Day 85

Topic: Social Engineering

Objective: To understand human-based attacks and use the Social-Engineer Toolkit (SET).

Theoretical Concepts:
Social Engineering exploits human psychology. We discussed Phishing, Pretexting, Baiting, and Quid Pro Quo. We focused on the technical delivery of these attacks.

Practical Work:
We used the **Social-Engineer Toolkit (SET)** on Kali Linux. We selected the "Website Attack Vectors" -> "Credential Harvester Method" -> "Site Cloner". We cloned a login page (e.g., Google login). SET hosted this fake page on our local IP. When we accessed it from the victim machine and entered credentials, the username and password appeared in our terminal.

Tools Used: SET Toolkit.

Outcome: Demonstrated how easily convincing phishing sites can be created and the risk of credential harvesting.