By: caami.sec

Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The DoS attack is the potential reason for the website's connection timeout error message. The logs show that the web server stops responding after being flooded with a large amount of SYN requests, which could be a type of DoS attack known as SYN flood

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. There is three steps of handshake connection: 1. The source sends a SYN request to the server; 2. The server replies to the source with a SYN-ACK packet to accept the connection. 3. Then the source replies with a final ACK packet to destination, confirming the permission to connection. When the destination, such as a server, receives an abnormal request, this system becomes overwhelming, so the response properly and it stops to work. When this happen the website, or server, or whatever was the destination, stop to work for everyone, so legitimate users/clients when try to connect will not be able to. The logs show that after several attempts, the server stopped working.