English:
Cybersecurity Incident Report:
Network Traffic Analysis

Server was not correctly directed to the host.
The UDP protocol reports that the DNS was not found. With the analysis obtained from the network, it shows that ICMP returned the error message (udp port 53 unreachable / udp port 54 unreachable) The problem could probably have been an ICMP flood attack.

Analyzing the information acquired, I inform you that:
What happened during the afternoon, when the team reported that they were experiencing incidents of slow access to the service, when we investigated what could have happened, using the “tcpdump” platform we realized that a route problem was occurring, where port 53 was inaccessible, meaning that the DNS port and underlying network transport were not being routed correctly, in the case of the website “www.ymmyrecipesforme.com” Our next strategy was to analyze the network and mainly its security and stability, checking the firewall and the HTTP network port (port 443). Analyzing the general context, we believe that there has been an ICMP flood attack, we will investigate further and take appropriate measures to overcome the vulnerabilities in data traffic on the websites.

Português:
Relatório de incidente de segurança cibernética:
Análise de tráfego de rede

Servidor não foi corretamente direcionado ao host.
O protocolo de UDP informa que o DNS não foi encontrado. Com a análise obtida pela rede, mostra que o ICMP retornou a mensagem de erro (udp port 53 unreachable / porta udp 54 inacessível) O problema provavelmente pode ter sido um ICMP flood attack.

Analisando as informações adquiridas, informo que:
O incidente aconteceu durante a tarde, quando a equipe informou que estava enfrentando lentidão em acessos ao serviço, quando fomos investigar o que poderia ter acontecido, utilizando a plataforma “tcpdump” percebemos que estava ocorrendo um problema de rota, onde a porta 53 estava inacessível, fazendo com que a porta DNS e o transporte subjacentes da rede não estava sendo encaminhado da forma correta, no caso o site “www.ymmyrecipesforme.com” Nossa próxima estratégia foi analisar a rede e principalmente sua segurança e estabilidade, verificamos o firewall e a porta de rede HTTP (porta 443). Analisando o contexto geral, acreditamos que tenha sido um ataque de flood ICMP, iremos investigar mais e tomar medidas cabíveis para contornar as vulnerabilidades no tráfego de dados nos sites.