

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: it was used to request a domain name resolution using the address of the DNS server over port 53. Port 53 was “unreachable” and it indicates the message did not go through to the DNS server. The browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.”

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: Port 53 is a well-known port for DNS service.

The most likely issue is: the DNS server is not responding.

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

Time incident occurred: 1:24 p.m., 32.192571 seconds.

Explain how the IT team became aware of the incident: Several customers contacted my company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

Explain the actions taken by the IT department to investigate the incident: Our network security team responded and began running tests with the network protocol analyzer tool tcpdump in order for customers to be able to access the website again.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The resulting logs revealed that Port 53, which is a well-known port for DNS service, is not reachable. The next step is to identify whether

the DNS server is down or traffic to port 53 is blocked by the firewall.

Note a likely cause of the incident: The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.