Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The website is showing an error of ‘connection timeout’. When the website was analyzed via packet sniffing, we observed that the website was flooded with the SYN requests from an unknown IP address. This could be a DoS attack and particularly a SYN flood attack which is coming from only one computer/IP. A DDoS is a type of attack where the request is coming from multiple computers. Since the website is flooded with huge SYN requests the website is taking longer time to respond to the requests and is getting overwhelmed so its giving a connection timeout error message

Section 2: Explain how the attack is causing the website to malfunction
The huge number of SYN requests from the unknown IP(203.0.113.0) is causing the website to delay the other requests made from the authentic users. The website is spending much of its time resolving or responding to the requests from the unknown IP thereby causing malfunction The potential consequences of this SYN flood attack can cause the business to halt thereby having a negative impact on the revenue. It stops the organizations normal operations. To prevent this type of attack in future we can use firewalls.