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: port 53 is unreachable

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “ICMP 203.0.113.2 udp port unreachable length 254”

The port noted in the error message is used for:

Domain Name System - DNS

The most likely issue is:

The UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" failed to reach the DNS server because no service was listening on the receiving DNS port.

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

Time incident occurred:13:24:32.192571

Explain how the IT team became aware of the incident:

This problem occurred today to customers who cannot access our web page, the engineers communicated the incident to us and we took it seriously, our team of analysts is seeing what solutions are to be expected and if the origin of this incident is an attack, in any case all our superiors are aware.

Explain the actions taken by the IT department to investigate the incident:

we are tasked with analyzing the situation and determining which network protocol was affected during this incident. First to first, we tried to visit the website and we also received the error "destination port unreachable" To resolve the problem, we loaded our network analysis tool, tcpdump, and tried to load the web page again. To load the web page, our browser sends a Request to a DNS server via the UDP protocol to retrieve the IP address of the website's domain name; this is part of the DNS protocol. our browser then uses this IP address as the destination IP to send an HTTPS request to the web server to display the web page The analyzer shows that when we were sending UDP packets to the DNS server, we receive ICMP packets containing the error message: "udp port 53 unreachable"

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): port affected 53 DNS protocol

Note a likely cause of the incident:

No Process Listening on Port 53 - Firewall or Network Configuration - Closed or Misconfigured DNS Service - Timeouts or Premature Socket Closure - VPN or NAT Issues - ISP-Level Filtering .