Incident Report: Network Traffic Analysis

```
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

At 13:24:32.192571, when attempting to visit the webpage “yummyrecipesforme.com”, an ICMP with the error delivery “destination port unreachable.” Upon running packets through the UDP protocol, it is determined the issue is at UDP port 53.
192.51.100.15.52444 > 203.0.113.2.domain

Part 2: Explain your analysis of the data and provide one solution to implement

Since port 53 is known to be associated with DNS, the message indicates there is an issue requesting the correct IP address associated with the webpage. The problem has been reported to our supervisors who are handling the issue with DNS. One solution to prevent this brute force attack in the future would be to require all employees and admins to have 2FA set up for each account. This will prevent malicious access even when a password is compromised by sending a notification to the account holder.