# Chapter 9: Social Engineering

## Technology Brief

In this Chapter, "Social Engineering," we will discuss the basic concepts of Social Engineering and how it works. This technique is different from other information stealing technique used so far. All previous tools and technique used for hacking a system are technical and requires a deep understanding of networking, operating systems, and other domains. Social Engineering is the non-technical part of gaining information. It is most popular among other technique because of its ease as humans are most prone to mistake in terms of carelessness.

Security model includes network security, security of other resources of a corporate network, but humans are the most important component of the security. All security measures are dependent upon. If a User is careless to secure its login credentials, all security architectures will fail. Spreading awareness, training and briefing the user about Social Engineering, Social Engineering attacks and the impact of their carelessness will help to strengthen the security from endpoints.

This chapter will cover an overview of Social Engineering concepts, Types of Social Engineering attacks; you will learn how different social engineering techniques works, what are insider threats, how can an attacker impersonate on social networking sites, identity theft and how these threats of social engineering can be mitigated. Let's start with Social Engineering Concepts.

## Social Engineering Concepts

### Introduction to Social Engineering

Social Engineering is an act of stealing information from humans. As it does not have any interaction with target system or network, it is considered as a non-technical attack. Social Engineering is considered as the art of convincing the target to reveal information. It may be physically one-to-one interaction with the target or convincing the target on any platform such as social media is a popular platform for social engineering. This is the fact that people are careless, or unaware of the importance of the valuable information they possess.

#### *Vulnerability to Social Engineering Attacks*

One of the major vulnerability which leads to this type of attack is "Trust." The user trusts another user and does not secure their credentials from them. This may lead to an attack by the user, to the second person may reveal the information to the third one.

Organizations unaware of Social Engineering attacks, and its countermeasure and precaution are also vulnerable to this attack. Insufficient training program and education

of employees create a vulnerability in the security against Social Engineering. Each organization must train their employees to be aware of social engineering.

Each organization must secure its infrastructure physically as well. An employee having a different level of authority should be restricted to perform in their restricted privileges. Employee not allowed to access the departments such as Finance department, he should be restricted to its allowed departments only. In the case where an employee is free to move may perform social engineering by Dumpster Diving or Shoulder surfing.

Lack of Security policies and privacy are also vulnerable. Security policies must be strong enough to prevent an employee from impersonating another user. Privacy in between unauthorized people or client and the employee of an organization must be maintained to keep things secure from unauthorized access or steal.

**Phases of a Social Engineering Attack**

Social Engineering attacks are not the complex attack which requires strong technical knowledge. An attacker might be Non-technical personal as defined earlier; it is an act of stealing information from people. However, Social Engineering attacks are performed by the following the steps mentioned below: -

***Research***

Research phase includes a collection of information about target organization. It may be collected by dumpster diving, scanning websites of the organization, finding information on the internet, gathering information from employees of the target organization, etc.

***Select Target***

In the selection of target phase, attacker select the target among other employees of an organization. A frustrated target is more preferred as it will be easy to reveal information from him.

***Relationship***

Relationship phase includes creating a relationship with the target in the way that he could not identify the intention in fact target will be trusting the attacker. More Trust level between target and attacker will be easier to reveal information.

***Exploit***

Exploit of relationship by a collection of sensitive information such as Username, Passwords, network information, etc.

## Social Engineering Techniques

### Types of Social Engineering

Social Engineering attacks can be performed by different techniques. Different social engineering attack techniques are classified into the following types: -

***Human-based Social Engineering***

Human-based Social Engineering includes one-to-one interaction with the target. Social Engineer gathers sensitive information by tricking such as ensuring the trust, taking advantage of habits, behavior and moral obligation.

***1. Impersonation***

Impersonating is a human-based social engineering technique. Impersonation means pretending to be someone or something. Impersonating in Social engineering is pretending of an attacker to be a legitimate user or pretending to be an authorized person. This impersonating may be either personally or behind a communication channel such as while communicating with Email, telephone, etc.

Personal- impersonating is performed by identity theft, when an attacker has enough personal information about an authorized person, attacker gather information impersonating as a legitimate user providing the personal information of a legitimate user. Impersonating as Technical support agent asking for the credential is another way to impersonate and gather information.

***2. Eavesdropping and Shoulder Surfing***

Eavesdropping is a technique in which attacker is revealed information by listening to the conversation covertly. It does not only include Listening to conversations; it includes reading or accessing any source of information without being notified.

Shoulder Surfing is defined in the section of Footprinting in this workbook. Shoulder Surfing, in short, a method of gathering information by standing behind a target when he is interacting with sensitive information.

***3. Dumpster Diving***

Dumpster Diving is the process of looking for treasure in trash. This technique is older but still effective. It includes accessing the target's trash such as printer trash, user desk, company's trash for finding phone bills, contact information's, financial information, source codes, and other helpful material.

### 4. *Reverse Social Engineering*

A Reverse social engineering attack requires the interaction of attacker and victim, where an attacker convinces the target of having a problem or might have an issue in future. If the victim is convinced, he will provide the information required by the attacker. Reverse social engineering is performed through the following steps: -

a. An attacker damages the target's system or identifies the known vulnerability.
b. Attacker advertises himself as an authorized person for solving that problem.
c. Attacker gains the trust of the target and obtains access to sensitive information.
d. Upon successful reverse social engineering, the user may often get the attacker for help.

