


Lesson 10: Social Engineering

Module 14: Ethical Hacking Principles

Topic: Social Engineering: Attacks & Prevention

 **Duration:** 3 hours

 **Objective:** Understand social engineering as a cybersecurity threat and learn how to recognize, execute, and prevent social engineering attacks.

Session Breakdown

1. Introduction (30 mins)

- Recap of Day 3 (Threat Actors)
- Introduction to Social Engineering:
 - Definition & history
 - Why humans are the weakest link
 - Real-world case studies (e.g., Twitter Bitcoin scam, Kevin Mitnick)

2. Practical Session (1 hour 30 mins)

- **Activity 1:** Watch short clips showing phishing and baiting scenarios (use YouTube videos or pre-approved materials)
- **Activity 2:** Simulate basic phishing email creation (e.g., a fake password reset email using free tools like GoPhish, SET)
- **Lab Exercise:**
 - Analyze a collection of phishing emails – identify triggers and techniques
 - Build a flowchart: “How a phishing attack is planned and executed.”
- Optional advanced: Demonstrate use of Social-Engineer Toolkit (SET) on Kali (ethical use only in closed lab)

3. Conclusion (30 mins)

- Recap key social engineering techniques:
 - Phishing, Vishing, Baiting, Pretexting, Tailgating
- Group discussion: “Have you ever been socially engineered without realizing it?”
- Introduce prevention strategies:
 - User awareness training, spam filters, 2FA, role-based access

Homework/Assignment:

- Create a checklist titled: “How to Detect a Phishing Attempt” with at least 10 items.
- Optional: Interview a friend/family member and ask if they’ve ever received a suspicious email or call. Summarize their experience in a paragraph.