Cybersecurity Incident Report

SYN Flood

Section 1: Identify the type of attack that may have caused this network interruption
Section 1: Identify and Explain the Network Disruption Our investigation into the network interruption began with an automated alert, signaling a problem with the web server and leading to a connection timeout error for website visitors. Analyzing Wireshark TCP/HTTP logs, our cybersecurity analyst detected a surge in TCP SYN requests from an unfamiliar IP address, indicative of a potential Denial of Service (DoS) SYN flood attack.

Section 2: Explain how the attack is causing the website to malfunction
In a SYN flood attack, the malicious actor exploits the TCP handshake, inundating the web server with connection requests. The handshake consists of three steps: 1. SYN (Synchronize): The initiating device sends a SYN packet to the destination device, indicating its desire to establish a connection. 2. SYN-ACK (Synchronize-Acknowledge): In response, the destination device sends a SYN-ACK packet back to the initiating device, acknowledging the connection request and indicating its readiness to proceed. 3. ACK (Acknowledge): The initiating device then sends an ACK packet to the destination, confirming the establishment of the connection. At this point, data exchange can commence between the two devices. The server, constrained by limited ports, struggles to respond, causing a slowdown and eventual operational paralysis. The repercussions encompass revenue loss, eroded customer trust, and potential server/data damage.

To thwart future attacks, proactive measures are crucial:

- Employ a Next Generation Firewall (NGFW) for vigilant network monitoring.
- Utilize VPNs and encryption to shield the web server's IP address.
- Implement subnets to contain outages, preventing widespread infrastructure impact.