Cybersecurity Incident Report: Network Traffic Analysis

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

During routine monitoring, an issue was detected affecting users' ability to access the website "www.yummyrecipesforme.com". Users reported receiving an error message stating "destination port unreachable." A detailed analysis of the DNS (Domain Name System) and ICMP (Internet Control Message Protocol) traffic logs was conducted to identify the root cause of the issue.

The DNS logs revealed that outgoing DNS requests were made correctly from the users' devices to resolve the domain name "www.yummyrecipesforme.com" to its corresponding IP address. However, the ICMP logs indicated that these requests were met with responses stating that UDP port 53 was unreachable. Port 53 is crucial for DNS operations as it is the default port for DNS queries.

The traffic logs showed multiple instances of DNS requests followed by ICMP error responses. These responses highlighted a disruption in the DNS resolution process, preventing users from obtaining the IP address of the website, thereby making it inaccessible.

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

The core problem appears to be with the DNS service, specifically relating to UDP port 53. The ICMP error message "destination port unreachable" indicates that the service expected to be running on port 53 is either down or not responding. This could be due to a variety of reasons such as server downtime, misconfiguration, or even a potential cyber attack targeting the DNS server.

(cont'd on next page)

Proposed Solution:

1. Server Check and Configuration Verification: First, ensure that the DNS server hosting the "www.yummyrecipesforme.com" domain is operational. Check for any recent changes in configurations or updates that might have disrupted the DNS service. Ensure that the server is properly configured to listen to and respond on UDP port 53.

2. Firewall and Network Configuration: Verify that there are no firewall rules or network configurations blocking or misrouting traffic intended for UDP port 53. Ensure that the network path from the user to the DNS server is clear and that there are no intermediate devices interfering with or blocking DNS traffic.

3. Alternate DNS Server: As an immediate mitigation step, consider configuring an alternate DNS server to handle requests for the domain. This could be a temporary measure until the primary server issue is resolved.

4. Monitoring and Alerting: Enhance monitoring on the DNS server to detect and alert any future anomalies quickly. Regularly review logs to ensure that the DNS service is functioning correctly.

5. Communication with Users: Update the affected users on the issue and the steps being taken to resolve it. Provide an estimated time for resolution and alternative access methods if available.