

# 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: [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) is unreachable. And there has been about 3 attempts and none of was successful as it was described by the ICMP port 53 unreachable

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The ICMP port 53 was unreachable. 203.0.113.2 domain did not respond, instead results were ICMP 203.0.113.2 port 53 unreachable

The port noted in the error message is used for: port 53 is used for UDP and TCP in this case it is to indicate that interactions between client and server failed

The most likely issue is: DDoS or DoS : Distribution denial of service or denial of service or it could be that the information requested by user require for them to be authorized to have access to it.

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

Time incident occurred: we had 3 times on this Incident 1:24pm , 1:26pm, 1:28pm

Explain how the IT team became aware of the incident: The IT team are aware of this incident by using the TCPdump analyzer tool that helps them identify the logs and all activities that are taking place in the organization network

Explain the actions taken by the IT department to investigate the incident: Identify the issue and analyze it. How to restore the web server so that the organization can go back to its normal daily function and the IT team also has to work strengthening their security in order to prevent such incidents in the future and this includes looking for other vulnerabilities that this incident might have made them aware of.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): DNS server unreachable port 53. DNS server not reachable

Note a likely cause of the incident: DDoS and DoS