Cybersecurity Incident Report

Section 1: Identify the Type of Attack Causing the Network Interruption

One potential explanation for the website's connection timeout error message is a **SYN Flood Attack**.

Evidence from Logs:

- Logs show a large number of TCP SYN requests from an unfamiliar IP address.

- The server becomes overwhelmed with half-open connections and cannot process legitimate requests.

Attack Type:

This event is identified as a **SYN Flood Attack**, a type of **Denial of Service (DoS)** attack.

Section 2: How the Attack Causes Website Malfunction

When visitors try to connect to the website, a three-way TCP handshake is used:

1. The client sends a **SYN** (synchronize) packet to the server.

2. The server replies with a **SYN-ACK** (synchronize-acknowledge) packet.

3. The client responds with an **ACK** (acknowledge) packet to establish the connection.

Malicious Behavior:

In a SYN Flood attack, the attacker sends a massive number of SYN packets but never completes the handshake (no final ACK). This leaves the server resources tied up, waiting for responses that never come.

Log Indications:

- The server responds to many SYN packets but receives no final ACK.
- The server struggles with system resources.
- Legitimate users experience connection timeouts and errors like **504 Gateway Timeout**.

Additional Information

Attack Definition

SYN Flood attacks exhaust server resources by exploiting the TCP handshake mechanism, leading to service disruptions.

Impact on Network Performance

- Half-open connections overwhelm the server.
- The server cannot handle legitimate user requests.
- The website becomes slow or completely inaccessible.

Potential Consequences

- Customer dissatisfaction

- Revenue loss

- Damage to the company's reputation

Prevention Recommendations

- **SYN Cookies:** Protect against half-open connections.

- **Firewall Rules:** Detect and block unusual SYN traffic patterns.

- **Load Balancers:** Distribute network load effectively.

- **Real-Time Monitoring:** Quickly detect and mitigate unusual traffic surges.

Prepared for GitHub publishing.