Cybersecurity Incident Report:

Network Traffic Analysis

You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage  The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that:the domain "www.yummyrecipesforme.com" did not go through to the DNS server  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: "udp port 53 unreachable"  The port noted in the error message is used for: Port 53 is a port for DNS service.  The most likely issue is: 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:1:24 p.m., 32.192571 seconds.  Explain how the IT team became aware of the incident:Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident:analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): ICMP packets were sent two more times, but the same delivery error was received both times.  Note a likely cause of the incident: no service was listening on the receiving DNS port. |