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 DNS and ICMP traffic log, the analysis indicates that the UDP protocol reveals the DNS server's unavailability or inaccessibility. This is evident from the ICMP echo reply that returned the error message "udp port 53 unreachable." Since Port 53 is commonly associated with DNS protocol traffic, it strongly suggests that the DNS server is not responding.

Part 2: Explain your analysis of the data and provide one solution to implement.
Today at 1:23 p.m., customers contacted our organization to report receiving a "destination port unreachable" message when attempting to access the website. As a result, our network security professionals promptly initiated an investigation to resolve the issue and restore customer access to the website. During our investigation, we conducted packet sniffing tests using tcpdump. The resulting log file indicated that DNS port 53 was unreachable. The next crucial step is to determine the cause of the unreachability: whether the DNS server is down or if traffic to port 53 is being blocked by the firewall. There are two possible reasons for the DNS server unavailability – it might have been affected by a successful Denial of Service (DoS) attack or there could be a misconfiguration issue. To address the problem, our proposed solution is to first verify the operational status of the DNS server. This can be done by checking its connectivity and responsiveness. Additionally, we need to investigate whether the firewall is blocking traffic to port 53 and ensure the necessary rules are in place to allow DNS traffic. By addressing these aspects, we can resolve the issue and restore proper DNS functionality, thereby enabling customers to access the website again.

DNS & ICMP traffic logs:

```
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
```