ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

Module 6. Social Engineering

Penetration testing course

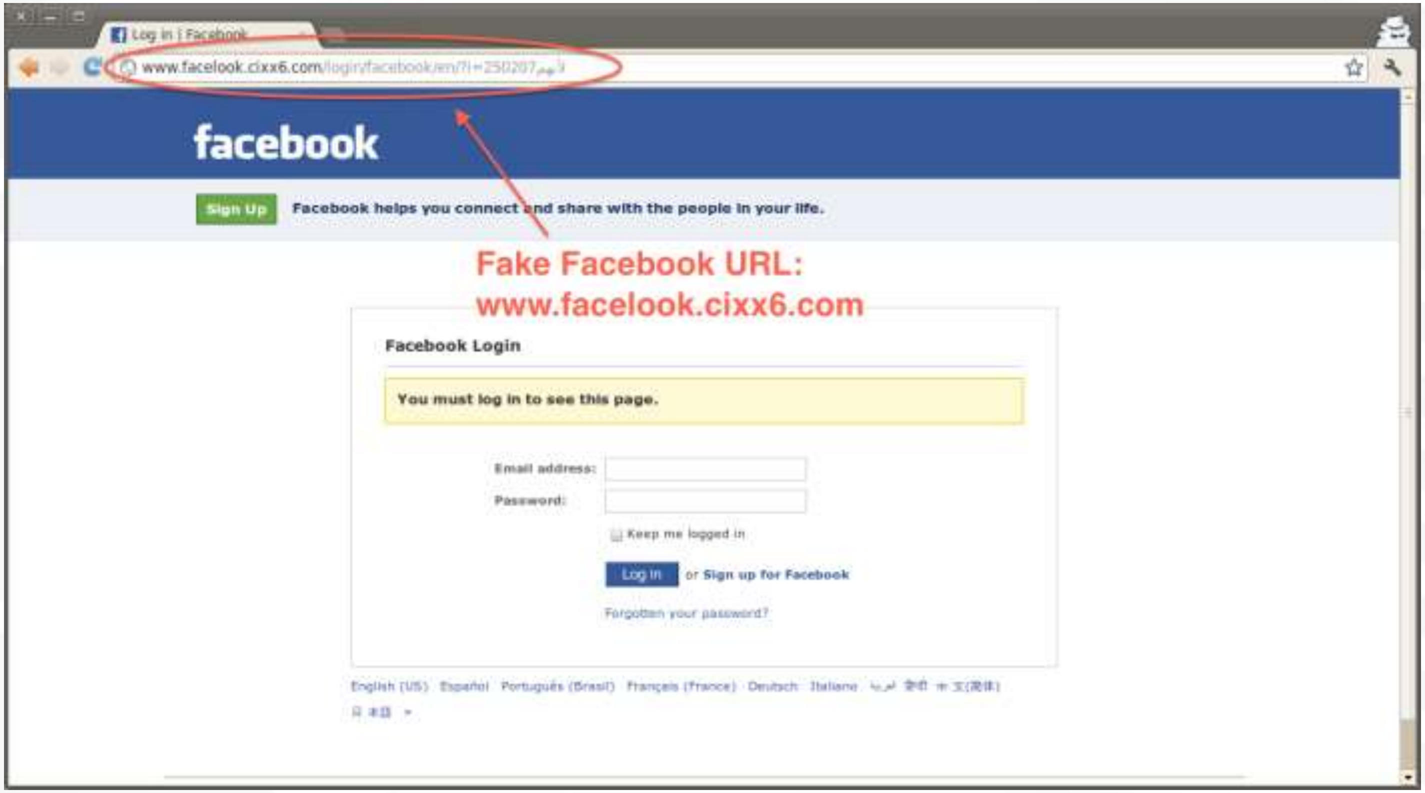
Social engineering

- The “hacking” of people.
- Obtaining, collecting, and using unauthorized information garnered via technical and non-technical means while interacting with others.
- Involves persuasion, lies, manipulation, and many other crafty methods while relying on a person’s natural sense to be helpful and their lack of understanding that the information being released is sensitive and/or confidential
- Use psychology methods in malicious way

Types of Attacks

- Phishing
- Impersonation on help desk calls
- Physical access (such as tailgating)
- Shoulder surfing
- Dumpster diving
- Stealing important documents
- Trojans

Phishing



Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207
facebook
Sign Up

Facebook helps you connect and share with the people in your life.

