# Relatório de incidente de cibersegurança

|  |
| --- |
| **Sessão 1: Identifique o tipo de ataque que pode ter causado essa interrupção na rede** |
| Um possível ataque DoS direto de SYN flood está sobrecarregando o servidor web impossibilitando acesso às páginas do site da empresa.  Os visitantes do site, incluindo funcionários, não estão conseguindo estabelecer conexão com as páginas, recebendo uma mensagem de erro de **timeout**, o que indica que o servidor gateway não obteve resposta do servidor web. Após análise do registro de log foi identificado que um único endereço de IP está inundando o servidor web com mais solicitações SYN que este pode lidar, isso explica o sobrecarregamento e a incapacidade de responder efetivamente ao servidor gateway e aos visitantes. |
|

|  |
| --- |
| **Sessão 2: Explique como o ataque está causando o mau funcionamento do site** |
| Após receber um alerta do monitoramento indicando problema no servidor web a equipe de segurança tentou acessar o site da empresa e não conseguiu, recebendo mensagem de erro de **timeout**.  Um sniffer de pacotes foi usado para capturar pacotes de dados e a análise do log mostrou que:   * Um único endereço de IP estava enviando um grande número de solicitações TCP SYN em um espaço de tempo muito curto. * As informações das solicitações de visitantes legítimos continham a mensagem de erro *HTTP/1.1 504 Gateway Time-out (text/html)* indicando que o servidor gateway não estava obtendo resposta do servidor web e pacotes [RST, ACK] pois o servidor web não estava recebendo seus pacotes [SYN, ACK] enviados.   Estes fatos justificam o sobrecarregamento do servidor web e se tornam fortes indícios de se tratar de um ataque DoS direto de SYN flood.  O servidor foi colocado offline temporariamente para que possa se recuperar e retornar as operações normais, o firewall também foi configurado bloqueando o endereço de IP que estava enviando as solicitações TCP SYN.  Por se tratar de uma empresa do segmento de venda de serviços, com foco em promoções de viagens, a suspensão de acesso ao site pode ocasionar em perda de clientes, que em muitos casos precisam deste tipo de serviço com urgência, indo buscar o serviço em outras empresas. Os funcionários por não terem acesso ao site, onde buscam as melhores ofertas para os clientes, também podem perder clientes com a inacessibilidade. |