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 network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the secure employee background check website. The port noted in the error message is used for: Port 53 is normally used for DNS traffic. The most likely issue is: This may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of a malicious attack on the web server, which caused it to be flooded and unusable.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occurred earlier this afternoon. Explain how the IT team became aware of the incident: The human resources (HR) team reported that they could not reach the background check web portal. Explain the actions taken by the IT department to investigate the incident: The network security team responded and began running tests with the network protocol analyzer tool tcpdump (1:24 p.m., 32.192571 seconds.). Note key findings of the IT department's investigation: The resulting logs revealed that port 53, which is used for DNS traffic, is not reachable. Note a likely cause of the incident: 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 HR team believes it is possible that a certain new hire may want to keep them from performing the background check. The network security team suspects this person might have launched an attack to crash the background check website.