# 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 UDP packet was unable to access the desired domain due to unreachable port 53.  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 used for UDP communication specifically regarding DNS.  The most likely issue is: |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  Explain how the IT team became aware of the incident:  Explain the actions taken by the IT department to investigate the incident:  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident:  The incident occurred earlier this morning when the human resources (HR) team reported that they could not reach the background check web portal. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 443, which is used for HTTPS traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. Our next steps include checking the firewall configuration to see if port 443 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. The HR team believes it is possible that a certain new hire may want to keep them from performing the background check. The network security team suspects this person might have launched an attack to crash the background check website. |