### 5. *Piggybacking and Tailgating*

Piggybacking and Tailgating is similar technique. Piggybacking is the technique in which unauthorized person waits for an authorized person to gain entry in a restricted area, whereas Tailgating is the technique in which unauthorized person gain access to the restricted area by following the authorized person. By using Fake IDs and close following while crossing the checkpoint, tailgating become easy.

### *Computer-based Social Engineering*

There are different ways to perform Computer-based Social Engineering including Pop-up windows requiring login credentials, Internet Messaging and Emails such as Hoax letters, Chain letters, and Spam.

### *Phishing*

Phishing process is a technique in which Fake Email which looks like legitimate email is sent to a target host. When the recipient opens the link, he is enticed for providing information. Typically, readers are redirected to the fake webpage that resembles an official website. The user provides all sensitive information to a fake website believing as an official website because of its resemblance.

### *Spear Phishing*

Spear Phishing is a type of phishing which is focused on a target. This is a targeted phishing attack on an individual. Spear phishing generates higher response rate as compared to a random phishing attack.

### *Mobile-based Social Engineering*

### 1. *Publishing Malicious Apps*

In Mobile-based Social Engineering, a technique is by Publishing malicious application on application store to be available for download on a large scale. These malicious applications are normally a replica or similar copy of a popular application. For example, an attacker may develop a malicious application for Facebook. The user instead of

downloading an official application may accidentally or intentionally download this third-party malicious application. When a user signs in, this malicious application will send the login credentials to the remote server controlled by the attacker.

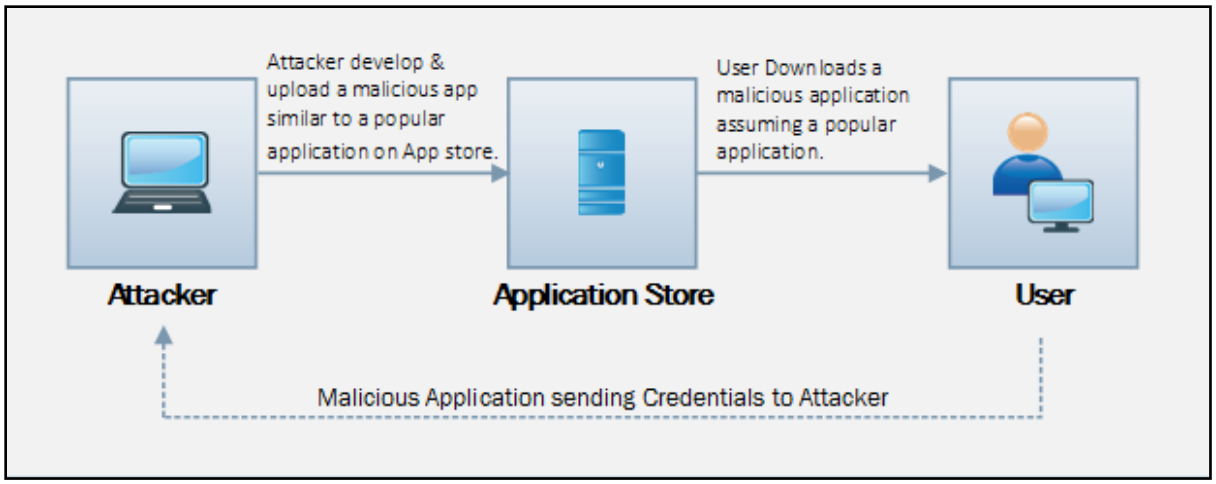



*Figure 9-01 Publishing Malicious Application*

### 2. *Repackaging Legitimate Apps*

In Mobile-based Social Engineering, another technique is by repacking a legitimate application with malware. Attacker initially downloads a popular, most in-demand application from application store typically Games and Anti-viruses are most commonly used. Attacker repackages the application with malware and uploads it to a third-party store. The user may not be aware of the availability of that application on application store or get a link for free download of a paid application. Instead of downloading from an official application from a trusted store, a user accidentally or intentionally downloads this repackaged application from the third-party store. When a user signs in, this malicious application will send the login credentials to the remote server controlled by the attacker.

