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 that the web server is under a SYN Flood attack. After receiving an alert from the monitoring system, I used a packet sniffer to analyze the incoming network traffic and discovered a large number of TCP SYN requests coming from a single unfamiliar IP address. These requests were targeting the company's web infrastructure at a very high rate. The logs showed that the web server was constantly being pinged with SYN packets, which resulted in it becoming overwhelmed and eventually unresponsive. This kind of activity strongly indicates a SYN Flood attack — a type of Denial-of-Service (DoS) attack designed to exploit the TCP handshake process. The result was a service disruption, where users and employees were unable to access the company's website to view vacation packages or make recommendations to clients.

Section 2: Explain how the attack is causing the website to malfunction
When a legitimate user tries to establish a connection with a web server, a three-way handshake takes place using the TCP protocol. This handshake involves three steps: The client sends a SYN (synchronize) packet to the server to initiate the connection. The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the request. The client sends back an ACK (acknowledge) packet, completing the handshake and establishing a stable connection. However, in the case of a SYN Flood attack, a malicious actor sends a high volume of SYN packets to the server, often without completing the handshake.

The attacker may spoof source IP addresses to avoid detection. Since the server allocates memory and resources for each half-open connection, it becomes overloaded and unable to accept new connections, including legitimate ones.

The logs clearly show a surge in SYN packets from a single IP address. This overwhelming flood of connection attempts left the server unable to complete handshakes or respond to real users, resulting in connection timeouts and effectively taking the web server offline. To temporarily mitigate the issue, the server was taken offline for recovery, and the attacker's IP address was blocked at the firewall. However, this is a short-term solution, as attackers can easily switch IPs or use botnets to launch distributed versions of this attack.