# Cybersecurity Incident Report:

# Network Traffic Analysis

Made by: NIDA AZAM

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log. |
| The UDP protocol reveals that:  It reveals that UDP port 53 is not reachable which means DNS is not working.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  It returned that “UDP port 53 is unreachable”  The port noted in the error message is used for:  DNS services which translates domain names into IP addresses.  The most likely issue is:  The DNS sever is likely down, not configuring properly and that’s why its service is not working properly. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  13:24:32.192571 seconds (first time attempt of login).  Explain how the IT team became aware of the incident:  When users were trying to login to the website they were getting errors so team confirmed it by trying to login by themselves and three times so it was confirmed that dns service has a problem.  Explain the actions taken by the IT department to investigate the incident:  The captured the logs from tcpdump, tried to login and get error. After multiple attempts it was confirmed that without dns resolution website won’t work at all.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   1. Source ip 192.51.100.15 used source port 52444 when sending the queries. 2. Then they get error like UPD port 53 unreachable. 3. Tried many times but still faced error so it means that the issue won’t resolve till we fix dns service.   Note a likely cause of the incident:  The DNS service is down maybe a firewall blocked or maybe some misconfigurations. |