Cybersecurity Incident Report

Cybersecurity Incident Report

Section 1: Identifing 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 Denial of Service (DoS) attack, specifically a TCP SYN flood attack.

The logs show that the web server is receiving an unusually large number of TCP SYN requests from an unfamiliar IP address within a short period of time. These requests are not being completed with the final acknowledgment required to establish a connection.

This event could be a TCP SYN flood DoS attack, which targets the availability of the server by overwhelming it with incomplete connection requests until it can no longer respond to legitimate users.

Section 2: Explaination 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:

1. The client sends a SYN (synchronize) packet to request a connection.
2. The server responds with a SYN-ACK (synchronize-acknowledge) packet.
3. The client completes the process by sending an ACK (acknowledge) packet, establishing the connection.

When a malicious actor sends a large number of SYN packets all at once, the server responds to each request with a SYN-ACK and waits for the final ACK that never arrives. These incomplete connections remain open and consume server memory and processing resources.

The logs indicate a high volume of half-open TCP connections, which causes the server to exhaust its available resources. As a result, the server becomes overwhelmed and is unable to respond to legitimate connection requests, leading to connection timeout errors for employees and customers accessing the website.

Activity Exemplar: Analyze network attacks

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 the web server stops responding after it is overloaded with SYN packet requests. This event could be a type of DoS attack called SYN flooding.

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

When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps:

1. A SYN packet is sent from the source to the destination, requesting to connect.
2. The destination replies to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect.
3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect.

In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server's available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.

The logs indicate that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message.