

Cybersecurity Incident Report:

Network Traffic Analysis

Part 1: Summary of the problem found in the DNS and ICMP traffic log

The UDP protocol reveals that:

The client system sent DNS queries using UDP to the DNS server on port 53 in order to resolve the domain name www.yummyrecipesforme.com.

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 (Domain Name System) services, which are responsible for resolving domain names to IP addresses.

The most likely issue is:

The DNS service on the destination server was unavailable, misconfigured, or blocked, causing DNS requests sent over UDP port 53 to be unreachable.

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

Time incident occurred:

13:24:32 (1:24 p.m.), as indicated by the timestamps in the tcpdump log.

Explain how the IT team became aware of the incident:

The IT team became aware of the incident after multiple users reported that they were unable to access the website and received a “destination port unreachable” error message.

Explain the actions taken by the IT department to investigate the incident:

The IT department used a network protocol analyzer (tcpdump) to capture and analyze DNS and ICMP traffic while attempting to access the affected website.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

- DNS queries were sent over UDP to port 53.
- The DNS server responded with ICMP error messages indicating that UDP port 53 was unreachable.
- DNS name resolution failed, preventing the browser from proceeding to HTTPS communication.

Note a likely cause of the incident:

A DNS server outage, firewall rule, or service misconfiguration that prevented UDP traffic on port 53 from reaching the DNS service.

A network flow diagram for the UDP DNS query and ICMP reply visualizes the failed resolution attempt from the tcpdump log. It highlights the outbound UDP packet and inbound ICMP error, clarifying the port 53 issue

