# 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: the UDP message requesting an IP address for the domain [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) did not go through to the DNS server because no service was listening on the receiving DNS port  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 unreachable  The port noted in the error message is used for: Port 53 is port for DNS service  The most likely issue is: the DNS server was down |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  13:24  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](http://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:  The IT department first attempted to visit the website and received the error “destination port unreachable”. To troubleshoot the issue, they used the network analyzer tool, tcpdump and attempted to load the website again. The browser sends a query to a DNS service via UDP protocol to retrieve the IP address for the website’s domain name. The browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage. The analyzer shows that when you send the UDP packets to the DNS server, you receive ICMP packets containing the error message “udp port 53 unreachable”  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  The initial outgoing request was from IP address 192.51.100.15 to the DNS server requesting the IP address for the domain yummyrecipesforme.com which was 203.0.113.2 which was sent to the UDP packet. The UDP packet returned the error message indicating the UDP packet was undeliverable to port 53 of the DNS server, the time of the incident was 13:24. The source IP address was 192.51.100.15 and the destination IP address was 203.0.113.2. For the ICMP error response the source IP address was 203.0.113.2 and the destination IP address was 192.51.100.15. In the error log, the query identification number appears as 35084 with a plus sign after, indicating the flag associated with the UDP message  Note a likely cause of the incident:  A likely cause of the incident would be that the DNS server is down and unreachable. It could be because of a DoS Attack to the server |