Cybersecurity Incident Report

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

The network protocol analyzer logs indicate that port 443 is unreachable when attempting to access the secure employee background check website. Port 443 is for HTTPS traffic. This may indicate a problem with the web server or the firewall configuration. This can indicate a web server attack so we must proceed with containing this.

Part 2: Explain your analysis of the data and provide one solution to implement

The incident occurred this morning when the HR team reported that they could not reach the background check web portal. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 443, which is used for HTTPS traffic, 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. We must first of all block this suspect access and conduct a log check of his user, this can be performed in non work hours to not suspend the team work, but must be executed as soon as possible in order to prevent further damage.