Cybersecurity Incident Report

Benjamin Taylor – Google Cybersecurity

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: A Denial of Service (DoS) or more specifically a SYN flood attack is happening.

The logs show that: Repeated TCP SYN packets from the same source IP (203.0.113.0) to destination port 443 (HTTPS) on 192.0.2.1 without completing TCP handshake.

This event could be: A SYN Flood Attack, where the attacker (203.0.113.0) is sending a high volume of half-open TCP connections to the server in order to saturate the connection and prevent it from handling actual traffic. This could result in a connection timeout for real users.

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. Explain the three steps of the handshake:

1. SYN: Client sends SYN packet to server requesting to start a connection.
2. SYN-ACK: Server receives SYN packet and responds with SYN-ACK, acknowledging the SYN from the client and includes the server's own SYN to start the connection.
3. ACK: Client receives SYN-ACK and responds with ACK packet. Both sides are now ready to communicate.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server is left waiting for a response that never comes, due to the hacker not completing the handshake with the final ACK step. The server's connection table fills up, leaving it unable to accept any more connections (even from actual users).

Explain what the logs indicate and how that affects the server: There are hundreds of SYN packets all coming from the same IP address to the same destination, and although the server replies with SYN-ACK to start there is no ACK back to complete the handshake. Users trying to actually connect are given timeouts (HTTP 504 errors).

https://docs.google.com/spreadsheets/d/1enpRzrIao3J2Lp2tOI0hmu1Cu7D7CjLGhFAiTiR9J64/edit?gid=218501934#gid=218501934