

# 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 packets can not reach the destination  
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 server  
The most likely issue is: Denial of Service Attack

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

The incident occurred around 1:24 p.m. Users reported that they can not reach the site  
We tried reaching the site via browser, then got an error, switched on the network analyzer, and tried to reach the site again, same error occurred, sent by ICMP. This shows that the DNS server port 53 is down; it can not accept requests. This is likely caused by DOS. Currently, the error persists, and we need to notify the DNS server company about the issue to investigate further.