Utilize subnets within the organization network. This will ensure the outage does not affect/spread to the entire network infrastructure and can be contained within the subnet. 2. Use of Next Generation Firewall (NGFW) which will actively monitor network traffic and identify suspicious activity real-time. 3. Utilize VPNs to encrypt the webserver data and IP address. |