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 **UDP protocol** reveals that DNS queries were sent from **192.51.100.15** to the DNS server **203.0.113.2** on **port 53**. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The **ICMP echo reply** returned the error message: **"udp port 53 unreachable"**, indicating that the request could not reach the intended DNS service. The port noted in the error message is used for: **Port 53** is primarily used for **DNS resolution**—it allows clients to query a DNS server for domain name translations to IP addresses. The most likely issue is: The DNS server at **203.0.113.2** is either **down, misconfigured, or blocked by firewall rules**, preventing it from responding to DNS queries.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The issue was observed starting at **13:24:32**, with repeated failed DNS queries at **13:26:32** and **13:28:32**. Explain how the IT team became aware of the incident: - Several **customers reported** they were unable to access the website **www.yummyrecipesforme.com**. - Users saw the error message **"destination port unreachable"** when trying to load the page. - The IT team **reproduced the issue** and confirmed DNS resolution failures. Explain the actions taken by the IT department to investigate the incident: 1. Attempted to **access the website manually**—confirmed failure. 2. Used **tcpdump** to **capture network traffic** and observed **DNS query failures**. 3. Analyzed the logs and found repeated **ICMP "port unreachable" errors** from the DNS server. 4. Verified that other network services were functioning properly. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): - The **DNS queries sent via UDP (port 53) to 203.0.113.2 failed**. - The **ICMP response from the DNS server confirmed** that port 53 was not accessible. - The **website itself might be operational**, but users cannot resolve the domain name due to DNS failures. Note a likely cause of the incident: - The **DNS server (203.0.113.2) may be offline or experiencing a configuration issue**. - A **firewall rule or security setting** could be **blocking** incoming DNS queries. - A **DDoS attack** might have overwhelmed the DNS server, causing it to **stop responding**. - The **server software handling DNS requests** could have **crashed or been disabled**.

Next Steps for Resolution

- Check the **status of the DNS server** at **203.0.113.2**.
- Investigate **firewall rules** or **network configurations** that may be blocking UDP port 53.
- If a **DDoS attack is suspected**, implement **rate limiting** and **firewall filtering**.
- Restart or **reconfigure the DNS service** on the affected server.