Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
Connection downtime of the company's website could be due to SYN flood. Wireshark shows a large amount of SYN requests coming from an unknown IP address.

Section 2: Explain how the attack is causing the website to malfunction
This afternoon, I received an automated alert on our SIEM tool indicating that there is an issue with the web server which aligns with the connection timeout of our organisation's website. I used Wireshark to capture data packets in transit to the web server, and noticed a large number of TCP SYN requests from an unfamiliar IP address which indicates a SYN flood attack. This is causing the website to malfunction as the server is overwhelmed by the volume of incoming traffic and is not able to respond to the large number of SYN requests causing the website to timeout. For the meantime, I have blocked the threat actor's IP address in the firewall but have alerted the manager as this will only last for so long, and so that we can work on preventing this from happening again.

Exemplar:

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.