# Relatório de Incidente de rede: DoS SYN Flood

| **Seção 1: Identifique o tipo de ataque que pode ter causado isso**  **interrupção da rede** | |
| --- | --- |
| **Uma possível explicação para a mensagem de erro de tempo limite de conexão do site é:** Ataque de Negação de Serviço (DoS) por Inundação SYN (SYN Flood).  **Os** [**registros**](https://docs.google.com/spreadsheets/d/1GUqZdYu8eg5mrm_eBspV0yfkK1Ein3q04YC6HZoOew8/edit?gid=218501934#gid=218501934) **mostram que:**   * Há um grande número de solicitações TCP SYN provenientes de um único endereço IP desconhecido ( 203.0.113.0 ) direcionadas ao servidor web (1 92.0.2.1 ). * O servidor web está sobrecarregado pelo volume do tráfego de entrada, perdendo a capacidade de responder ao número anormalmente grande de solicitações SYN. * Os logs indicam falhas de comunicação entre visitantes legítimos do site e o servidor web, com mensagens de erro como "HTTP/ . pacotes [RST, ACK] sendo enviados pelo servidor. Gateway Time-out” e pacotes [RST, ACK] sendo enviados pelo servidor.   **Este evento pode ser:** classificado como um ataque de Negação de Serviço (DoS) porque a interrupção do serviço é causada por uma única fonte (o endereço IP 203.0.113.0 ) que inunda o servidor com solicitações, esgotando seus recursos e impedindo que usuários legítimos acessem o serviço. A natureza específica do ataque, com a inundação de pacotes SYN, caracteriza-o como um ataque de inundação SYN. | |
|

| **Seção 2: Explique como o ataque está causando o mau funcionamento do site** |
| --- |
| **Quando os visitantes de um site tentam estabelecer uma conexão com o servidor web, ocorre um handshake triplo usando o protocolo TCP. Explique as três etapas do handshake:**   1. **SYN (Sincronizar):** O cliente (neste caso, o navegador de um funcionário) inicia a conexão enviando um pacote SYN para o servidor. Este pacote indica a intenção do cliente de estabelecer uma conexão e sincronizar os números de sequência. 2. **SYN-ACK (Sincronizar-Reconhecimento):** O servidor, ao receber o pacote SYN, responde com um pacote SYN-ACK. Este pacote serve a dois propósitos: reconhece o SYN do cliente e envia seu próprio número de sequência para sincronização. Ao enviar o SYN-ACK, o servidor também aloca recursos para a conexão pendente. 3. **ACK (Reconhecimento):** Finalmente, o cliente recebe o pacote SYN-ACK do servidor e responde com um pacote ACK. Este pacote reconhece o SYN-ACK do servidor, completando o handshake de três vias e estabelecendo uma conexão TCP bidirecional totalmente funcional.   **Explique o que acontece quando um agente malicioso envia um grande número de pacotes SYN de uma só vez:** Quando um agente malicioso executa um ataque de Inundação SYN, ele envia um volume massivo de pacotes SYN para o servidor, mas intencionalmente não responde com o pacote ACK final para completar o handshake. Cada pacote SYN recebido faz com que o servidor aloque recursos (como memória e entradas na tabela de conexão) para uma conexão que nunca será estabelecida. O servidor fica esperando pelo ACK final que nunca chega, mantendo essas conexões em um estado de "meia-abertura" (half-open). À medida que o número de conexões half-open aumenta, o servidor esgota rapidamente seus recursos disponíveis. Ele não consegue mais alocar novos recursos para conexões legítimas, nem processar as solicitações de usuários válidos. Isso leva à sobrecarga do servidor, tornando-o incapaz de responder a qualquer tráfego, seja ele legítimo ou malicioso  **Explique o que os logs indicam e como isso afeta o servidor:** Os logs do Wireshark ( WiresharkTCP\_HTTPlog.csv ) indicam claramente os efeitos do ataque de Inundação SYN no servidor web ( 192.0.2.1 ):     * **Inundação de SYNs:** A partir do item de log , observa-se uma frequência extremamente alta de pacotes [SYN] originados do endereço IP do atacante (2 03.0.113.0 ). Esses pacotes são enviados em rápida sucessão, sobrecarregando o servidor. * **Respostas SYN-ACK do servidor ao atacante**: Inicialmente (itens , ), o servidor tenta responder aos SYNs do atacante com pacotes [SYN, ACK] , conforme o protocolo TCP. No entanto, o atacante não envia o ACK final, deixando essas conexões em estado de meia-abertura. * **Falha nas conexões legítimas:** Conforme o ataque progride, o servidor começa a falhar em estabelecer conexões legítimas. Por exemplo, o item de log mostra um pacote [RST, ACK] enviado pelo servidor para um cliente legítimo (1 , 98.51.100.16 ), indicando que o servidor está resetando a conexão devido à sua incapacidade de gerenciá-la. Isso se repete em outros itens ( , , , , , , , , , , ). * **Erros de tempo limite:** O item de log exibe uma mensagem Gateway Time-out para uma solicitação legítima ( HTTP/1.1 504 198.51.100.5 ). Isso significa que o servidor web demorou muito para responder à solicitação, resultando em um erro de tempo limite para o usuário. Isso é um sintoma direto da sobrecarga do servidor, que não consegue processar as requisições HTTP normais. * **Inacessibilidade total:** A partir do item de log , os logs mostram que o servidor web para de responder completamente ao tráfego legítimo de funcionários. Os únicos itens registrados a partir desse ponto são os pacotes SYN do atacante, demonstrando que o servidor está completamente saturado e incapaz de processar qualquer outra solicitação. Isso confirma que o ataque de Inundação SYN conseguiu esgotar os recursos do servidor, tornando o site inacessível para os usuários legítimos. |