Cybersecurity Incident Report: Network Traffic Analysis

Provide a summary of the problem
ICMP error message is reading “UDP port 53 unreachable” which means the UDP protocol was used to request a domain name resolution usually this goes through port 53, however, the message did not go through to the DNS server and the IP address couldn’t be obtained.

Analysis
Reports were coming in stating that the website was returning the message “Destination Port Unreachable” when trying to log in. The traffic logs were reviewed and it was narrowed down to have started around 13:24. It seems that traffic to port 53 is not going through and the DNS server is not functioning properly. This could be due to a Denial of Service attack which would be flooding information to a server in order to make it crash and unreachable. Additionally, the firewall should first be reviewed to ensure that there are no parameters that were accidentally set to block port 53.

The following are the traffic logs that were reviewed:

```
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
```