

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:

The browser attempted to send DNS queries to the server (IP: 203.0.113.2) using UDP on port 53, but these requests were met with ICMP error messages.

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," indicating that the DNS server is not responding on its designated port.

The port noted in the error message is used for:
Domain Name System (DNS) services.

The most likely issue is:

The DNS server on IP 203.0.113.2 is either misconfigured, the service is inactive, or a firewall is blocking access to UDP traffic on port 53.

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

Time incident occurred:

The first instance of the issue was recorded at 13:24:32.

Explain how the IT team became aware of the incident:

Clients reported that the website www.yummyrecipesforme.com was inaccessible, and attempts to load the site resulted in the error "destination port unreachable."

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

- Captured network traffic using `tcpdump` while attempting to access the site.
- Analyzed the logs to identify trends in DNS and ICMP traffic.

Note key findings of the IT department's investigation (i.e., details related to the port

affected, DNS server, etc.):

- UDP packets sent to the DNS server (203.0.113.2) on port 53 failed to elicit a proper DNS response.
- ICMP error messages indicated that the "udp port 53 is unreachable."
- The issue is isolated to the DNS server responsible for resolving the domain www.yummyrecipesforme.com.

Note a likely cause of the incident:

The DNS server on IP 203.0.113.2 is either:

1. Experiencing a service outage or configuration issue.
2. Blocked by a firewall preventing incoming or outgoing UDP traffic on port 53.