SCENARIO PRACTICE

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.

CYBERSECURITY INCIDENT REPORT: SYN FLOOD ATTACK

EXECUTIVE SUMMARY

On January 2, 2026, at approximately 10:20 PM WAT, the company's public-facing sales webpage experienced a service outage due to a Denial of Service (DoS) attack. The attack manifested as a SYN flood, which overwhelmed the web server's capacity to handle new connection requests.

Immediate actions were taken to contain the incident, and a plan for long-term remediation is in development.

IMPACT ANALYSIS

The attack successfully disrupted service for both external customers and internal employees, who received connection timeout errors when attempting to access the website.

The web server became unresponsive due to resource exhaustion caused by the accumulation of "half-open" TCP connections, as it was unable to complete the three-way handshake for legitimate requests. The primary business impact was a complete service disruption for online sales and package searches.

ACTIONS TAKEN

The following actions were immediately executed to contain and mitigate the active threat:

1. **Detection**: A packet sniffer was used to capture data packets, revealing a high volume of TCP SYN requests originating from an

unfamiliar IP address.

2. **Containment**: The web server was temporarily taken offline to allow system recovery and return to a normal operating status.
3. **Initial Mitigation**: The company's firewall was configured to block the identified malicious IP address.

ROOT CAUSE ANALYSIS

The incident was caused by the exploitation of a vulnerability in the standard TCP three-way handshake procedure. In a typical connection, a client sends a SYN packet, the server responds with a SYN-ACK, and the client replies with a final ACK. The attacker sent numerous SYN packets without sending the final ACK, causing the server to reserve memory resources for each incomplete connection until its connection table was full. This consumed all available resources, preventing legitimate users from establishing new connections.

The underlying root cause is a lack of sufficient, multi-layered DDoS protection mechanisms capable of handling high-volume, spoofed traffic attacks at scale.

RECOMMENDATIONS

To prevent recurrence and improve our security posture, the following measures are recommended:

- **Implement SYN Cookies**: Enable SYN cookies at the operating system or application level to mitigate attacks by deferring resource

allocation until a valid final ACK packet is received.

- **Rate Limiting**: Configure firewalls and load balancers to limit the number of SYN requests per second from a single source IP address.
- **Increase Backlog Queue**: Temporarily increase the maximum number of allowable half-open connections to create a buffer during an attack.