Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

A connection timeout error message was received when accessing the company's website server. The connection must have been interrupted due to the large volume of incoming traffic. WireShark was used to capture data packets in transit to and from the web server and the logs show that the server has been receiving a large number of TCP SYN requests from an unfamiliar IP address. This event could be a Denial of Service (DoS) attack by a malicious actor.

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.

1. The client sends a synchronize request to the server in the form of SYN packets, under TCP/IP protocol.
2. The server then responds with a SYN/ACK packet to acknowledge that it has received the request.
3. The client then sends a final ACK packet, confirming that the connection has been established successfully.

When the server receives a large number of SYN requests, it gets overloaded and loses its ability to respond to them. This results in slowing down, or in other cases crashing of the website. A malicious actor exploits the TCP protocol by sending many SYN requests, which hampers the connectivity of the website.

After analyzing the logs obtained from a packet sniffing tool, WireShark, it is observed that an unknown source IP has been sending many SYN requests to the server which has led to a disruption in network connection. The server has even stopped responding to legitimate employee visitor traffic. This is possibly a Denial of Service (DoS) attack.

In response to this malicious activity, we have temporarily switched the server to offline so that the machine can recover. The company's firewall has also been configured and the suspicious IP address has been blocked. The attacker can still spoof other IPs, therefore we need to discuss the further steps to be taken with the manager. We also need to take up certain measures to prevent this from happening in the future.