Foot-printing & Social Engineering Investigation

Name : Rohinish

Mini-Project

Project Objective

- Gather passive information about a test organization
- Develop a social engineering exploit scenario

Key Topics

- Foot-printing
- Social Engineering
- Countermeasures

What is Footprinting?

- Footprinting means **gathering information** about a target (a company, a website, or a person) using publicly available data — without any direct contact or illegal activity.

Footprinting Tools

- whois, dig – domain info
- theHarvester – email & domain gathering
- Google Dorks – find hidden files
- Maltego – data visualization
- Shodan – discover devices on the internet
- LinkedIn – find employees & roles

What is Social Engineering?

- It is a manipulation technique that exploits human error to gain personal information, access and valuables.

Types of Social Engineering Attacks

- Phishing – fake emails or websites
- Pretexting – pretending to be someone
- Baiting – using infected USBs
- Tailgating – physically following into secure areas

Exploit Plan

- Target: Victim Machine
- Scenario: Fake Internship email
- Attachment: Document with payload

Defense Recommendations

- Security awareness training
- Email filtering & antivirus
- Limit public exposure of sensitive data
- Implement access controls

Project Outcome

- Understood how attackers gather data
- Designed a legal and safe exploit scenario
- Developed practical defense strategies

Thankyou