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 53 is unreachable when attempting to access the secure employee background check website. Port 53 is the default port for DNS.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “udp port 53 unreachable”.

The port noted in the error message is used for: Port 53 is normally used for DNS protocol traffic.

The most likely issue is: It is highly likely that the DNS server is not responding.

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

Time incident occurred: 1.24pm

Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

Explain the actions taken by the IT department to investigate the incident: In order to troubleshoot the issue, the IT department loads network analyser tool, tcpdump to conduct packet sniffing tests.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): In the resulting network log files, we received ICMP packets that contain the error message: “udp port 53 unreachable”

Note a likely cause of the incident: Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. DNS server may be down due to successful Denial of Service(DoS) attack or a misconfiguration of firewall.