Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
There are attacks aimed at extorting or encrypting data, or attacks aimed at paralyzing a company's network, which consequently leads to a lack of access to resources. This is associated with potentially large financial, reputational, and trust losses. In this case, the server works slowly and eventually stops responding to requests. This fits the definition of a DoS attack. The logs showed that there was only one IP address from which large amounts of SYN packets were sent, causing the server to overload and become unable to function

Section 2: Explain how the attack is causing the website to malfunction
It was a SYN flood DoS attack. Step 1: The malicious actor began sending SYN packets to the server, which are the first step in establishing a TCP connection. Step 2: The server responds to the connection attempt by replying with a SYN-ACK packet. Step 3: The malicious actor continues to send more SYN packets, which the server cannot keep up with, slowing down its performance. Over time, the server's resources are entirely consumed by attempts to respond to the incoming SYN packets. Eventually, the resources are exhausted, and the server stops responding to requests. As a result, the company's employees and clients cannot access the important website. This leads to delays in work, chaos, and losses. Potentially, using cloud servers that can scale resources as needed and actively monitor traffic and respond to suspicious requests could prevent the lack of access to such an important resource.