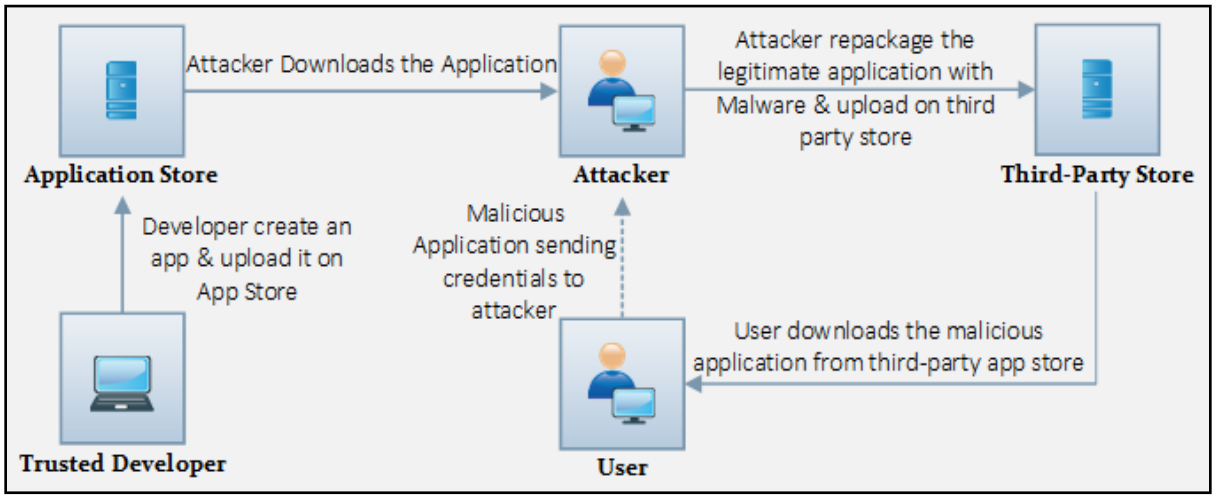



*Figure 9-02 Repackaging Legitimate Application*

### 3. *Fake Security Apps*

Similar to above technique, an attacker may develop a fake security application. This security application may be download by a pop-up window when the user is browsing website on the internet.

**Insider Attack**

Social Engineering is not all about a third person gathering information about your organization. It may be an insider, an employee of your organization having privileges or not, spying on your organization for malicious intentions. An insider attack is those attacks which are conducted by these insiders. These insiders may be supported by the competitor of an organization. A competitor may support a person in your organization for revealing sensitive information's and secrets.

Other than spying, Insider may have the intention of taking revenge. A disgruntled person in an organization may compromise the confidential and sensitive information to take revenge. An employee may be a disgruntled person when he not satisfied with the management, trouble facing him from the organization, demotion or going to be terminated.

## Impersonation on Social Networking Sites

**Social Engineering Through Impersonation on Social Networking Sites**

Impersonation on social networking site is very popular, easy, and interesting. The malicious user gathers personal information of a target from different sources mostly from social networking sites. Gathered information includes Full name, Recent profile picture, date of birth, residential address, email address, contact details, professional details, educational details as much as he can.

After gathering the information about a target, the attacker creates an account that is exactly the same with the account on the ocial networking site. This fake account is then introduced to friends and groups joined by the target. Usually, people do not investigate too much when they get a friend request, and when they find accurate information, they will definitely accept the request.

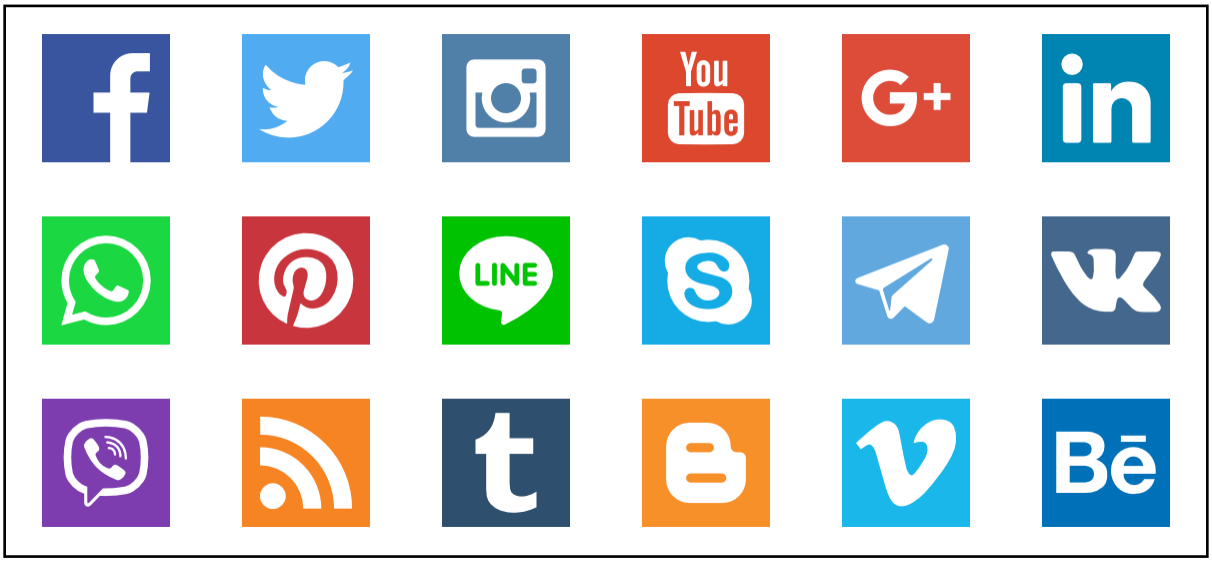



*Figure 9-03 Social Networking Sites*

Once the attacker joined the social media group where a user shares his personal and organizational information, he will get updates from groups. An attacker can also communicate with the friends of the target user to convince them to reveal information.

**Risks of Social Networking in a Corporate Networks**

A social networking site is not secured enough as a corporate network secures the authentication, identification, and authorization of an employee accessing the resources. The major risk of social networking is its vulnerability in the authentication. An attacker may easily manipulate the security authentication and create a fake account to access the information.

An employee while communicating on social networking may not take care of sensitive information. Any employee may accidentally, and intentionally reveal the information which may be helpful for the one he is communication with, or the third person monitoring his conversation. It requires a need for a strong policy against data leakage.

## Identity Theft

**Identify Theft Overview**

Identity theft is stealing the identification information of someone. Identity theft is popularly used for frauds. Anyone with malicious intent may steal your identification by gathering documents such as utility bills, personal information and other relevant information and create a new ID card to impersonate someone. It is not all about an ID card; he may use this information to prove the fake identity and take advantage of it

**The process of Identity theft**

Identity theft process starts with the initial phase in which attacker is focused on finding all necessary, beneficial information including personal and professional information.

