# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| This afternoon, I had an automated alarm from the company's monitoring system. I visited the company's website and received a timeout error. I used a wireshark packet sniffer packet sniffe in transit to and from the web server and noticed a large number of TCP SYN requests coming from a single source of an unfamiliar IP address. Due to the large number of requests, the server was slowing down.  This event is definitely a DoS attack, specifically a TCP SYN request DoS attack, so I took the server offline to recover it and added the suspicious IP address to the firewall.   This attack might happen again as the attackers can easily spoof a new IP address and attack again. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| This is a TCP SYN request DoS attack. A threat attacker uses a tool to spam/overflow the network or the server by sending a SYN (synchronize) request and not sending an ACK (acknowledge) back.  Usually, when a client requests access to a website, the TCP protocol takes over. It will initiate a three-way handshake:   1. The client sends a SYN (synchronize) request to the web server. 2. The web server acknowledges the SYN request and responds with a SYN-ACK (synchronize acknowledgment). 3. The client system sends back an ACK (acknowledge) to complete the handshake.   This is how a three-way handshake works.  But in a TCP SYN request DoS attack, the last part of the handshake is not completed, which leaves the server half open, waiting for an ACK from the client. With these incomplete requests being repeatedly sent, the network gets overloaded, slowing down services and causing a denial of service to legitimate users, potentially crashing the server. |