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 that the web server is experiencing a SYN flood attack, a type of Denial-of-Service (DoS) attack. In this attack, an attacker sends a high volume of TCP SYN requests to the server but does not complete the handshake, leaving the server's connection queue overwhelmed and unable to handle legitimate requests. As a result, employees and customers are unable to access the website, impacting business operations.

The logs show an unusually high number of incomplete TCP connections from a single unfamiliar IP address, indicating that the web server is being targeted with a SYN flood. This event could be an attempt to disrupt services or test for vulnerabilities before launching a more sophisticated attack. While blocking the identified IP address can provide temporary relief, additional mitigation strategies such as rate limiting, SYN cookies, and intrusion prevention systems (IPS) should be implemented to prevent similar attacks in the future.

Section 2: Explain how the attack is causing the website to malfunction

When website visitors attempt to establish a connection with the web server, the TCP three-way handshake takes place to initiate communication. First, the client sends a SYN packet to the server, requesting to start a connection. The server responds with a SYN-ACK packet, acknowledging the request and indicating that it is ready to establish a connection. Finally, the client sends an ACK packet, completing the handshake, and allowing data transmission to begin. This process ensures a reliable connection between the client and the server.

However, when a malicious actor sends many SYN packets all at once, the web server attempts to respond by allocating resources for each incoming request. Since the attacker does not complete the handshake, these half-open connections remain in the server’s backlog, quickly consuming available resources. This is known as a SYN flood attack, a type of Denial-of-Service attack that overwhelms the server and prevents it from processing legitimate user requests. As a result, website visitors experience connection timeouts, effectively taking the website offline.

The logs indicate an unusual spike in SYN requests from an unfamiliar IP address, many of which never completed the handshake. This suggests that the web server is under a SYN flood attack, causing it to exhaust system resources and fail to respond to normal traffic. Consequently, employees and customers are unable to access the website, disrupting business operations. While blocking the IP address of the attacker provides a temporary fix, a more robust defense is needed. Implementing SYN cookies, rate limiting, and an Intrusion Prevention System can help mitigate future attacks and protect the web server from further disruptions.