# **Cybersecurity Incident Report:**

# **Network Traffic Analysi**s

|  |  |
| --- | --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| **UDP Protocol:** The network analysis indicates the use of UDP protocol. | **Awareness of Incident:** Customers reported website access issues. |
| **ICMP Echo Reply Error:** The ICMP echo reply returned the error message "udp port 53 unreachable". | **IT Actions:** Loaded network analyzer, identified UDP and ICMP patterns. |
| **Port 53:** The port noted in the error message is used for DNS service. | **Key Findings:** Impact on DNS service over port 53 with UDP. |
| **Likely Issue:** The DNS service over UDP (port 53) was impacted. | **Likely Cause:** DDoS attack causing DNS server unavailability. |

|  |  |
| --- | --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| UDP Protocol: The network analysis indicates the use of UDP protocol. |  |
| ICMP Echo Reply Error: The ICMP echo reply returned the error message "udp port 53 unreachable". |  |
| Port 53: The port noted in the error message is used for DNS service. |  |
| Likely Issue: The DNS service over UDP (port 53) was impacted. |  |

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| **Awareness of Incident:** Customers reported website access issues. |
| **IT Actions:** Loaded network analyzer, identified UDP and ICMP patterns. |
| **Key Findings:** Impact on DNS service over port 53 with UDP. |
| **Likely Cause:** DDoS attack causing DNS server unavailability. |
|  |