Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

Based on the tcpdump log data, an issue was found with the DNS server, where the destination server could not be reached on port 53 (not port 43). This caused the domain name resolution process to fail, making it likely that the user could not access the requested website, `yummyrecipesforme.com`.

The issue becomes clearer with the presence of an ICMP message: **"udp port 53 unreachable"** from the DNS server (`203.0.113.2`), indicating that no active service was available on that port to handle the DNS request. The **"A?"** signifies that the client was making a DNS request for an A record (IPv4 address), and **"35084+"** indicates DNS flags included in the packet.

In other words, the DNS request using the **UDP protocol** from the client to the DNS server failed because the server did not respond or the DNS service was unavailable—clearly indicated by the ICMP error response. As a result, the process of retrieving the IP address from the domain name was unsuccessful.

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

Based on the tcpdump log, the issue began at timestamp **13:24:32**, when the client attempted to access the domain **yummyrecipesforme.com**. The request was sent using the **UDP protocol** to the DNS server at IP address **203.0.113.2**, targeting **port 53**, which is the standard port for DNS queries.

However, the client did not receive a valid DNS response. Instead, an **ICMP error message** was returned indicating **"udp port 53 unreachable"**, which means the DNS request could not be delivered—most likely because there was

By I Wayan Okta Arianta

no DNS service actively listening on that port.

This incident suggests that the DNS server was **unavailable** at the time of the request. Possible causes of this issue include:

- The DNS server was **down or offline** (e.g., due to a system crash or power failure).
- **Firewall rules** were blocking access to port 53, either inbound or outbound.
- The DNS server was **misconfigured**, so it was not properly responding to queries.
- The DNS server may have been the target of a **Denial-of-Service (DoS or DDoS) attack**, which overwhelmed the server and made it unresponsive.

As a result, the client was unable to resolve the domain name, which prevented access to the requested website.

By I Wayan Okta Arianta