Dumpster Diving and by access the Desk of an employee is very effective technique. However, Social Engineering also work. The attacker will find Utility bills, ID cards, or Documents which will be helpful to get a fake ID card from an authorized issuing source such as Driving License office.

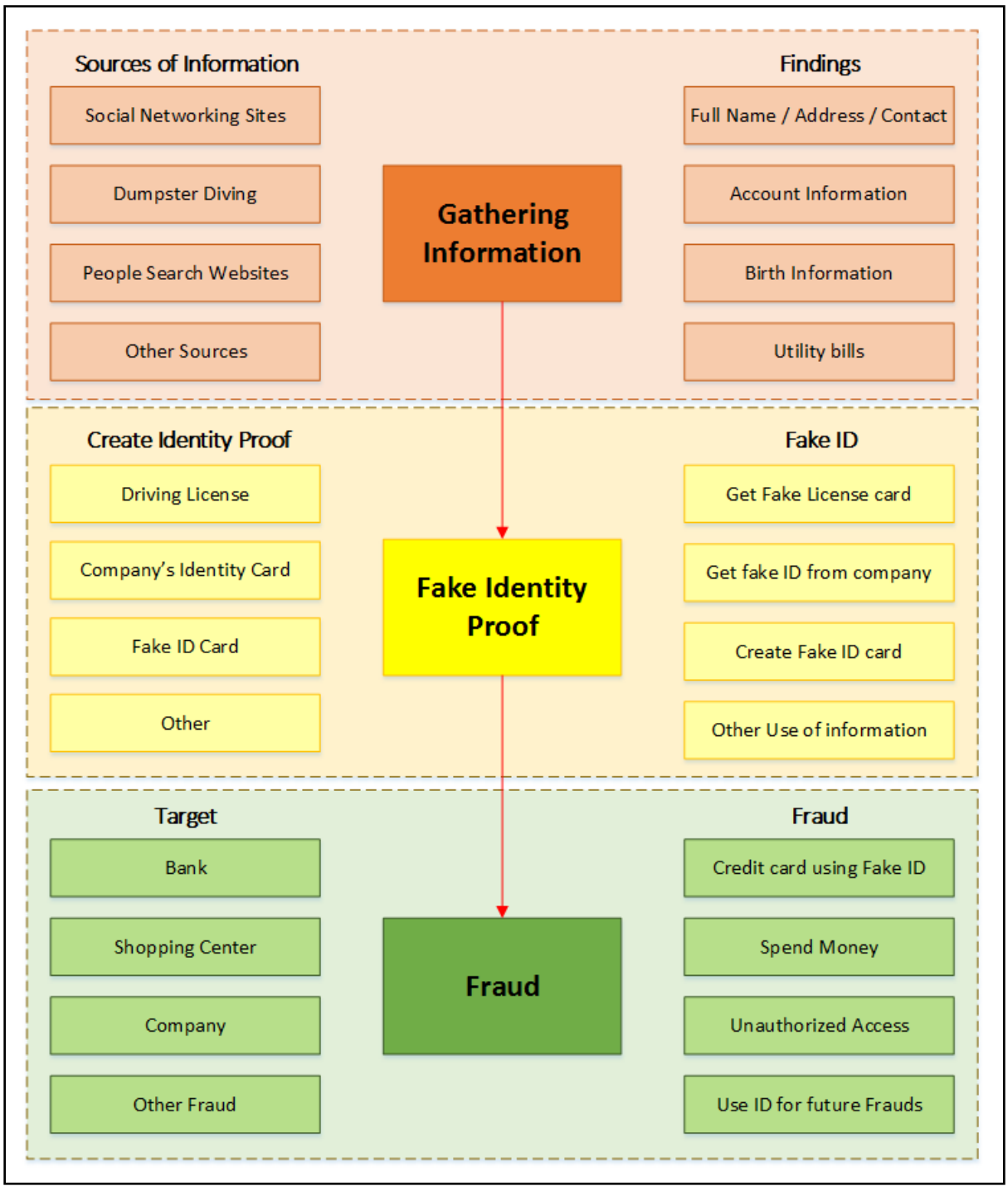



*Figure 9-04 Processes of Identity Theft*

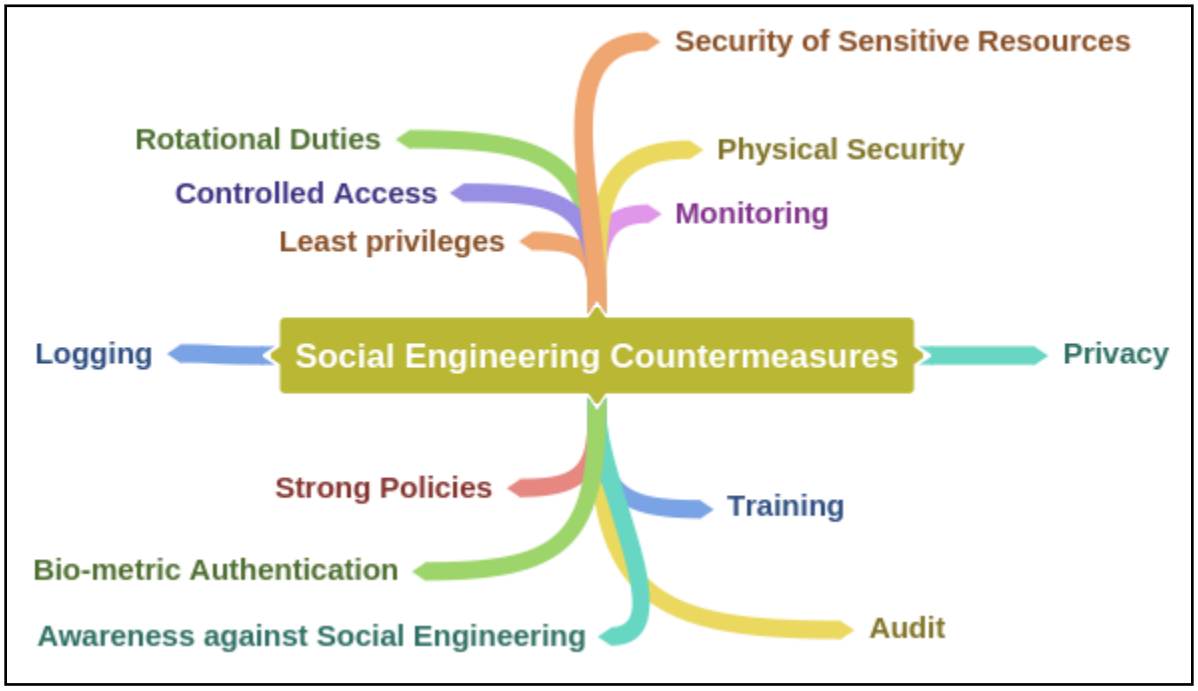
Once you get an ID from an authorized issuer such as Driving license centers, National ID card centers, Organization's administration department, you can take advantage of it. It is

not as easy; you will need utility bills to prove your ID, you have provided all required parameters to prove yourself. Once you pass this checkpoint, you get the access using the ID by impersonating legitimate employee.

### Social Engineering Countermeasures

Social Engineering attacks can be mitigated by several methods. Privacy in the corporate environment is necessary to mitigate shoulder surfing and dumpster diving threats. Configuring strong password, securing passwords, keeping them secret will protect against social engineering. Social networking is always a risk of information leakage, but now, social engineering is also becoming an important platform for an organization to use. Keep monitoring social networking platforms, logging, training, awareness and audit can effectively reduce the risk of social engineering attacks.

### Mind Map




## Lab 09-1: Social Engineering using Kali Linux

**Case Study:** We are using Kali Linux Social Engineering Toolkit to clone a website and send clone link to victim. Once Victim attempt to login to the website using the link, his credentials will be extracted from Linux terminal.

