# Cybersecurity Incident Report

Nela-officer

Date: 02/12/2024

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| One potential explanation for the website's connection timeout error message is:  *A large number of TCP SYN requests come from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. The server is under attack by a malicious actor*.  The logs show that:   * *The attacker’s SYN request is answered normally by the web server (log items 52-54), then the attacker keeps sending more SYN requests, which is abnormal. The web server is still able to respond to normal visitor traffic.* * *An employee visitor with the IP address of 198.51.100.14 successfully completes a SYN/ACK connection handshake with the webserver (log item nos. 55, 56, 58). Then, the employee’s browser requests the sales.html webpage with the GET command and the web server responds (log item no. 60 and 62).* * *In the next 20 rows, the log begins to reflect the struggle the web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace. The attacker is sending several SYN requests every second.* * *The log includes two type of errors:*  1. *An HTTP/1.1 504 Gateway Time-out (text/html) error message. This message is generated by a gateway server that was waiting for a response from the web server. If the web server takes too long to respond, the gateway server will send a timeout error message to the requesting browser.* 2. *An [RST, ACK] packet, which would be sent to the requesting visitor if the [SYN, ACK] packet is not received by the web server. RST stands for reset, acknowledge. The visitor will receive a timeout error message in their browser and the connection attempt is dropped. The visitor can refresh their browser to attempt to send a new SYN request.*  * *The rest of the log shows the web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on,* ***the web server stops responding****.*   This event could be: *Direct DoS SYN flood attack due there is only one IP address attacking the web server.* |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:   1. *The [SYN] -synchronize- packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server.* 2. *The [SYN, ACK] -synchronize acknowledge- packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake.* 3. *The [ACK]-acknowledge- packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection.*   Explain what happens when a malicious actor sends many SYN packets all at once:  *The server will become overwhelmed and unable to respond to the requests.*  Explain what the logs indicate and how that affects the server:  *The log begins to reflect the struggle the web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace. The attacker is sending several SYN requests every second. The web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server* |