Relatório de Incidente de rede:
Análise de tráfego de rede

Parte 1: Forneça um resumo do problema encontrado no DNS e no ICMP registro de tráfego.
O protocolo UDP revela que: O computador cliente (192.51.100.15) está tentando resolver o nome de domínio yummyrecipesforme.com através de uma consulta DNS enviada para o servidor DNS (203.0.113.2) na porta . Essa consulta é encapsulada em um pacote UDP **Isso se baseia nos resultados da análise de rede, que mostram que a resposta de eco do ICMP retornou a mensagem de erro:** "udp port 53 unreachable". Esta mensagem é enviada do servidor DNS (203.0.113.2) de volta para o computador cliente (192.51.100.15), indicando que a porta UDP 53 no servidor DNS não está acessível ou não há um serviço escutando nela. **A porta indicada na mensagem de erro é usada para:** O serviço DNS (Domain Name System), que é responsável por traduzir nomes de domínio em endereços IP. A porta 53 é a porta padrão para o tráfego DNS. **O problema mais provável é:** Que o servidor DNS (203.0.113.2) não está respondendo às consultas DNS na porta 53, ou que um firewall está bloqueando o tráfego para essa porta, ou que o serviço DNS não está em execução no servidor. Isso impede que o computador cliente obtenha o endereço IP para *yummyrecipesforme.com*, resultando na falha de acesso ao site.

Parte 2: Explique sua análise dos dados e forneça pelo menos uma causa do incidente.

Horário em que o incidente ocorreu: Os registros do tcpdump mostram que o incidente ocorreu em várias ocasiões, começando por volta das 13:24:32.192571, seguido por 13:26:32.192571 e 13:28:32.192571.

Explique como a equipe de TI tomou conhecimento do incidente: Vários clientes relataram que não conseguiam acessar o site www.yummyrecipesforme.com e viam o erro "porta de destino inalcançável". O analista de segurança cibernética também tentou acessar o site e recebeu o mesmo erro.

Explique as ações tomadas pelo departamento de TI para investigar o incidente: O analista de segurança cibernética utilizou a ferramenta tcpdump para capturar o tráfego de rede ao tentar acessar o site novamente. A análise do tcpdump revelou que, ao enviar pacotes UDP para o servidor DNS, eram recebidos pacotes ICMP com a mensagem de erro "porta udp 53 inacessível".

Observe as principais descobertas da investigação do departamento de TI (por exemplo, detalhes relacionados à porta afetada, servidor DNS, etc.): O tráfego DNS (protocolo UDP na porta 53) do cliente (192.51.100.15) para o servidor DNS (203.0.113.2) está falhando. - O servidor DNS (203.0.113.2) está respondendo com mensagens de erro ICMP "udp port 53 unreachable" de volta para o cliente. - Isso indica que o serviço DNS na porta 53 do servidor 203.0.113.2 não está respondendo ou está inacessível.

Observe uma causa provável do incidente: A causa provável do incidente é que o serviço DNS no servidor 203.0.113.2 não está em execução. O servidor DNS pode estar inativo devido a um ataque de negação de serviço bem-sucedido, ou está configurado incorretamente, ou há um firewall bloqueando o tráfego UDP na porta 53 para este servidor. Isso impede a resolução de nomes de domínio, resultando na incapacidade de acessar o site yummyrecipesforme.com.