Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
A SYN(synchronize) flood attack. This is a type of Denial of Service (DoS) attack. Access or the normal functioning of the website is hindered, using a packet sniffer I found an abnormal number of SYN requests. From log 125, we notice a continuous SYN flood request, from a particular source port “203.0.113.0”, since the attack is from one source, it is a direct DoS SYN flood attack. A DDoS (Distributed Denial of Service) attack would have the SYN requests from different locations (i.e. source port)

Section 2: Explain how the attack is causing the website to malfunction
This is a direct DoS SYN flood attack. There is an abnormal number of SYN requests even before the initial one is completed, and they seem to be from one source port (i.e. one location). There’s a three-way “handshake” before a TCP connection is established between a device and a server ● The user sends SYN (synchronized) requests to the device ● The server responds by sending SYN/ACK (synchronize acknowledge) packets to acknowledge receiving the request. This is the server agreeing to connect with the user. ● The device sends an ACK (acknowledge) packet to the server, once received a TCP connection is made. Because of the numerous SYN request from the attacker, genuine requests from the users cannot be completed hence giving the “time-out error” on the user’s browser or a “Gateway Time-out (text/html) error message”. Because of the attack, the network had to be taken down temporarily to solve the issues and this has hindered the normal running of the business. This can also result in financial loss or reputation damage to the company/business. Ways to secure the network:

- Using Next Generation Firewall (NGFW): This can be configured to detect network anomalies to ensure that oversized broadcasts are detected before they have a chance to bring down a network. This is better than just configuring the firewall to block requests from one IP address, which threat actors can easily spoof to other IP addresses. NGFW detects any network/IP addresses with an abnormal number of requests, even if the IP addresses are changed.