Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: permintaan keluar awal dari komputer Anda ke server DNS yang meminta alamat IP yummyrecipesforme.com This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 tidak dapat dijangkau The port noted in the error message is used for: DNS The most likely issue is:pesan UDP yang meminta alamat IP untuk domain "www.yummyrecipesforme.com" tidak diteruskan ke server DNS karena tidak ada layanan yang mendengarkan pada port DNS penerima

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 13:24:32.192571 Explain how the IT team became aware of the incident: aware of dns server Explain the actions taken by the IT department to investigate the incident: check dns server Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): dns server Note a likely cause of the incident: dns server