Cybersecurity Incident Report:
Network Traffic Analysis

Prepared By: Dhyanam
Role: Cyber Security Student (Training)
Year: 2025

Scenario:

Customers reported that the website *www.yummyrecipesforme.com* was unreachable. Network traffic captured using tcpdump showed ICMP messages indicating “UDP port 53 unreachable,” meaning DNS requests were not reaching the DNS server. This caused users to experience connection failures when attempting to load the website. The analysis suggests the DNS server may have been overwhelmed or intentionally blocked, potentially due to a DDoS attack or misconfiguration. Further investigation of firewall rules and server health is required to restore normal service.

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The Tcpdump network protocol analyzer reveals that the UDP packet was undeliverable to the DNS server. 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”. Port 53 is a port for DNS service. The word "unreachable" in the message indicates 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. The most likely issue is the DNS server is under a malicious attack which is most likely a DDoS attack.

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

The time this incident occurred was at 1:24PM when some customers of clients reported that they were unable to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

The network security team responded and began running tests with the network protocol analyzer tool tcpdump.

Looking at the logs generated by the tcpdump we can clearly see a problem with the UDP protocol where port 53 is unreachable. The DNS server with IP address 203.0.113.2 is unreachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. Our next step includes checking the firewall configurations because Network administrators may block it intentionally to force secure DNS and contacting the system administrator for the web server to have them check the system for signs of an attack.

Conclusion:

Based on the network traffic analysis, the DNS server was unreachable due to UDP port 53 being blocked or overwhelmed. The evidence suggests a possible DDoS attack or misconfiguration. Further investigation of firewall rules and server health is required to restore normal service.