# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| Network attacks are when a threat actor with malicious intent attempts to debilitate an organization’s network. The symptoms present from the attack such as the multiple SYN requests sent from an individual IP indicates that it is a SYN flood attack which is a type of DoS (Denial of Service) attack. The difference between a DoS and DDoS (Distributed Denial of Service) attack is that Denial of Service attack comes from one direct malicious source while the latter comes from multiple difference sources- this doesn’t only mean from multiple different computers it could mean from all devices part of the IoT. The website was taking a long time to load because the gateway server was waiting for a response from the web server and when the web server did not respond the “connection timeout error” was printed. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| In this attack, the TCP protocol was taken advantage of by exploiting the TCP handshake where the web server would first send a SYN packet request then the gateway server would respond with SYN, ACK and then the web server would then finally respond with ACK where a connection would be established. However, in this network level DoS attack, the number of SYN requests sent to the gateway server exceeded the number of available resources to answer those requests which caused the network bandwidth of the gateway server to be overwhelmed. This type of DoS attack is called a SYN flood attack. Because there were multiple SYN requests sent, the web server is getting flooded, and it is using up its network bandwidth hence slowing down the website. Then once it gets overwhelmed then the website is rendered useless and legitimate traffic is not honored. DoS attacks could cost the organization financially, cause them to lose their reputation and could also come with legal complications such as lawsuits if data was stolen. An immediate solution would be to block the malicious IP address; however, the threat actor could just spoof their IP and do it again. So, this situation would have to be escalated to the security engineers to come up with a more robust solution that could even prevent a DDoS attack. |