Cybersecurity Incident Report

Activity Exemplar: Analyze Network Attacks

Section 1: Identify the type of attack that may have caused this network interruption
A potential cause for the website's connection timeout error message is a Denial of Service (DoS) attack. The logs indicate that the web server ceases to respond after being inundated with numerous SYN packet requests. This scenario suggests a type of DoS attack known as SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction
When visitors attempt to access the website, a three-way handshake using the TCP protocol is initiated to establish a connection. This process involves three steps: 1. The source (client) sends a SYN packet to the destination (server) to request a connection. 2. The destination (server) responds with a SYN-ACK packet to acknowledge the request and indicate its readiness to establish the connection. It reserves resources for this potential connection. 3. The source (client) sends an ACK packet back to the destination (server) to finalize the handshake and confirm the connection. In a SYN flood attack, the malicious actor sends an excessive number of SYN packets to the server, overwhelming its ability to handle these requests. The server allocates resources for each incoming SYN request, anticipating the completion of the handshake. However, the malicious actor does not complete the handshake, causing the server to exhaust its resources.