Nicholas Coleman

Cybersecurity Incident Report

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

The most likely explanation of why the website is showing an error message is due to the host server being overloaded with SYN requests. This has caused it to crash. The logs show that after log no. 57, there are repeated SYN requests to the server hosting the client’s website. The IP address associated with these requests, 203.0.113.0, already successfully made a connection previously, in logs 52-54. This means that this is most likely a type of Denial of Service (DoS) attack called the “SYN flood attack”. Since the malicious actor has already made a successful request, the abnormal number of subsequent SYN requests is suspicious.

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. Here is an explanation:

1. At first, the website visitor’s device sends a SYN (synchronize) request packet to the website’s server.

2. The server responds to the visitor’s device with an SYN/ACK (synchronize-acknowledgement) packet.

3. The visitor’s device then confirms this by responding with a final ACK packet of its own.

When a malicious actor sends a large number of SYN packets to a server all at once, the server will not be able to handle the other legitimate SYN requests and eventually will crash entirely. The logs indicate that the server received a SYN packet from the IP address, 203.0.113.0. While the website is still functioning, this IP address then proceeds to send more SYN packets. Eventually, around logs 79-97, the server becomes overloaded with requests. After log 97, the server crashes entirely and is unable to handle any legitimate SYN packets from any of the visitors' devices.

In the future, the client’s firewall should be configured to detect and block suspicious traffic patterns as well as limiting the rate of incoming SYN packets to a single IP address. The firewall can also be configured to block packets coming from spoofed IP addresses. Installing an intrusion-detection-system (IDS) can also help the client prevent an attack like this from occurring in the future.