**Cybersecurity Incident Report.**

**Network Timeout**

The website's connection timeout error could be due to the web server being overwhelmed by a large number of SYN packets from an attacker. As a result, the server was unable to process legitimate requests in a timely manner, leading to timeout errors for website visitors.

**Logs Show the Following:**

* SYN Flood Attack: The logs reveal a high volume of SYN packets from a single IP address (203.0.113.0) targeting port 443 on the server. The server initially responds to these SYN packets, but the attacker continues to send more SYN requests at a rapid pace. This excessive traffic overwhelms the server's capacity to manage connections.
* Impact on Legitimate Traffic: The logs also indicate that during the attack, connection attempts from legitimate visitors were disrupted or timed out. This is evident from the log entries highlighted in yellow, showing HTTP 504 Gateway Timeout errors and [RST, ACK] packets, suggesting the server was unable to complete connections with legitimate users.

**This Event Could Be:** A **Denial of Service (DoS) attack**:

Specifically, this is a type of DoS attack known as a SYN Flood attack. The attacker floods the server with a large number of SYN packets, overwhelming the server's resources and preventing it from handling legitimate connection requests. As a result, users experience connection timeouts and errors because the server cannot process their requests due to the malicious traffic overload.

**What is Happening:**

When website visitors attempt to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The three steps are:

1. SYN Request (Synchronize)
   * The visitor (client) sends a packet with the SYN flag to the web server. This initial packet requests to establish a connection and synchronizes sequence numbers between the client and server.
2. SYN-ACK Response (Synchronization-Acknowledgment)
   * The web server responds to the client with a packet that has both the SYN and ACK (Acknowledgment) flags set. This indicates that the server agrees to establish the connection and also synchronizes its own sequence number with the client.
3. ACK Confirmation (Acknowledgment)
   * The client replies with an ACK packet, confirming it has received the server's SYN-ACK response. This completes the three-way handshake and establishes a full TCP connection between the client and server.

In a SYN flood attack, a malicious actor sends a large number of SYN packets to the server. The web server receives many SYN requests simultaneously and allocates resources for each request. However, if the number of SYN requests exceeds the server's capacity to handle connections, the server becomes overwhelmed. This prevents the server from processing legitimate requests and can lead to a failure in handling new connections, causing timeout errors for legitimate users.

**Log Information:**

The logs indicate that the web server is being targeted by a SYN flood attack, as evidenced by a large number of SYN packets originating from a malicious IP address. As the server attempts to handle these SYN requests, it is unable to process legitimate requests from website visitors due to the overload. This results in error messages such as HTTP 504 Gateway Timeout, as the server cannot respond to requests in a timely manner. Over time, the server may stop responding entirely to legitimate requests, leading to a denial of service for real users.