

# Cybersecurity Incident Report

## Section 1: Identify the type of attack that may have caused this network interruption

The DNS protocol relies on UDP to communicate with the DNS server and retrieve the IP address for a domain, in this case, *yummyrecipesforme.com*. However, an ICMP error message was returned, indicating that port 53, the standard port for DNS traffic, was unreachable. This suggests an issue with the DNS server itself.

The logs show that the outgoing UDP message from the browser to the DNS server includes a query identification number (35084) and flags, as indicated by a plus sign (+) and the "A?" symbol. These flags highlight potential issues with the DNS protocol operations. The ICMP error response further confirms that the DNS server is likely unresponsive, preventing successful domain name resolution.

## Section 2: Explain how the attack is causing the website to malfunction

At 1:24 p.m. today, customers reported receiving a "destination port unreachable" error when trying to access *yummyrecipesforme.com*. The cybersecurity team began investigating the issue to restore website access. Using packet sniffing tests with `tcpdump`, they identified that DNS port 53 was unreachable. The next step is to determine whether the issue is caused by the DNS server being down or by a firewall blocking traffic to port 53. Potential causes include a Denial of Service (DoS) attack or a misconfiguration affecting the DNS server.