Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The Web server of the website has been a victim to a Denial of Service attack. The Unknown IP 203.0.113.0 seems to have flooded the server with Tremendous amount of TCP SYN requests. Hence the errors such as Gateway time out are received as the server is unable to respond to legitimate requests.

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

Initially during the time span of 3.6 seconds the server was responding properly to the SYN requests that were being sent by Legitimate employees. After the first SYN request sent by the Malicious IP i.e 203.0.223.0 the server seems to have responded to the requests with SYN-ACK. But the Malicious IP sends more and more Requests to the server eventually flooding it. After the Last successful connection that was established with the server which was at around 6.22 secs according to the TCP dump, the server seems to have stopped responding to any SYN requests.