Relatório de Incidente de Segurança Cibernética

# Seção 1: Identificação do tipo de ataque que pode ter causado a interrupção da rede

Uma possível explicação para a mensagem de erro de tempo limite de conexão do site é que ele foi alvo de um ataque de negação de serviço (DoS), mais especificamente um ataque SYN Flood. Esse tipo de ataque sobrecarrega o servidor com múltiplas solicitações de conexão TCP não finalizadas, causando falhas no serviço.

Os registros mostram que o endereço IP malicioso 203.0.113.0 enviou diversos pacotes TCP SYN para o servidor 192.0.2.1. Inicialmente, o servidor respondeu com SYN-ACK, mas com o tempo começou a não responder às requisições legítimas, emitindo pacotes RST e erros 504 Gateway Timeout.

Esse evento pode ser caracterizado como um ataque SYN Flood, cujo objetivo é consumir os recursos do servidor e impedir o acesso de usuários legítimos ao site.

# Seção 2: Explicação de como o ataque está causando o mau funcionamento do site

Quando os visitantes tentam se conectar ao servidor web, ocorre o processo de handshake de três vias (three-way handshake) utilizando o protocolo TCP. Os três passos são:

1. O cliente envia um pacote TCP com a flag SYN ao servidor para iniciar a conexão.

2. O servidor responde com um pacote TCP contendo as flags SYN e ACK.

3. O cliente responde com um pacote TCP com a flag ACK, finalizando a conexão.

Quando um agente malicioso envia um grande número de pacotes SYN de forma contínua, o servidor aloca recursos para cada tentativa de conexão e aguarda o pacote ACK que nunca chega. Isso esgota os recursos disponíveis do servidor, impedindo novas conexões legítimas.

Os registros indicam que o servidor recebeu uma enxurrada de pacotes SYN do IP 203.0.113.0. Com o tempo, ele deixou de responder às conexões reais, retornando mensagens de erro como RST e HTTP 504 Gateway Timeout, demonstrando que estava sobrecarregado e incapaz de atender às solicitações normais dos usuários.