Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
Clientes relataram que, ao tentar acessar o site "www.yummyrecipesforme.com", recebiam como retorno apenas a mensagem de erro "destination port unreachable". Uma análise pelo tcpdump indicou que a mensagem, um ICMP echo reply, vinha após uma tentativa de consulta à porta 53, associada ao servidor DNS, após a requisição do endereço IP referente ao site. Isso indica que pode haver um problema com o servidor DNS, como um erro de configuração ou um ataque DoS.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
O incidente ocorreu hoje às 13h24. A equipe de TI soube do incidente por relato de clientes que tentaram acessar o site e receberam a mensagem de erro "destination port unreachable". Para analisar a situação, foi utilizado o tcpdump para fazer tentativas de acesso ao site e investigar o tráfego durante a requisição. Foi descoberto que a porta associada ao DNS em seu servidor não está recebendo a requisição, podendo ser por um erro de configuração, como um firewall interno ou a porta trocada durante alguma manutenção, ou o não funcionamento do serviço, que pode ter sido desligado ou ter sofrido um ataque. Os próximos passos para a resolução desse problema envolvem a verificação de logs do servidor DNS para entender o que aconteceu no período em que o serviço parou de funcionar ou eventos anteriores que podem tê-lo afetado.