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: The network protocol analyzer logs indicate that port 443 is unreachable when attempting to access the secure employee background check website.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: This may indicate a problem with the web server or the firewall configuration.

The port noted in the error message is used for: Port 53 is normally used for DNS (domain name system) traffic.

The most likely issue is: It is possible that this is an indication of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred: The incident occurred today at 1:24p.m.

Explain how the IT team became aware of the incident: Customers notified the organization that they received the message “destination port unreachable” when they try to visit the website yummyrecipesforme.com.

Explain the actions taken by the IT department to investigate the incident: The network security team responded and are currently running tests with the network protocol analyzer tool tcpdump to make sure the website is accessible again.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The resulting logs revealed that port 443, which is used for HTTPS traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. Our next steps include checking the firewall configuration to see if port 443 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack.

Note a likely cause of the incident: DNS server might be down due to a successful Denial of Service attack or a misconfiguration.