# 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 user’s computer tried to request the IP address of yummyrecipesforme.com from the DNS server using the port 53, which is the standard port for DNS service.  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”, indicating that the DNS server was not listening on the port 53 or that the port was blocked by a firewall or other network device.  The port noted in the error message is used for: resolving domain names to IP addresses, which is essential for accessing websites by their names instead of their numerical addresses.  The most likely issue is: the DNS server was down, misconfigured, or compromised, preventing the user’s computer from obtaining the IP address of yummyrecipesforme.com and thus accessing the website. Alternatively, there could be a network problem between the user’s computer and the DNS server that prevented the UDP packets from reaching the port 53. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: \*\*The incident occurred on January 24, 2024, between 16:00 and 17:00 GMT.\*\*  Explain how the IT team became aware of the incident: \*\*The IT team became aware of the incident when they received an alert from the network monitoring system, which detected a spike in DNS and ICMP traffic on port 53.\*\*  Explain the actions taken by the IT department to investigate the incident: \*\*The IT department checked the DNS and ICMP traffic log, which showed a large number of requests from an external IP address to the company's DNS server. They also performed a traceroute to the external IP address, which revealed that it belonged to a known malicious actor.\*\*  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): \*\*The IT department found that the port affected was port 53, which is used for DNS queries. The DNS server was the company's internal DNS server, which handles the resolution of domain names for the company's network. The external IP address was 192.168.1.100, which is associated with a cybercriminal group that has been involved in previous DNS amplification attacks.\*\*  Note a likely cause of the incident: \*\*A likely cause of the incident was a DNS amplification attack, which is a type of distributed denial-of-service (DDoS) attack that exploits the vulnerability of DNS servers to amplify the traffic sent to a target. The attacker sends a large number of DNS queries with a spoofed source IP address to a DNS server, which then responds with a larger amount of data to the target IP address. This results in a flood of traffic that overwhelms the target's network bandwidth and resources.\*\* |