# 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: We sent a request properly from our computer, but the server did not return it. It wasn’t rejected, just unreachable. This was verified using tcpdump.  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 lenght 254.  The port noted in the error message is used for: DNS services.  The most likely issue is: The DNS server is down. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 13:24:32  Explain how the IT team became aware of the incident: The IT team was controlling the access to the companies’ websites, and found that this particular one could not be accessed.  Explain the actions taken by the IT department to investigate the incident: We sent two more requests to make sure it wasn’t a one time thing. After proving that it was a recurring issue, we tried other webpages, checking specifically for pages hosted in different servers. We then found that the issue affected an entire particular server (pod 11).  We then went on to check the server status of the Pod 11 server, and as it turns out, there was a computing error. We rebooted the server and everything seemed to work correctly.  We finally investigated for sign of a malicious attack.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): It turned out that the server was not affected by a malicious attack, but instead, there was a problem with the latest server update, which caused the server to crash due to a file error. This was fixed by reverting the server to the last correct working snapshot.  Note a likely cause of the incident: Rushed installation of new server updates. |