Cybersecurity Incident Report

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

One potential explanation for the website's connection timeout error message is the struggle the web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace.

The logs show that the web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack.

This event could be a direct DoS 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.

1. The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN stands for “synchronize.”

2. The [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge.”

3. The [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.”

If the number of SYN requests is greater than the server resources available to handle the requests, then the server will become overwhelmed and unable to respond to the requests. This is a network level denial of service (DoS) attack, called a SYN flood attack, that targets network bandwidth to slow traffic. A SYN flood attack simulates a TCP connection and floods the server with SYN packets. A DoS direct attack originates from a single source. A distributed denial of service (DDoS) attack comes from multiple sources, often in different locations, making it more difficult to identify the attacker or attackers.