# 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 when an attempt is made to access the DNS server. Port 53 is normally used for UDP packets.  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 accessing a secure DNS server for IP resolution.  The most likely issue is an ongoing malicious attack on the DNS server, or a misconfiguration of the DNS firewall. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24pm  Explain how the IT team became aware of the incident: Our clients reported that their customers were experiencing downtime while attempting to access their website.  Explain the actions taken by the IT department to investigate the incident: In response, the IT team began investigating possible causes by running tests using our network analyzer tool, TCP dump. The logs revealed that port 53 which is used for UDP traffic was unreachable. We are still investigating the issue to determine the root cause of the outage and restore access to the DNS server in the shortest possible time. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the administrator to check for any signs of malicious activity.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Details from the log revealed that this was an internal attack from a disgruntled employee who left the company a week ago. The network security team believes that the employee still had permissions that allowed him to block the port number on the firewall which subsequently caused the outage. It is possible the employee’s intent was for the company to temporarily lose money. |

**TCP DUMP LOGS**