# Relatório de Incidente de Cibersegurança:

## 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:

As consultas DNS enviadas do IP 192.51.100.15 ao servidor DNS 203.0.113.2 na porta UDP 53 não obtiveram resposta válida. Em vez disso, o cliente recebeu mensagens ICMP informando que a porta de destino está inacessível. Isso indica que o servidor DNS não estava ouvindo ou não estava disponível na porta padrão para consultas DNS (porta 53/UDP).

Isso é baseado nos resultados da análise de rede, que mostram que a resposta ICMP retornou a seguinte mensagem de erro:

"udp port 53 unreachable"

A porta mencionada na mensagem de erro é usada para:

Serviço DNS (Domain Name System) — protocolo UDP, porta 53.

O problema mais provável é:

O servidor DNS no IP 203.0.113.2 está inativo, mal configurado, sobrecarregado ou bloqueado. Isso impede que os clientes resolvam nomes de domínio e acessem sites, como www.yummyrecipesforme.com.

### Parte 2: Explique sua análise dos dados e forneça ao menos uma causa para o incidente

Hora em que o incidente ocorreu:

O incidente foi registrado por volta das 13:24:32, conforme os carimbos de data/hora nos pacotes analisados.

Explique como a equipe de T.I. tomou conhecimento do incidente:

Diversos clientes relataram problemas ao tentar acessar o site da empresa, recebendo mensagens como "porta de destino inacessível". Após testes internos, a equipe técnica confirmou o problema.

Explique as ações tomadas pelo departamento de T.I. para investigar o incidente:

Foi utilizada a ferramenta tcpdump para capturar e analisar o tráfego de rede durante uma tentativa de acesso. A análise mostrou que os pacotes UDP enviados ao servidor DNS não estavam sendo respondidos e estavam retornando mensagens ICMP de erro.

Registre os principais achados da investigação do departamento de T.I.:

- O IP do servidor DNS é 203.0.113.2.  
- Todas as tentativas de resolução DNS usando esse servidor falharam.  
- As mensagens de erro retornadas foram "udp port 53 unreachable".  
- O domínio consultado foi yummyrecipesforme.com.  
- Nenhuma resposta DNS foi recebida durante o teste.

Registre uma possível causa do incidente:

O serviço DNS no servidor 203.0.113.2 pode estar fora do ar por falha técnica, manutenção não programada, má configuração ou — potencialmente — devido a um ataque de negação de serviço (DoS), que sobrecarregou o servidor e tornou a porta 53 inacessível. Esse tipo de ataque pode esgotar os recursos do servidor, impedindo respostas válidas a consultas legítimas.