# 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: Ataques do tipo SYN FLOOD, onde várias requisições são enviadas ao servidor e ele não consegue responder, porque ele não consegue estabelecer uma conexão com o solicitante.  The logs show that: Um grande volume de solicitações do IP 203.0.113.0  This event could be: Um Ataque DDos que visa tornar um servidor sobrecarregado com uma quantidade de pacotes que não consegue lidar. | |
|

| **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. O solicitante envia um pacote SYN   2. O Servidor responde com um pacote SYN, ACK  3. O Solicitante responde com um pacote ACK  Explain what happens when a malicious actor sends a large number of SYN packets all at once: Quando um ator malicioso envia vários pacotes SYN e não completa o ciclo do HandShake.  Explain what the logs indicate and how that affects the server: O servidor fica esperando que o ciclo se complete, mas mais pacotes SYN continuam chegando e isso sobrecarrega o servidor porque o handshake não é concluído e com isso mais recursos do servidor são consumidos. |