**Procedure:**

1. Open Kali Linux


*Figure 9-05 Kali Linux Desktop*

2. Go to Application

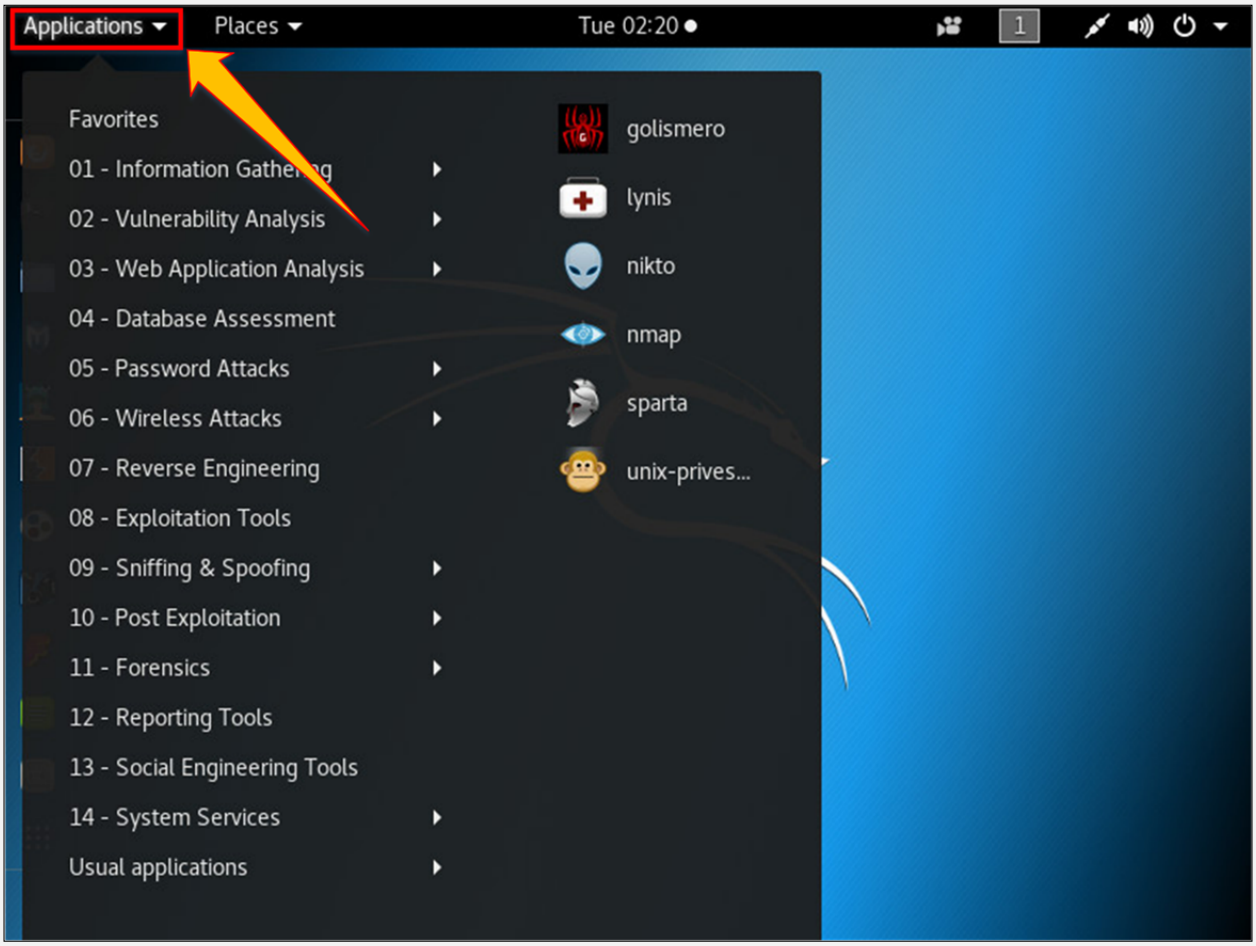



*Figure 9-06 Kali Linux Applications*

