Yazeed

Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Summary of the problem found in the DNS and ICMP traffic log
The network protocol analyzer logs indicate that the "udp port 53" used for domain name resolution (DNS) is unreachable. This means that the DNS requests sent in UDP packets from the computer to the DNS server were not successfully delivered. As a result, the browser was unable to obtain the IP address for the website www.yummyrecipesforme.com, leading to the "destination port unreachable" error. The ICMP response indicated that the DNS server did not have a service listening on the receiving DNS port, causing the delivery failure.

Part 2: Analysis of the data and solutions to implement
Based on the analysis, it is evident that the incident impacted the DNS protocol and service. The failure to reach the DNS server on port 53 prevented the resolution of the domain name for www.yummyrecipesforme.com. As a solution, the following steps can be taken: 1. Verify DNS server availability: Check the DNS server's availability and ensure that it is operational. Ensure that the server is configured to listen on port 53 for DNS requests. 2. Check DNS service configuration: Review the DNS service configuration on the server to ensure it is correctly set up to handle DNS requests and resolve domain names. Verify that there are no misconfigurations or issues with the DNS service. 3. Firewall inspection: Verify that there are no firewall rules or settings blocking DNS traffic on port 53. Review the firewall configuration to ensure that DNS requests can reach the DNS server without any restrictions. 4. DNS server troubleshooting: If the DNS server itself is experiencing issues, it may be necessary to troubleshoot the server and address any underlying problems. This could involve checking server logs, performing diagnostics, or consulting with the DNS server administrator.

DNS & ICMP traffic logs:

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084 + A? yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```