Day 15

Objective: To generate phishing URLs and capture credentials using RubikPhish.

Work Description: Fake login pages were generated using RubikPhish in a controlled lab environment. The captured credentials were displayed in the terminal to demonstrate how attackers steal sensitive information. Defensive measures such as MFA and URL verification were discussed alongside the demonstration.

Outcome: Learned how credential harvesting attacks are executed ethically for awareness.