3. Click Social Engineering Tools
4. Click Social Engineering Toolkit

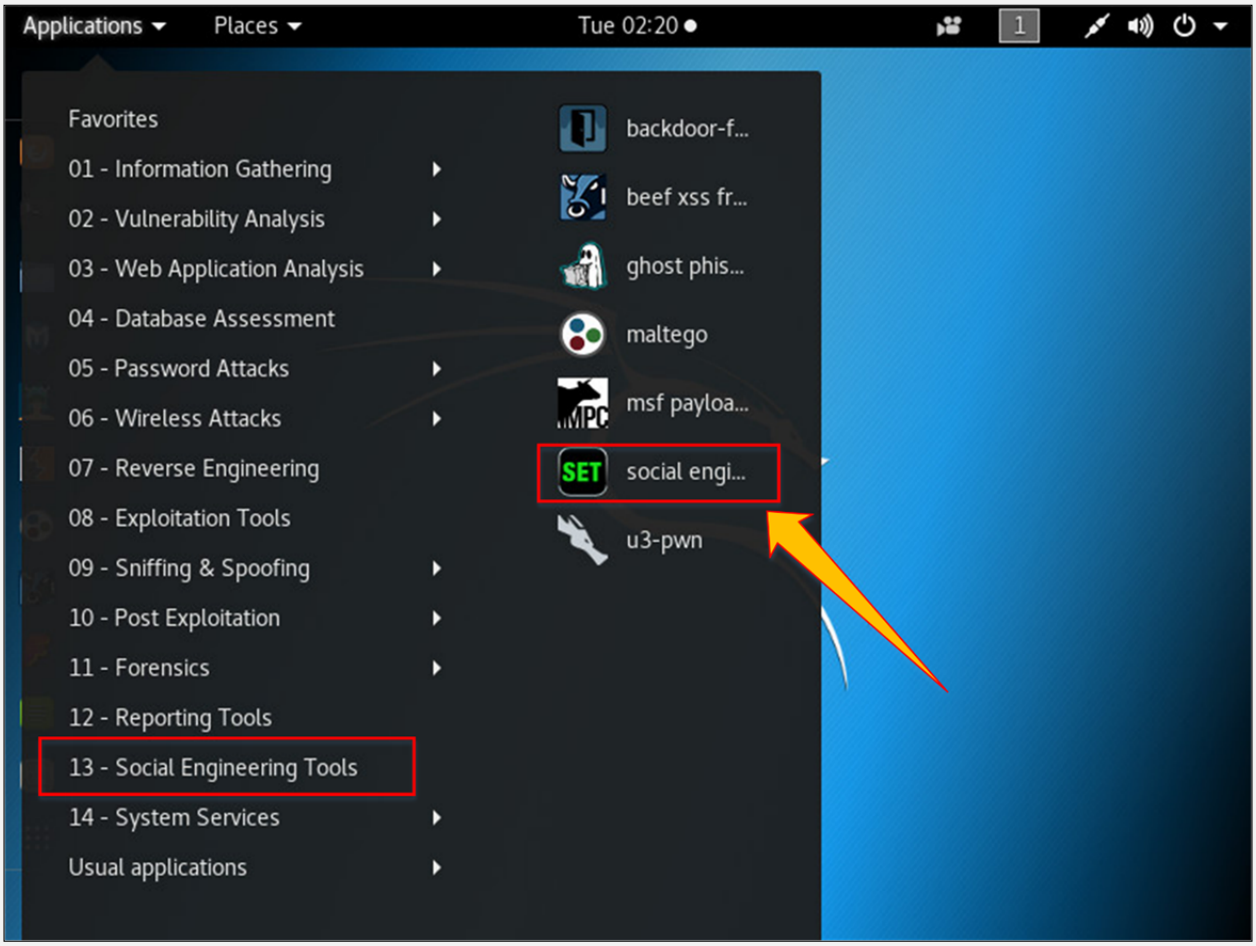



*Figure 9-07 Social Engineering Toolkit*

5. Enter "Y" to proceed.

