Cybersecurity Incident Report

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.

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

The type of attack described in this document is a direct denial-of-service (DoS), specifically a SYN flood attack.
In this attack, the attacker exploits the TCP handshake process to exhaust the server's resources, where travel information needed by employees to inform customers is stored, preventing legitimate users from accessing the website. It is called a SYN flood because the attacker sends a large number of synchronization requests, overwhelming the server's ability to complete the handshake and transmit correct information.

The log shows that a single IP address, 203.0.113.0, is sending a high volume of TCP SYN requests to the web server (port 443) repeatedly.
The server responds with SYN-ACK packets, but the final ACK of the handshake is never completed, leaving numerous half-open connections.
Legitimate connection attempts by employees (highlighted in green) begin to fail, showing errors such as HTTP 504 Gateway Time-out and [RST, ACK] responses, indicating that the server is overloaded.
Only after entry 125 does the server completely stop responding to legitimate traffic, while the attacker's flood of SYN packets continues unabated.

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. SYN: The client (e.g., an employee’s browser) sends a SYN packet to the web server (port 443) to initiate a connection. This packet includes a sequence number to start the communication.

2. SYN-ACK: The server responds with a SYN-ACK packet, acknowledging the client’s request and sending its own sequence number. This reserves server resources for the final step of the handshake.

3. ACK: The client replies with an ACK packet to confirm the connection. At this point, the TCP connection is fully established, and data transfer (such as loading a webpage) can begin.

When a malicious actor sends a large number of SYN packets simultaneously, without completing the handshake by sending the final ACK, it creates a SYN flood attack. The server responds to each SYN packet with a SYN-ACK and waits for the final ACK, keeping each connection in a "half-open" state. Since the attacker never sends the ACK, these half-open connections consume server resources (memory, connection queue). When the server’s capacity is exhausted, it cannot accept new connections, even from legitimate users, leading to a Denial of Service (DoS).
The logs show that a single IP address (203.0.113.0) is repeatedly sending SYN packets to

the server (port 443), highlighted in red. Initially, the server responds with SYN-ACK packets, but the attacker does not complete the handshake. Over time, the flood of SYN requests overwhelms the server.

The logs show errors such as:

HTTP/1.1 504 Gateway Time-out: Indicates the server is too slow or unable to respond.

[RST, ACK] packets: Sent by the server to reset connections from legitimate users, meaning the server cannot process their requests.

After log entry 125, the server stops responding to legitimate traffic entirely and only the attacker's SYN packets continue to be logged.
This indicates the server is completely overwhelmed and effectively offline for employees trying to access critical information like sales pages.
Since the attack originates from a single IP address, this is a **direct DoS SYN flood attack**, not a distributed (DDoS) attack. The server's resources are exhausted, preventing normal operation and disrupting business services.