# Relatório de incidente de segurança cibernética: análise de tráfego de rede

|  |
| --- |
| Part 1: Forneça um resumo do problema encontrado no log de tráfego DNS e ICMP. |
| Os logs de análise de rede indicam que foram detectadas várias tentativas de conexão com o servidor DNS através de requisições UDP que não obtiveram resposta, sugerindo uma possível sobrecarga ou falha no servidor DNS. A análise do tráfego ICMP revelou uma mensagem de erro "udp port 53 unreachable" (porta UDP 53 inacessível), indicando que nenhum serviço estava detectando a porta DNS receptora. A porta mencionada, UDP 53, é comumente usada para consultas de DNS. O problema mais provável é uma interrupção no serviço de DNS, possivelmente causada por um ataque DDoS direcionado ao servidor DNS. |
|

|  |
| --- |
| Part 2: Explique sua análise dos dados e forneça pelo menos uma causa do incidente. |
| O incidente foi registrado às 13:24, quando vários clientes relataram dificuldades ao acessar o site da empresa [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com), recebendo a mensagem "porta de destino inalcançável" após tentativas de carregamento da página. A equipe de TI foi informada do problema e iniciou uma investigação utilizando a ferramenta de análise de rede tcpdump para capturar e examinar o tráfego DNS e ICMP. A investigação revelou uma série de requisições UDP para a porta 53 que não receberam resposta do servidor DNS, além de múltiplas respostas ICMP de "Destino Inacessível." Identificou-se que a porta UDP 53 do servidor DNS estava sobrecarregada com tráfego excessivo, o que impedia respostas normais. A causa provável do incidente foi uma sobrecarga no servidor DNS, possivelmente devido a um ataque DDoS. |