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: Um crash no sistema por inúmeros pedidos Syn, Crashando o servidor. The logs show that: Um dispositivo de IP: 203.0.113.0 fez inúmeros pedidos SYN ao servidor em poucos segundos indicando ataque malicioso ao servidor This event could be: um Ataque de Rede DOS(um ataque de negação de segurança), Direcionado a crashar o servidor com inundação de informação.

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. Pedido de pacote SYN ao servidor. 2. Análise do servidor sobre o pedido do pacote. 3. Entrega do Serviço Pedido. Explain what happens when a malicious actor sends a large number of SYN packets all at once: Inundação do tráfego de rede, interrompendo operações. Explain what the logs indicate and how that affects the server: Os logs mostram os pedidos e a resposta do servidor, e mostram o que aconteceu, e quando o servidor começou a não responder pedidos normais TCP