

Cybersecurity Incident Report

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

The network protocol analyzer logs show that the website www.yummyrecipesforme.com cannot be resolved by the DNS server. The user's computer attempts to resolve the domain's IP address by sending a DNS request (UDP packet to port 53), but receives an ICMP response indicating that UDP port 53 is unreachable.

This means that the DNS server (203.0.113.2) is not responding to name resolution requests, possibly because the DNS service on that server is down or port 53 is being blocked by a misconfigured firewall. As a result, the user's browser cannot retrieve the IP address of the website and displays a "destination port unreachable" error.

This behavior may indicate a failure in the DNS server, a network configuration issue, or even a potential denial-of-service (DoS) attack aimed at disrupting name resolution services.

Part 2: Explain your analysis of the data and provide one solution to implement

The incident occurred when several clients reported they could not access the website www.yummyrecipesforme.com and received a "destination port unreachable" error. After replicating the issue and analyzing the traffic with the tcpdump tool, multiple failed DNS resolution attempts were observed. Outgoing requests from IP 192.51.100.15 to the DNS server at 203.0.113.2, using the UDP protocol and port 53, were not properly answered. Instead, ICMP messages were received indicating that UDP port 53 was unreachable.

This pattern suggests that the DNS server does not have its resolution service running or the port is being blocked. Since the domain's IP cannot be resolved, the browser is unable to load the website.

Proposed solution:

- Verify that the DNS service is running properly on the 203.0.113.2 server.
- Ensure that UDP port 53 is open and not being blocked by a firewall.
- Check whether the DNS server has been the target of any attacks (such as DoS) that may have caused the service to go down.

