Several customers contacted company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

TCPDUMP log:

```
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
```

Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: ICMP data packets are not going through to the DNS server as port 53 is unreachable The port (port 53) which is being highlighted in this whole case is used for DNS(Domain

Name System) for communication using UDP port. There can be multiple issues which may be causing the error. The error most likely would be the DNS server must be down or there must be some firewall configuration errors. It can also indicate that a malicious activity such as spoofing or phishing is being performed by threat actors.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

August 18 2023 the incident was reported by a lot of customers that the website was not responding. Destination port is unreachable is the error being faced by the user. On close inspection using a network analyzer tool it was observed that UDP port 53 is causing the error. ICMP packets were sent to check the network from the IP address 192.51.100.2 to domain 203.0.113.2 and an ICMP error was received which said UDP port 53 is unreachable.
This most likely indicated that the dns server is affected and issues need to be resolved. UDP 53 port is usually used to query and send information to a DNS server if it says that the destination port is unreachable, which means the socket closes before it even gets a response. Which means the DNS server is taking too long to respond. Most likely cause of this could be DNS server is currently busy/ Down some firewall configuration needs to be done to allow Communications port 53 may be denied thats why users cannot connect to the website or some type of malicious activity may be performed such as spoofing by threat actors.: