Scenario

You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. The employees of the company regularly access the company's sales webpage to search for vacation packages their customers might like.

One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser.

You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.

You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won't last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees

For the logs, please see the document "How to read a Wireshark TCP_HTTP log.pdf".

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 a DoS attack. The logs show that there are a bunch of SYN requests before it stops responding which could be a SYN flood attack.

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. Explain the three steps of the handshake: 1. SYN packet sent from requesting device to connect to the server 2. Destination server responds with a SYN-ACK packet to accept the connection request and reserves resources 3. Finally the requesting device sends and ACK packet back to the destination In the case of a SYN flooding attack a device sends a bunch of the initial SYN packets which overwhelms the destination server which then ends up reserving all its resources not allowing for any other connections. The logs indicated that as the flood of SYN packets came in the server became overwhelmed and no longer started processing new SYN requests, thus users started to get timeout requests.