Cybersecurity Incident Report:
Network Traffic Analysis

Scenario:
You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. 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.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage. The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Part 1: Provide a summary of the problem found in the tcpdump log.

As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address for the domain name of yummyrecipesforme.com. The ICMP protocol was used to respond with an error message, indicating issues contacting the DNS server. The UDP message going from your browser to the DNS server is shown in the first two lines of every log event. The ICMP error response from the DNS server to your browser is displayed in the third and fourth lines of every log event with the error message, "udp port 53 unreachable."

Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the "A?" symbol indicates flags with performing DNS protocol operations.

Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval.

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

The incident occurred today at 1:24 p.m. Customers notified the organization that they received the message "destination port unreachable" when they attempted to visit the website yummyrecipesforme.com. The cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump.

In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whether the DNS server is down or if traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.

Part 3: Provide actionable recommendations for how to follow up with this event.

To resolve the DNS server unresponsiveness and prevent future incidents, the following steps should be taken:

1. **Verify DNS Server Status:**
   Use tools like **ping** to check server availability and **dig** or **nslookup** to test DNS resolution. If the server is unresponsive, escalate to the infrastructure team to investigate potential outages or hardware failures.

2. **Inspect Firewall Rules:**
   Review firewall logs for any blocked traffic to UDP port 53. Misconfigured rules or overly restrictive policies may be inadvertently preventing legitimate DNS queries. Temporarily whitelisting the DNS server's IP for testing may help isolate the issue.

3. **Audit DNS Server Configuration:**
   Check for recent changes to DNS settings (e.g., zone files, forwarders) or software updates that could disrupt service. Compare configurations against a known-good baseline or backup.

4. **Monitor for DoS Activity:**
   Analyze network traffic for unusual spikes or patterns indicative of a Denial-of-Service attack. If detected, implement rate-limiting or leverage DDoS mitigation services.