# 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 the DNS server is down or unreachable. As evident by the results of the network analysis, the ICMP echo reply returned the error message “udp port 53 unreachable,” Port 53 is commonly used for DNS protocol traffic. It is highly likely that the DNS server is not responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred today at 1:23 p.m.. Customers called the organization to notify the IT team that they received the message “destination port unreachable” when they attempted to visit the website. The network security professionals within the organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.   When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps:     1. A SYN packet is sent from the source to the destination, requesting to connect. 2. The destination replies to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect.   In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server’s available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.  The logs indicate that the web server has become overwhelmed and is unable to process the visitors’ SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message. |