Relatório de incidente de segurança

Seção 1: Identifique o tipo de ataque que pode ter causado a interrupção da rede
À tarde, a equipe de segurança recebeu um alerta automatizado do nosso sistema de monitoramento indicando um problema no servidor web. Após ser designado para tratar do caso, eu tentei acessar o site da empresa mas recebi uma mensagem de “connection timeout error” no navegador. Logo, prossegui a investigar o incidente utilizando uma ferramenta de análise de tráfego de rede, wireshark, que mostrou um grande número de requisições SYN vindo de um endereço IP estranho. As requisições SYN fazem parte do processo de “handshake” do protocolo da camada de transporte, TCP e um grande número de requisições pode acabar sobrecarregando os recursos do servidor. Esse tipo de evento é caracterizado como “SYN flood attack” um tipo de ataque de negação de serviço (DoS).

Seção 2: Explique como o ataque está causando o comportamento anômalo no site
Quando os usuários tentam estabelecer uma conexão com o servidor web, um processo de três passos chamado de “handshake” ocorre usando o protocolo TCP. O primeiro passo se dá quando o cliente ao tentar acessar o site, envia uma requisição SYN para estabelecer uma conexão com o servidor web. Ao receber a requisição, o servidor responde com a mensagem SYN/ACK, reconhecendo a conexão e separando recursos para ela. E por fim, o cliente manda uma requisição ACK finalizando o processo e podendo a partir de agora fazer outras requisições. Quando um agente de ameaças envia um grande número de pacotes SYN ao mesmo tempo, o servidor web pode ficar sobrecarregado e apresentar problemas. A partir da análise dos registros de tráfego da rede, é mostrado o indício claro de “SYN flood attack” um tipo de ataque de negação de serviço (DoS), oriundo de um IP estranho que causou o mau funcionamento do servidor.