

Cybersecurity Incident Report

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: 504 Gateway Time-out

The logs show that:

HTTP/1.1 504 Gateway Time-out (text/html)

This event could be a denial of service

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 client sends the SYN to the server.
2. The server sends back the SYN-ACK
3. The client responds with ACK, and the connection establishes

Explain what happens when a malicious actor sends a large number of SYN packets all at once: If the resources of the server are less than the number of SYN packets, the servers stop responding and this happens in the network layer

Explain what the logs indicate and how that affects the server: The log indicates that this is a DOS attack because only a single computer is involved.