# Cybersecurity Incident Report

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 flooded with requests  The logs show that: A large number of TCP SYN requests came from an unfamiliar IP address  This event could be: Due to a malicious actor spoofing an IP address and sending tons of SYN packets from that address to carry out an DoS attack  After being notified by the automated alert of the monitoring system about the web server I checked the logs. The logs indicated that there was an abnormally large number of SYN requests all coming from the same unfamiliar IP address. It seems that these packets overwhelmed the web server and caused it to be unresponsive to normal requests. This is likely due to a malicious actor carrying out 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. Sender sends a Syn packet   2. Receiver sends a Syn/ack to sender   1. Sender sends a ack to receiver to finish handshake   Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends too many SYN packets at once, the server gets flooded and can’t respond to genuine requests.  Explain what the logs indicate and how that affects the server: The logs indicate that there is an abnormally large number of SYN requests coming from one IP address. This affects the server by making it overwhelmed and lost its ability to respond to events.  The attacker is using the TCP protocol for the SYN attack. In a normal TCP/UDP handshake process there are three steps. The sender sends a SYN packet, the receiver sends a SYN/ACK packet back and then the sender finishes the handshake with an ACP packet to the receiver. But when a large number of SYN packets get sent at once, the server is liable to be overwhelmed and unable to respond to genuine requests to the server. The logs indicate this, especially since a majority of the packets come from the same unfamiliar IP address. Technically this is also called a DoS attack (large number of network requests from a single source). |

Reflection after reviewing exemplar: SYN stands for synchronize and during the second step the receiver reserves space for the data stream of the TCP protocol to start.