Cybersecurity Incident Report

CASE STUDY-01

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 that 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 an 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 the 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.

Incident ID: 2025-05-001

Date/Time Reported: 2025-05-18, 10:30 AM

Reported By: Navya Nagpal, IT Security Analyst

Department: IT Security

At approximately 10 AM, 2025-05-20, unusual network traffic was detected on the company's web server log records. A SYN packet was repeatedly flooding the network pathways of a webpage.

Section 1: Identify the type of attack that may have caused this network interruption

One potential explanation for the website's connection timeout error is a network-level DOS attack. Logs indicate that after some time, the system stops responding to the normal visitor traffic. This event could possibly 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. The **SYN** packet is the initial request where a visitor is trying to connect with the web page on the web server.

2. The **SYN,ACK** packet is the web server's response to the visitor's request, agreeing to build a connection.

3. The **ACK** packet is the final step where the visitor's machine acknowledges the permission to connect.

In this case of a SYN flood attack, the malicious actor will send a large number of SYN packets all at once, which overwhelms the server's availability of resources to reserve a connection. When this happens, the normal traffic, i.e., the authorised visitors, are denied access to the resources.

Due to server overload, incoming connection requests from visitors cannot be processed, causing them to receive a connection timeout error.

Actions taken:

1. An immediate response plan was activated.

2. Regular analysis of Logs and traffic patterns
3. Enabled SYN cookies
4. Updated Firewall rules accordingly
5. Deployed Intrusion Prevention System (IDS)
6. Disabled unnecessary services
7. Updated policies and training

Reported by:
XYZ
IT Security Analyst
Signature: ______________________
Date: 2025-05-20