Cybersecurity Incident Report: Network Traffic Analysis

TCP Dump Reading

```
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 DNS and ICMP traffic log.
The UDP protocol reveals that: The request for DNS resolution to DNS servers is not responded by DNS server therefore there have to be some problems with DNS service running in the server This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 unreachable The port noted in the error message is used for: DNS service The most likely issue is: Either DNS service is not running at all or it is running but listening in different port (non standard port)

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at around 13.24 local time. The IT team became aware of this situation because several customers reported that they could not open the company website and receive “destination port unreachable” while waiting for the page to be loaded. IT team try to investigate the situation by running our traffic analyzer tool (tcpdump) and got several key findings : ● Request from test server to DNS server was replied with error message that udp port unreachable ● The information from tools also mention that the port affected is port 53 which is standard port where DNS service running ● The situation still persist even when IT team has run the tools for some time The cause of incident is likely due ; ● There are firewall blocking the request to mentioned port 53, or ● The DNS service is not listening at standard port 53, or ● The DNS service is not running at all