Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs indicated that port 53 is unreachable when attempting to access the secure employee background check website. Port 53 is normally used for DNS service. This may indicate a problem with that no service was listening on the receiving DNS port. It is possible that this is an indication of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred after several customers of clients were not able to access a client's website (www.yummmyrecipesforme.com). The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS service, 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 443 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.