

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 traffic shows that: DNS resolution is failing because the server at 203.0.113.2 is returning ICMP port unreachable messages for UDP port 53.

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: DNS service

The most likely issue is: DNS destiny service is not active or being blocked by a Firewall or external cause

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

Time incident occurred: 3 incidents reported at 1:24 pm, 1:26 pm and 1:28

Explain how the IT team became aware of the incident: IT was denied the access to main url (Yummierrecepesforme.com)

Explain the actions taken by the IT department to investigate the incident: It was confirmed that 3 requests sent from IP 192.51.100.15 to the server 203.0.113.2 Systematically failed with ICMP error port 53 unreachable

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): We got 3 ICMP error messages at port 53

Note a likely cause of the incident: Port 53 DNS Being Blocked by security measures (firewall config) or External cause.

We are continuing to investigate the cause of this incident to determine how to restore service to the main url. Our next step is to check Firewall configuration to check if port 53 is being blocked and contacting DNS server provider for them to check logs and identify signs of a malicious incident.

