# Relatório de incidente de segurança cibernética

|  |
| --- |
| **Section 1: Identifique o tipo de ataque que pode ter causado essa interrupção de rede** |
| Uma possível explicação para a mensagem de erro de tempo limite de conexão do site é um ataque DoS.Os logs mostram que um número anormal de solicitações SYN chegando em um ritmo rápido, sendo solicitado pelo endeeço de ip 203.0.113.0. Fazendo o servidor web parar de responder.Este evento pode ser um ataque direto de inundação DoS SYN. |
|

|  |
| --- |
| **Section 2: Explique como o ataque está causando o mau funcionamento do site** |
| Quando os visitantes do site tentam estabelecer uma conexão com o servidor web, ocorre um handshake de três vias usando o protocolo TCP. Explique as três etapas do handshake:   1. SYN (solicitando a conexão) 2. SYN/ACK (resposta do servidor web à solicitação do visitante concordando com a conexão. O servidor reservará recursos do sistema para a etapa final do handshake) 3. ACK (confirmando a permissão de conexão)   Explique o que acontece quando um agente malicioso envia um grande número de pacotes SYN de uma só vez: Ele simula uma conexão TCP e inunda o servidor com pacotes SYN, que tem como alvo a largura de banda da rede para diminuir o tráfego. Fazendo com que o servidor web apresente falhas parando de responder os traficos legitimos  Explique o que os logs indicam e como isso afeta o servidor: o servidor web para de responder ao tráfego legítimo de visitantes de funcionários. Os visitantes recebem mais mensagens de erro indicando que não conseguem estabelecer ou manter uma conexão com o servidor web. |