# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| This attack was identified after an automated alert from our monitoring system highlighted an issue with the web server. When attempting to access the company’s website, users encountered a connection timeout error message.  Upon analyzing the TCP/HTTP log with Wireshark, a network protocol analyzer, the cybersecurity analyst discovered a high volume of TCP SYN requests originating from an unfamiliar IP address. The server initially handled the requests and continued normal operations, but the sheer volume eventually overwhelmed the server, preventing it from responding to legitimate requests.  This appears to be a Denial of Service (DoS) SYN flood attack. The large number of SYN requests originated from a single IP address, indicating that the attacker is not currently using multiple devices for a Distributed Denial of Service (DDoS) attack. As the volume of SYN requests exceeded the server's available ports, the server was unable to process further requests, causing all attempts to access the site to result in a connection timeout error. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| A SYN flood attack is when a malicious actor abuses the TCP handshake process and repeatedly sends requests to connect to the web server. The server tries to respond to each one of these requests but only has so many ports available to do so, and the attacker’s goal is to send more requests than the amount of server ports.  At first, the attack will slow the network down and users may experience long loading times when visiting the site but eventually the server will become too overwhelmed and will be completely unable to operate.  The consequences of this attack include loss of revenue due to inability to complete regular business operations, loss of customer trust, and potential damages to the server and its data.  There are many ways to prevent future attacks like this such as:  1. Using a Next Generation Firewall (NGFW) to proactively monitor the network for suspicious activity  2. Using VPNs and encryption to conceal the IP address of the web server  3. Using subnets to ensure that one outage does not affect/spread to the entire organization’s infrastructure. |