# 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 DNS server is down, when attempting to retrieve the IP address of the corresponding domain.  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, 53, is commonly used for DNS protocol traffic.  The most likely issue is a malicious attack on the DNS server, maybe an ICMP flood. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred:  The incident occurred today, at 13:24.  Explain how the IT team became aware of the incident:  The IT team became aware of the incident through our customers reporting that they can’t access our website, receiving a “destination port unreachable” message.  Explain the actions taken by the IT department to investigate the incident:  Thus far, we investigated by conducting packet sniffing analysis using tcpdump, in which 3 messages were found, giving out the same delivery error: “udp port 53 unreachable”.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  We discovered that port 53 interrupts communication, which is typically used for DNS. Our team thinks that the DNS server is overflown. We are currently further investigating the root cause of this issue to determine how we can restore access to the website.  Note a likely cause of the incident:  We think a Denial of Service attack on the DNS server impacted the functioning of the website, possibly an ICMP flood/ a ping of death, or even a setting change in our firewall. |