Fake Facebook URL:
www.facelook.cixx6.com

Facebook Login

You must log in to see this page.

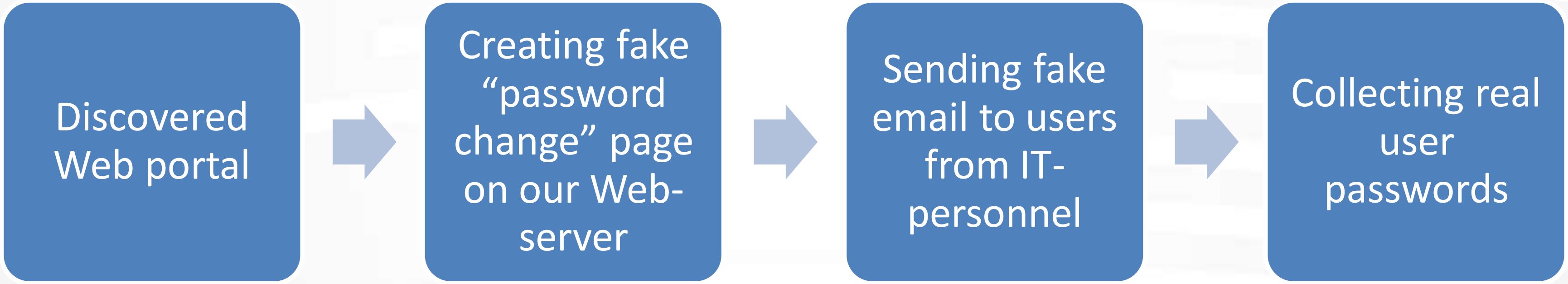
Email address:

Password:

□ Keep me logged in

Log In
or Sign up for Facebook
Forgotten your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
日本語

Example of phishing scenario for penetration testing



Discovered Web portal

Creating fake “password change” page on our Web-server

Sending fake email to users from IT-personnel

Collecting real user passwords

Impersonation on phone calls

- Impersonation on help desk calls
- Usually someone with authority

Example

- Penetration tester intercepts communication between administrator's computer and border router.
- When administrator tries to login to router he will get message that certificate is not valid. In normal situation he will stop.
- To enforce human error penetration tester could call to administrator pretending to be a top manager and ask him to solve the problem with internet.

Physical access

- Tailgating\Piggy backing
- Ultimately obtains unauthorized building access

Shoulder surfing

- Someone can watch the keys you press when entering your password
- Hidden cameras\binoculars may be used

