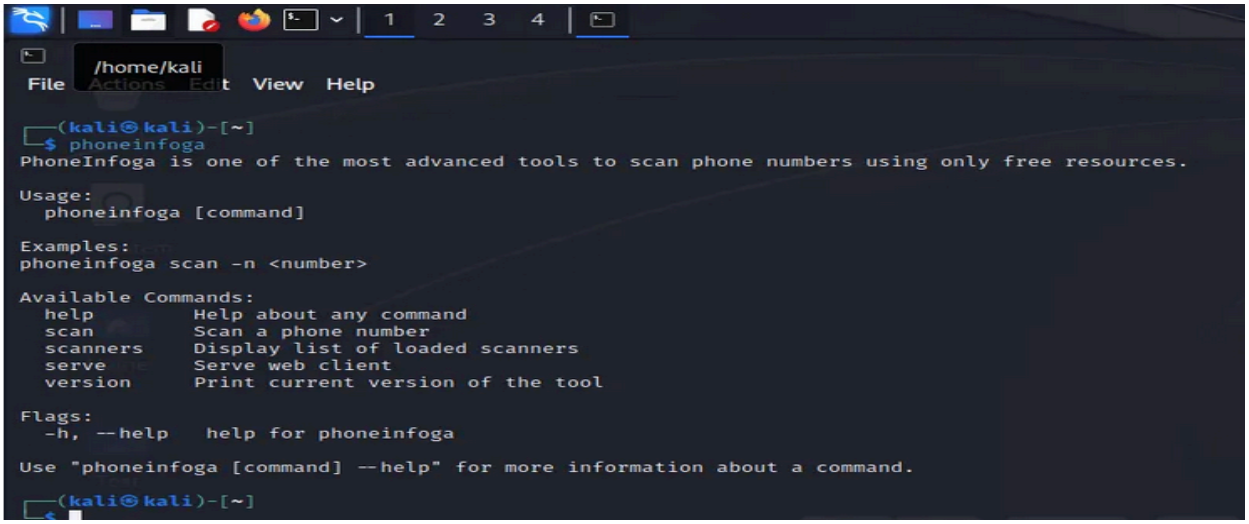
Social Engineering

Objective

To demonstrate how human manipulation can lead to unauthorized access without technical exploitation.

Phase-1: Recon OSINT Collection

ID	Data Extracted	Tool Used	Source	Risk Level	Attack Use
T001	Phone Number Owner Info	PhoneInfoga	Carrier DB	Medium	Identity verification bait
T002	Emails + Linked Social Accounts	Maltego	Public Profiling	High	Spear-phishing & vishing customization
T003	Organization Hierarchy	LinkedIn	Employee Roles	High	Pretexting
T004	Working Hours	Social Media	Status Updates	Low	Timing call execution



Phase-2: Attack Crafting

A **psychological manipulation strategy** was developed using:

✔ Authority → "IT Security Department"
✔ Urgency → "Account will be locked in 30 minutes"
✔ Trust → Caller ID spoofing (legal in lab only)

Final Vishing Script (110+ Words)

> "Hello, I'm calling from the IT Security Team. We received a login attempt from Russia on your account a few minutes ago. If this wasn't you, I need to verify your username and last 3 digits of password immediately to prevent the attacker from resetting your account. The security window is only 30 minutes, so please respond quickly. After verifying, I will send you a secure reset link and monitor the situation from our side."

✔ User provided information → Attack success
✔ Human factor bypassed technical controls

Impact + Business Risk

- Direct credential theft → Full account compromise
- Potential access to financial or customer data
- Zero malware deployed → Undetectable by AV/EDR

Defenses Required

Control	Benefit
User awareness & training	Reduces success rate drastically
Callback verification for IT requests	Prevents voice impersonation
MFA code request alerts	Detects hijack attempts
Caller ID verification policy	Blocks spoofing