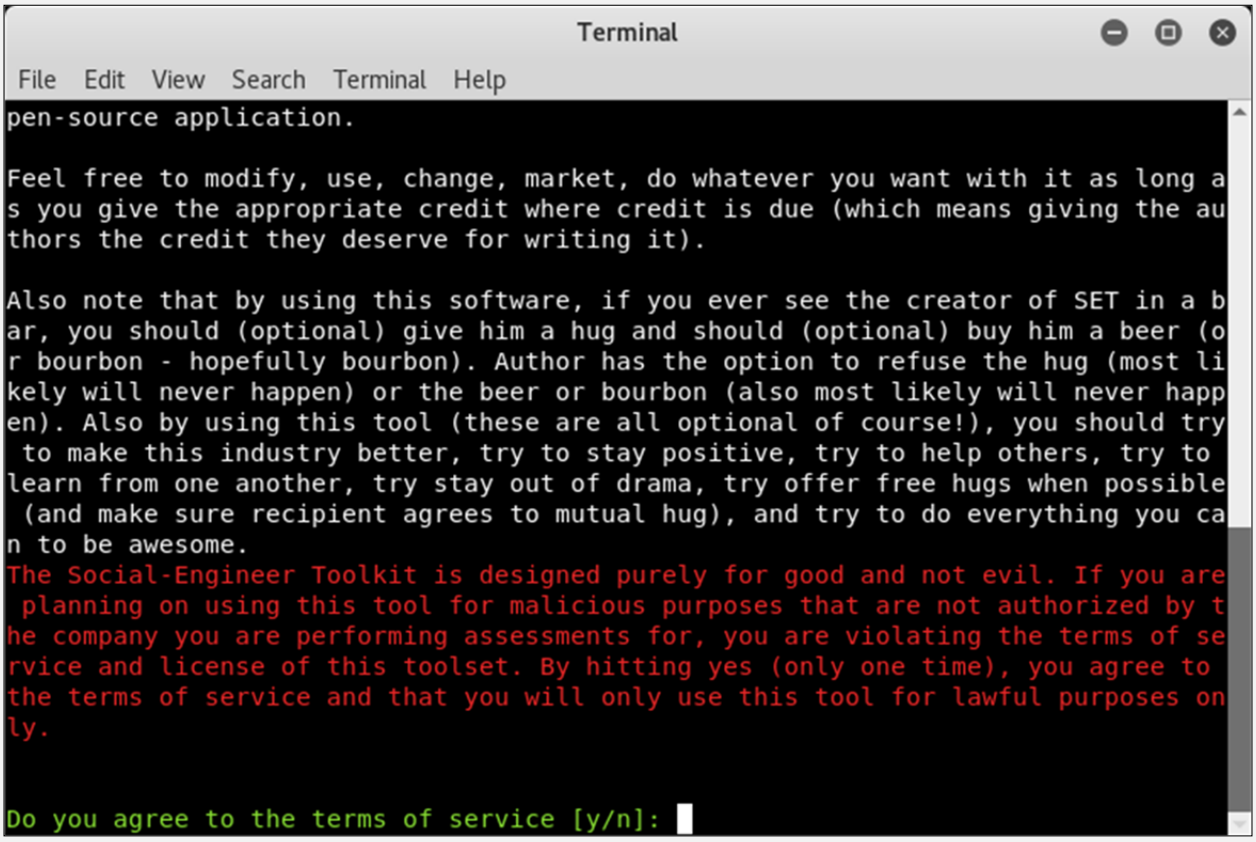



*Figure 9-08 Social Engineering Toolkit*

6. Type "1" for Social Engineering Attacks

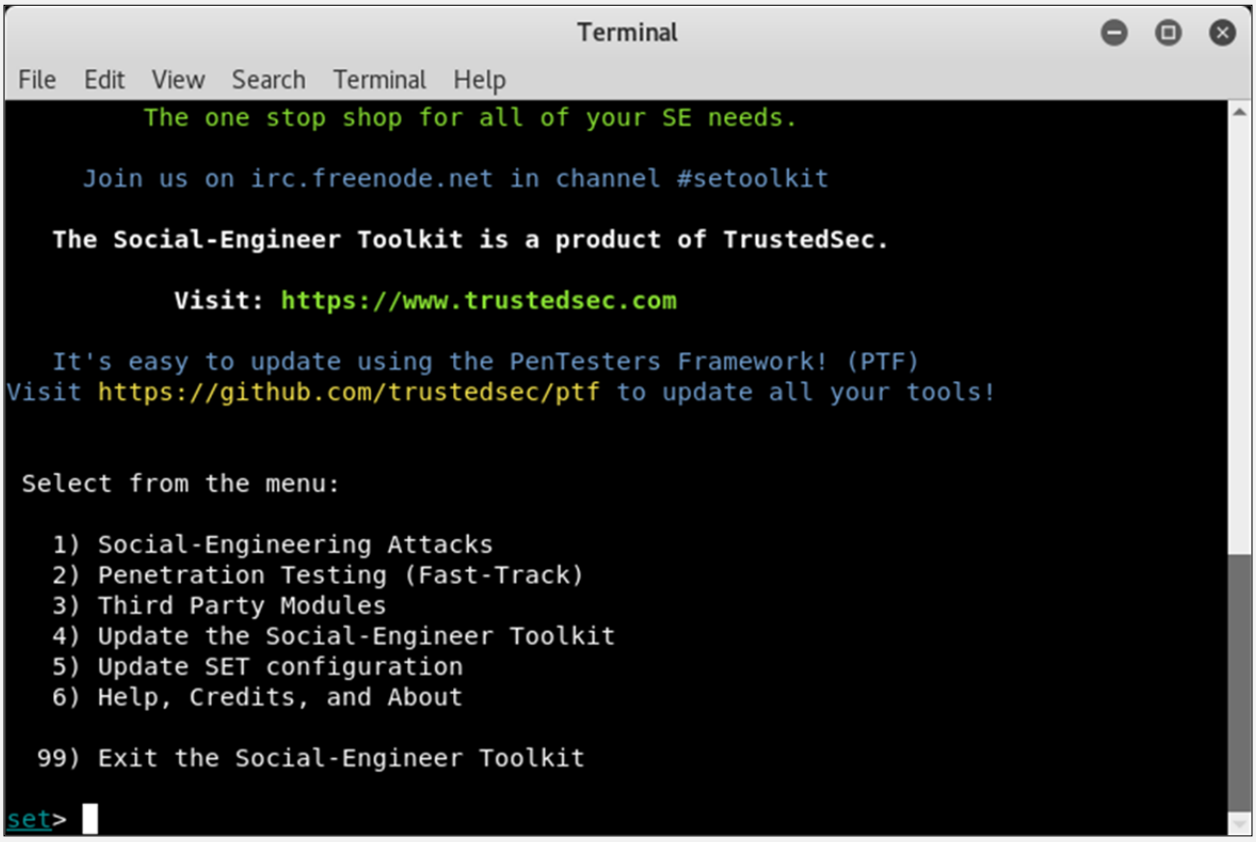



*Figure 9-09 Social Engineering Toolkit Menu*