Dumpster diving

- Looking through the trash for sensitive information

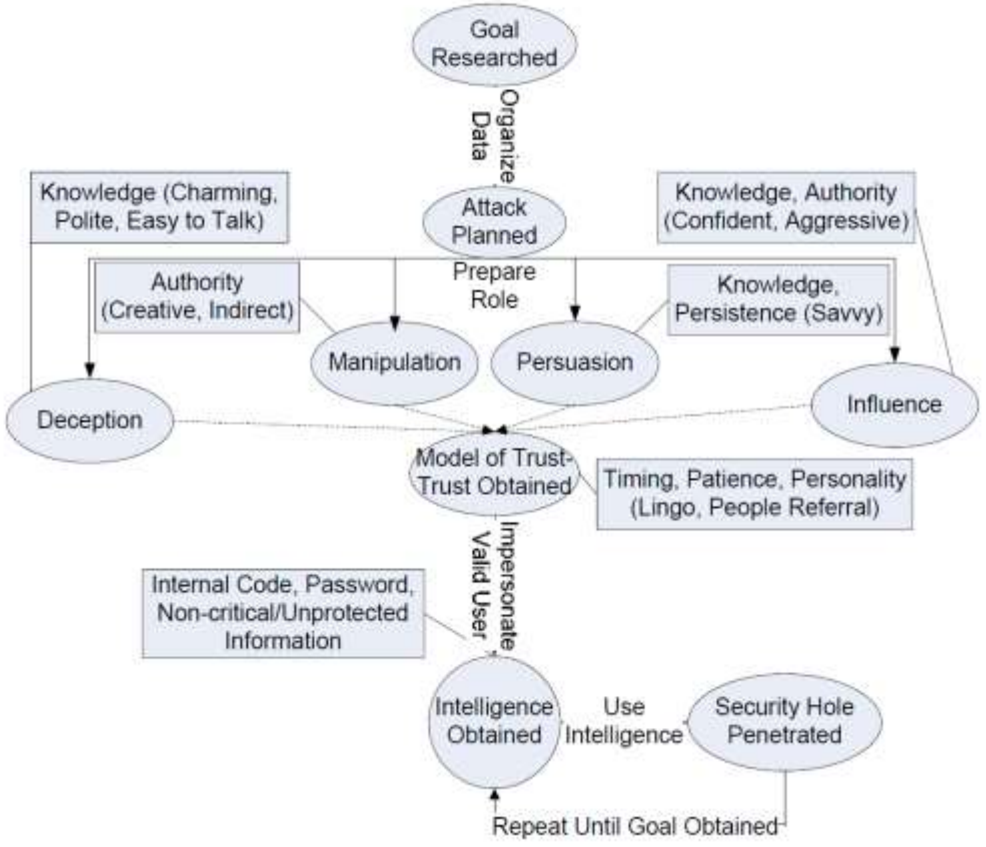
Stealing important documents

- Can take copy of documents on someone's desk

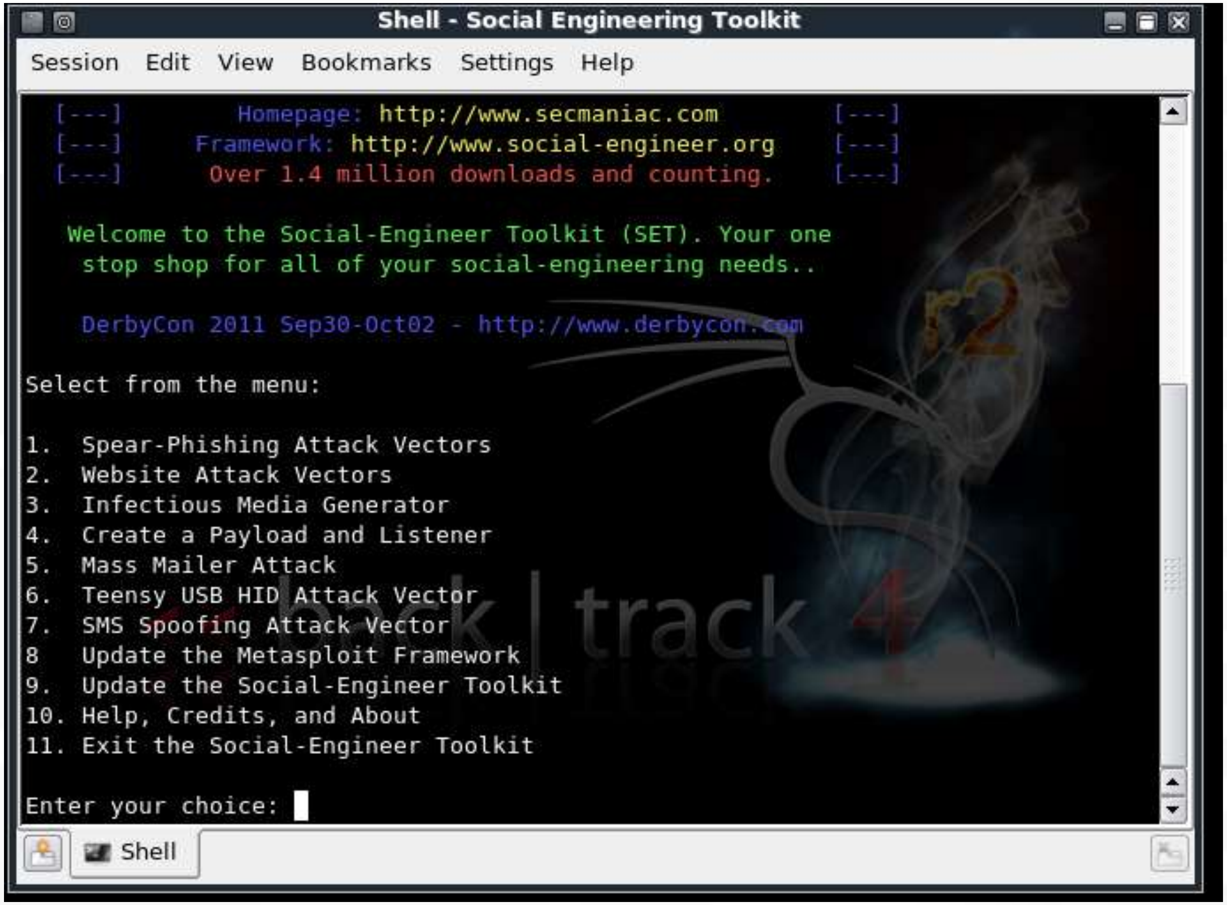
Trojans

- Appears to be useful and legitimate software before running
- Performs malicious actions in the background
- Does not require interaction after being run

Social engineering attack model


Goal Researched
Organize Data
Attack Planned
Knowledge (Charming, Polite, Easy to Talk)
Knowledge, Authority (Confident, Aggressive)
Prepare Role
Authority (Creative, Indirect)
Knowledge, Persistence (Savvy)
Manipulation
Persuasion
Deception
Influence
Model of Trust-Trust Obtained
Timing, Patience, Personality (Lingo, People Referral)
Impersonate Valid User
Internal Code, Password, Non-critical/Unprotected Information
Intelligence Obtained
Use Intelligence
Security Hole Penetrated
Repeat Until Goal Obtained

SET – social engineering toolkit



Shell - Social Engineering Toolkit
Session Edit View Bookmarks Settings Help
Shell

```
  [---]        Homepage: http://www.secmaniac.com          [---]
  [---]     Framework: http://www.social-engineer.org      [---]
  [---]      Over 1.4 million downloads and counting.      [---]

   Welcome to the Social-Engineer Toolkit (SET). Your one
    stop shop for all of your social-engineering needs..

    DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com

Select from the menu:

1.  Spear-Phishing Attack Vectors
2.  Website Attack Vectors
3.  Infectious Media Generator
4.  Create a Payload and Listener
5.  Mass Mailer Attack
6.  Teensy USB HID Attack Vector
7.  SMS Spoofing Attack Vector
8   Update the Metasploit Framework
9.  Update the Social-Engineer Toolkit
10. Help, Credits, and About
11. Exit the Social-Engineer Toolkit

Enter your choice:
```

SET

The Social Engineer Toolkit incorporates many useful social-engineering attacks all in one interface. The main purpose of SET is to automate and improve on many of the social-engineering attacks out there. It can automatically generate exploit-hiding web pages or email messages, and can use Metasploit payloads to, for example, connect back with a shell once the page is opened