Cybersecurity Incident Report

Section 1: Identification of the Type of Attack Responsible for the Network Disruption

One possible explanation for the website's connection timeout errors is a network-level denial-of-service (DoS) attack, specifically a SYN flood. The server logs indicate that the web server ceases to respond to legitimate employee traffic, resulting in repeated error messages stating that connections cannot be established or maintained. Beginning with log entry 125, the server exclusively logs activity from a single IP address—the suspected attacker—while legitimate traffic is no longer processed. This pattern strongly suggests a direct DoS SYN flood attack.

Section 2: Explanation of How the Attack Is Causing Website Malfunctions

TCP Three-Way Handshake Explained

When a website visitor attempts to establish a connection with a web server, a **three-way handshake** occurs using the **TCP (Transmission Control Protocol)**. This process ensures a reliable connection between client and server. The steps are as follows:

1. **SYN (Synchronize)**: The visitor's device sends a SYN packet to the server to initiate the connection.

2. **SYN-ACK (Synchronize-Acknowledge)**: The server responds with a SYN-ACK packet, acknowledging the request and reserving resources for the session.

3. **ACK (Acknowledge)**: The visitor's device sends an ACK packet back to the server, confirming the connection. At this point, the TCP connection is established.

What Happens During a SYN Flood Attack

In a **SYN flood attack**, a malicious actor sends a large volume of SYN packets to a web server without completing the handshake. Since the server allocates resources for each incoming SYN packet and awaits the final ACK that never arrives, its connection table fills up. If the number of SYN requests exceeds available server resources, the server becomes overwhelmed and **unable to process legitimate traffic**, resulting in a **Denial of Service (DoS)** condition.

What the Logs Indicate and How It Affects the Server

- **HTTP/1.1 504 Gateway Time-out (text/html)**: This error message is returned by a gateway server when it does not receive a timely response from the web server. It informs the user's browser that the request could not be completed due to server delay.

- **RST, ACK (Reset-Acknowledge) Packet**: If the TCP handshake cannot be completed—such as when the server fails to send a SYN-ACK—an RST, ACK packet may be sent, resetting the connection attempt. The visitor's browser will display a timeout error, and they may retry the request by refreshing the page.

- **Server Behavior Based on Logs**: Starting from log entry 125, the web server stops responding to legitimate employee traffic. Instead, the logs show only incoming SYN packets from a single IP address. This behavior is consistent with a **direct SYN flood attack**, as the server is no longer able to process legitimate connections and logs only show evidence of the malicious activity.