Cybersecurity Incident Report by Jovworie Tanshi: 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 client computer (IP: 192.51.100.15) sent multiple DNS queries using the UDP protocol to the DNS server (IP: 203.0.113.2) requesting the IP address of the domain `yummyrecipesforme.com`. **This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:** The ICMP error message indicated "udp port 53 unreachable." This means the DNS server could not process the UDP packets because there was no service listening on port 53. **The port noted in the error message is used for:** Port 53 is used for DNS (Domain Name System) services. DNS translates domain names to IP addresses, allowing browsers to load internet resources. **The most likely issue is:** The DNS service on the server (IP: 203.0.113.2) was either down, misconfigured, or blocked by a firewall or network policy, preventing it from listening on port 53 and thereby causing the "unreachable" error messages.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occurred at approximately 1:24 p.m. (timestamp: 13:24:32.192571). **Explain how the IT team became aware of the incident:** The IT team became aware of the incident through automated monitoring tools that flagged repeated ICMP error messages indicating DNS service unavailability. Additionally, end-users reported issues with domain name resolution when attempting to access websites. **Explain the actions taken by the IT department to investigate the incident:** **Log Analysis:** The IT team analyzed tcpdump logs to identify the pattern of DNS requests and ICMP error responses. **Service Check:** The team verified the status of the DNS service on the server (IP:

203.0.113.2).
Network Configuration Review: They examined firewall rules, network policies, and recent configuration changes that could impact DNS traffic.
Redundancy Verification: Checked the availability and performance of redundant DNS servers to ensure they were functioning correctly.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
Affected Port: The incident specifically involved UDP traffic on port 53, which is used for DNS services.
DNS Server Unavailability: The DNS server at IP address 203.0.113.2 was not responding to DNS queries due to the service not being reachable on port 53.
ICMP Error Messages: The server returned ICMP error messages indicating "udp port 53 unreachable," confirming the DNS service was either down or inaccessible.
Multiple Attempts: The logs showed multiple attempts by the client to resolve the domain, all resulting in the same error

Note a likely cause of the incident:
The most likely cause of the incident was that the DNS service on the server (IP: 203.0.113.2) was either:

Service Outage: The DNS service may have been stopped or crashed, preventing it from listening on port 53.
Misconfiguration: Incorrect DNS server configuration could have resulted in the service not being bound to port 53.
Network Blockage: Firewall rules or network policies may have blocked UDP traffic on port 53, causing the server to be unreachable for DNS requests.