Relatório de Incidente de Cibersegurança

Seção 1: Identificar o tipo de ataque que pode ter causado essa interrupção na rede
Uma explicação potencial para a mensagem de erro de tempo limite de conexão do site é: O servidor foi alvo de um ataque de negação de serviço (DoS), especificamente um 'SYN Flood'. Os logs mostram que: Um único endereço IP de origem, '203.0.113.0', está enviando um volume anormal e contínuo de pacotes TCP com a flag 'SYN' para o servidor web da empresa '192.0.2.1'. This event could be: Um ataque de DoS do tipo SYN Flood.

Seção 2: Explicar 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 three-way handshake usando o protocolo TCP. Explique as três etapas do handshake: 1. SYN: O cliente envia um pacote 'SYN' para o servidor para iniciar uma conexão. 2. SYN, ACK: O servidor responde com um pacote 'SYN, ACK', confirmando o recebimento da solicitação e alocando recursos para a nova conexão. 3. ACK: O cliente finaliza o processo enviando um pacote 'ACK' de volta ao servidor, estabelecendo assim a conexão. Explique o que acontece quando um ator malicioso envia um grande número de pacotes SYN de uma só vez: O ataque força o servidor a manter muitas conexões semiabertas (half-open), o que esgota seus recursos de sistema. Uma vez que seus recursos se esgotam, o servidor fica sobrecarregado e se torna incapaz de responder a novas solicitações de usuários legítimos, causando uma negação de serviço (DoS). Explique o que os logs indicam e como isso afeta o servidor: Os logs mostram que o endereço IP de um único atacante '203.0.113.0' está enviando continuamente pacotes 'SYN' para o servidor web da empresa. Essa inundação de solicitações sobrecarrega o servidor, que começa a ter dificuldades para lidar com o tráfego. Como resultado, o serviço é negado aos usuários legítimos.