Kimberly Chau

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: ***a DoS attack***

The logs show that: ***numerous SYN requests were sent from one IP address leading to web server having timeout errors and then not responding***

This event could be: ***a direct DoS SYN flood attack***

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. ***First, a [SYN] packet is sent as an initial request from a visitor trying to connect to a web page hosted on the web server.***

2. ***Then, a [SYN, ACK] packet is sent back as the web server's response to the visitor's request agreeing to the connection and reserves system resources for the final part of the handshake.***

3. ***Lastly, a [ACK] packet is sent from the visitor's machine to acknowledge the permission to connect and then a successful TCP connection is made.***

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
The web server starts to struggle with the abnormal amount of SYN requests coming quickly and fails some communications with legitimate employee website visitors. Then shortly after, the web server stops responding completely to legitimate employee visitor traffic and visitors cannot establish or maintain connections to the web server since there are no more available server resources.

Explain what the logs indicate and how that affects the server:
The logs show that many SYN packets are sent from one IP address. At first, the web server is able to make a SYN/ACK connection handshake and complete the HTTP protocol for a normal visitor. However, as the attack continues, we see errors with "[RST, ACK]" and "HTTP/1.1504 Gateway Time-out" appear showing that the web server is unable to respond to requests from a gateway server and SYN requests. Afterwards, the logs only show items that are from the attack and the web server stops responding to any legitimate traffic.