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: DNS queries typically use UDP on port 53. The blockage prevented successful name resolution. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: Additionally, the ICMP traffic log showed that ICMP echo replies returned an error message indicating that the destination port was unreachable. This confirms that the DNS server was not responding to requests, likely due to port-level filtering or misconfiguration. The port noted in the error message is used for: DNS (UDP port 53), ICMP The most likely issue is: DNS resolution failure due to blocked UDP traffic. • Secondary Impact: HTTP requests failed because domain names could not be resolved to IP addresses.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 13:24:32.192571 pm Explain how the IT team became aware of the incident: The IT team was alerted through user complaints and automated monitoring systems that flagged repeated HTTP request failures and DNS timeouts. Explain the actions taken by the IT department to investigate the incident: The IT department initiated a network traffic analysis using packet inspection tools. They reviewed DNS and ICMP logs to trace the source of the failure. ICMP echo replies indicated that port 53 was unreachable, and DNS queries over UDP were consistently dropped.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
• DNS queries sent via UDP to port 53 failed to reach the DNS server.
• ICMP responses confirmed that the destination port was blocked or filtered.
• HTTP requests failed due to unresolved domain names, confirming a DNS resolution issue.
• No anomalies were found in the DNS server configuration, suggesting a network-level blockage.

Note a likely cause of the incident: The most probable cause was a firewall or network policy blocking UDP traffic on port 53, which disrupted DNS resolution and caused cascading failures in HTTP-based services.