# 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 three requests from the source IP 192.51.100.15 to the website yummyrecipesforme.com did not go throught to the DNS server because no service was listening on the receiving DNS port. (ICMP packets return)  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:  53  The most likely issue is:  Possible DoS attack. Needs for further investigation | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred:  Between 13:24 and 13:26  Explain how the IT team became aware of the incident:  Tcpdump fidnings while trying to load the yummyrecipes.com  Explain the actions taken by the IT department to investigate the incident:  The IT Team load the page and found “destination port unreachable”. Therefore, they tried to load anetwork analyzer tool ( in this case, tcpdump) and tried to load the webpage yummyrecipes.com. They received three failed requests stating “udp port 53 unreachable”  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Port affected: 53  Destination IP: 203.0.113.2  ICMP pakctes requests length: 1) 254, 2) 320, 3) 150  Duration of requests: all of them - 32.192571 s  Query identification number: 35084+  All teh three requests were sent to the A record domain  Note a likely cause of the incident:  Possible DoS attack or bad gateway error. Need for futher investigation |