# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| On 06/05/23 employees began reporting issues with accessing the sales website. Employees reported receiving 504 error messages from the web server. The Wireshark packet sniffing tool was used to analyze network traffic. The data revealed an unusual number of SYN packets originating from IP address 203.0.113.0. The SYN packets originating from this address are unusual and likely malicious. The web server appears to be under an active SYN flood DoS attack. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| The connection to the webserver consists of three steps:  1) The source computer sends a SYN packet over TCP to the destination computer to request to connect.  2) The destination computer sends an SYN/ACK packet over TCP to the source computer acknowledging the request.  3) The source computer responds with an ACK packet to the destination computer and the connection is established.  The flood of SYN packets from 203.0.113.0 are overloading the webserver’s ability to respond to requests and denying service to legitimate requests. The web server is no longer responding to any requests and the gateway server is serving 504 error messages to all clients attempting to connect to the web server. Access to the sales website server is necessary for business operations. Various business units will be unable to function without the ability to access and manipulate the data on the sales website server. The network security team will contact the firewall administrator to investigate potential changes to the firewall to reject packets from 203.0.113.0 and/or reject packets consistent with a SYN flood attack. |