Cybersecurity Incident Report

Scenario
Review the following scenario. Then complete the step-by-step instructions.

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.

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 there is **a Dos attack**. The logs show that the server stops responding because it has been overloaded with too many SYN packet requests. This event could be a SYN flood attack or a DoS 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
2. SYN-ACK
3. ACK

The client sends a SYN packet from the source to the destination, requesting a connection. Then, the destination responds with a SYN-ACK packet, acknowledging the client's request. Finally, the ACK packet is sent from the source so the destination, acknowledging the server's permission to connect, and then connection is now established.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: **When a malicious actor sends a large number of SYN packets all at once, the website cannot handle all the SYN requests. Hence, others users cannot connect to the website because**

Explain what the logs indicate and how that affects the server: **The logs indicate that the web server is being overloaded and cannot process the SYN requests of its users. Hence, the server cannot open connections to new users when their connection times out.**