Cybersecurity Incident Report(1): Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals: The network capture shows that the computer sent a DNS query using the UDP protocol to port 53 on the DNS server 203.0.113.2, attempting to resolve the domain name www.yummyrecipesforme.com into an IP address. **This is based on the results of the network analysis:** an ICMP "Destination Unreachable Port 53 Unreachable" message was returned. This indicates that the server could not receive or process the request because no service was listening on that port. As a result, the IP address for this webpage could not be retrieved, and the computer was unable to complete the DNS resolution.. **The port noted in the error message is used for**: DNS services-port 53 is the standard port used for domain name resolution. **The most likely issue is that** the DNS server is either not configured correctly or not running the DNS service on port 53, which prevents it from responding to the request and causes the DNS lookup to fail.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 13:24:32 (1:24 PM and 32 seconds) **Explain how the IT team became aware of the incident:** The IT team noticed a failed DNS lookup in the network logs and captured an ICM error message when the user reported that the website was not loading. **Explain the actions taken by the IT department to investigate the incident:** The IT department used a network analyzer tool called tcpdump to trace the DNS request traffic, reviewed the outgoing DNS query, and the returning ICMP error messages that showed the server was not responding as expected. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

- The DNS request was sent from the local computer to the DNS server at IP 203.0.113.2.
- The request used the UDP protocol on port 53, which is the standard port for DNS lookups.
- The DNS server responded with an ICMP error, which means the server was not accepting traffic on port 53.
- This prevented the system from resolving the domain name into an IP address.

Note a likely cause of the incident:
I think the most likely cause was that the DNS server was either misconfigured, offline, or the DNS service on port 53 was off and not running, making it impossible for the DNS request to be processed.

A few suggestions I can make are:
- If the service has been unresponsive, restart it.
- If restarting the service does not help, reboot the DNS server
- Set up monitoring tools or alerts to check the status of the DNS server and the availability of port 53, ensuring that an immediate notification is sent to the IT department if the service goes down again.
- Update the system or network settings.

Finally, document the issue, investigate, take notes on the steps and solution, and share this with the team so they can use it for training and future prevention.

Tool name: tcpdump

```
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
```