Cybersecurity Incident Report: Network Traffic Analysis

Summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer reveals that UDP port 53 is unreachable when trying to connect to the domain: “yummyrecipesforme.com”. 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”. port 53 is used for DNS to resolve domain names to IP addresses. The most likely issue is either the firewall is blocking the replies, the DNS server is offline, overwhelmed or possibly even unresponsive due to a DoS attack.

Analysis of the data and possible causes of the incident.
The time incident occurred was at 1:24 PM but it happened before this time as the customers complained beforehand. Several customers 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. The IT team attempted to visit the website in question “www.yummyrecipesforme.com” but was met with a “destination port unreachable” error message, to troubleshoot the incident, the IT team opened tcpdump network analyzer and loaded the webpage again, the browser sent a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name, the browser then used this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer showed that when we sent UDP packets to the DNS server, we received ICMP packets containing the error message: “udp port 53 unreachable.” Key findings of the IT department's investigation: port 53 was unreachable when attempting to send domain name resolutions to 203.0.113.2.domain over the UDP protocol. Possible causes of the incident: - A successful DoS attack - Misconfigured DNS server - Overwhelmed DNS server - Firewall blockage

The tcpdump log is provided in the next page.

```
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
```