Relatório de Incidente de Segurança Cibernética: Análise de Tráfego de Rede

Parte 1: Forneça um resumo do problema encontrado no log de tráfego DNS e ICMP.
O protocolo UDP revela que: A mensagem UDP solicitando um endereço IP para o domínio 'www.yummyrecipesforme.com' não chegou ao servidor DNS porque nenhum serviço estava escutando na porta DNS receptora. Isso se baseia nos resultados da análise de rede, que mostram que a resposta de echo ICMP retornou a mensagem de erro: Porta UDP 53 inacessível. A porta indicada na mensagem de erro é usada para: A porta 53 é a porta para o serviço DNS. O problema mais provável é: O servidor estava fora do ar.

Parte 2: Explique sua análise dos dados e forneça pelo menos uma causa para o incidente.
Horário em que o incidente ocorreu: 13:24. Explique como a equipe de TI tomou conhecimento do incidente: Vários clientes relataram que não conseguiam acessar o site da empresa cliente 'www.yummyrecipesforme.com' e viram o erro 'destination port unreachable' após esperarem o carregamento da página. Explique as ações tomadas pelo departamento de TI para investigar o incidente: Um analista de segurança cibernética primeiro confirmou o problema e depois usou a ferramenta de análise de rede 'tcpdump' para capturar e analisar o tráfego de rede durante outra tentativa de carregar a página da web. Aponte as principais descobertas da investigação do departamento de TI (ou seja, detalhes relacionados à porta afetada, servidor DNS, etc.): A análise dos pacotes capturados mostrou que as consultas DNS enviadas via UDP do IP de origem '192.51.100.15' para o servidor DNS em '203.0.113.2' estavam falhando. O servidor respondeu com uma mensagem de erro ICMP indicando que a porta UDP 53 estava inacessível.

Aponte uma causa provável do incidente: Uma causa provável do incidente pode ser devido a um Ataque DDoS ao Servidor.