# 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: port 53 is unreachable  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: the ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server.  The port noted in the error message is used for: DNS client applications use the DNS protocol to query and request information from DNS servers, and the server returns the results to the client using the same port.  The most likely issue is: the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 13:24:32  Explain how the IT team became aware of the incident: Several customers of clients 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.  Explain the actions taken by the IT department to investigate the incident: used network analyzer tool, tcpdump, and attempt to load the webpage again  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): the query identification number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address. The third line displays the protocol of the response message to the browser: "ICMP," which is followed by an ICMP error message.  Note a likely cause of the incident: **DDoS attacks** can be targeted towards UDP port 53 to exhaust the DNS server resources and cause downtime. |