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:

The web server is experiencing a ***SYN flood attack(a type of DoS attack)*** where an attacker sends a large number of TCP SYN rquests but never completes the three-way hanshake. This exhausts the server's resouces, making it unable to process legimate connections.

The logs show that:

A high volume of ***TCP SYN packets*** is coming from a single IP (203.0.113.0), but the expected ***ACK responses*** to completye de handshake are missing.This means the server is holding open a large number of half-open connections, consuminh system memory and preventing legimate users from acessinf the website.

This event could be:

A ***SYN flood attack***, which is a ***DoS(Denial-of-service) attack*** aimed at overwhelming the server's ability to handle connections requests, leading to perfomance degradation and an eventual unavailability.

Section 2: Explain how the attack is causing the website to malfunction

One potential explanation for the website's connection timeout error message is:

When a user visits a website, the TCP three-way handshake is required to establish a connection.

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(synchronize): The client sends a SYN packt to the server , requesting to establish a connection.

2.SYN-ACK(Synchronize-Acknowedge): The server responds with a SYN-ACk packet, acknowledging the request and confirming readiness for communication.

3.ACK(Acknowledge): The client responds with an ACK packet, completing the hanshake and establishing a conncection.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

1. The attacker floods the server with a massive number of SYN packets buds neves responds with the final ACK.
2. The server reserves memory and system resouces for each half-open connection, waiting for the missing ACK.
3. Eventually the server reaches its limits of pending connections and can no longer accept new legimate users.
4. This results in connection time-ou errors for real visitors, affectively denying acces to the website.

What the logs indicate and how that affects the server:
The logs indicate an abnormally high number of SYN packets from 203.0.113.0, with very few corresponding SYN_ACK and ACk responses This pattern sugests that:

- The server is being overwhelmed with half-open connections.
- It is running out of available resouces, leadinf to slowdowns or total service failure.
- Legimate users are unable to acces the website, affecting emplyees and costumers.