Cybersecurity Incident Report

Network Traffic Analysis (DNS & ICMP)

Part 1 (Step 1): Summary of the Problem Found in the DNS and ICMP Traffic Log

The UDP protocol reveals that repeated DNS query packets were sent from the client system (192.51.100.15) to the DNS server (203.0.113.2) in order to resolve the domain www.yummyrecipesforme.com. These DNS queries were transmitted using UDP port 53, which is the standard port for DNS services.

This is based on the results of the network analysis, which show that the ICMP response returned the error message 'UDP port 53 unreachable'. This message indicates that the DNS server was unable to receive or process the UDP packets sent to port 53.

The port noted in the error message is used for Domain Name System (DNS) services, which are required to translate domain names into IP addresses so that web connections can be established.

The most likely issue is that the DNS service on the destination server is unavailable, stopped, misconfigured, or blocked by a firewall, preventing DNS queries from being successfully processed.

Part 2 (Step 2): Initial Incident Awareness and Investigation

The incident occurred at approximately 13:24, as indicated by the timestamps in the tcpdump logs. The IT team became aware of the incident after several users reported that they were unable to access the website www.yummyrecipesforme.com and experienced destination port unreachable errors.

In response to these reports, the IT department initiated an investigation by capturing network traffic using the tcpdump protocol analyzer. The goal was to determine whether the issue was related to DNS resolution, network connectivity, or a potential security incident.

Part 3 (Step 3): Detailed Analysis of the tcpdump Log

The tcpdump logs revealed a consistent pattern of DNS queries sent from the client to the DNS server using UDP. Each DNS request was followed by an ICMP error message indicating that UDP port 53 was unreachable. This confirms that the DNS server was not accepting DNS requests at the time of the incident.

The protocols observed during the investigation include UDP for DNS queries, DNS for name resolution services, and ICMP for reporting network-level errors back to the client.

Part 4 (Step 4): Incident Explanation, Root Cause, and Resolution Steps

The error messages appeared because the DNS server was unable to receive traffic on UDP port 53. Without successful DNS resolution, the client system could not obtain the IP address needed to establish an HTTPS connection to the web server.

Key findings from the investigation include the confirmation that the client system was functioning correctly, DNS requests were being transmitted successfully, and the failure originated from the DNS server or its network configuration.

The most likely root cause of the incident is that the DNS service on the server was stopped, misconfigured, or blocked by firewall rules. This prevented UDP traffic on port 53 from being processed.

Recommended next steps include verifying that the DNS service is running, reviewing firewall rules to ensure UDP port 53 is allowed, restarting the DNS service if necessary, and implementing monitoring to detect similar issues in the future.