Cybersecurity Incident Report

| **Part 1: Summary of the problem found in the DNS and ICMP traffic log** | |
| --- | --- |
| The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the client company website. This is based on the results of the network analysis, which shows that the ICMP echo reply returned the error message “Udp port 53 unreachable”. The port noted that in the error message, indicates the UDP message requesting an IP address for the domain “[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)” did not go through to the DNS server because no service was listening on the receiving DNS port. | |
|

| **Part 2: Analysis of the data and Cause of the incident** |
| --- |
| The incident occurred earlier this afternoon when several customers of clients reported that they were not able to access the client company website.. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53 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 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. The network security team suspects a hacker might have launched an attack to crash the client company website. |