7. Type "2" for website attack vector

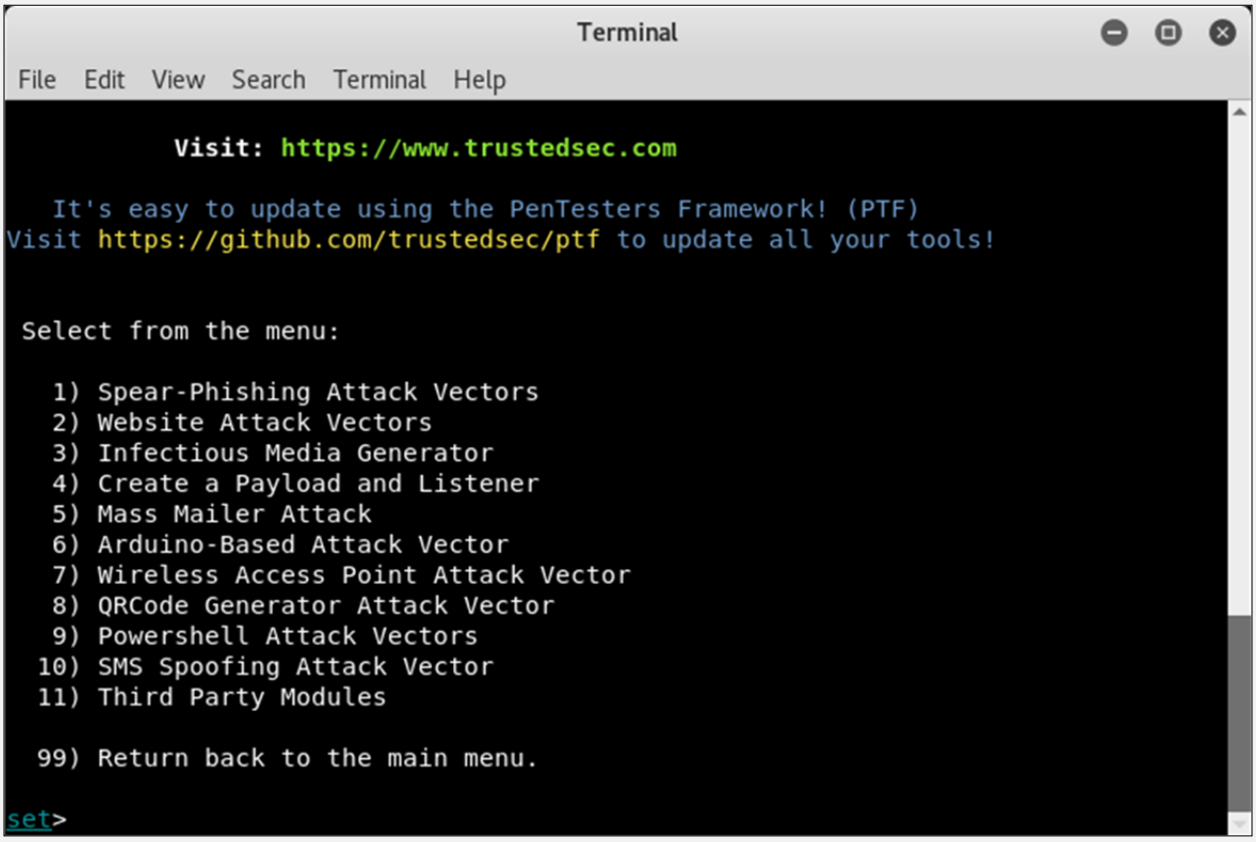



*Figure 9-10 Social Engineering Attack Menu*

8. Type "3" for Credentials harvester attack method

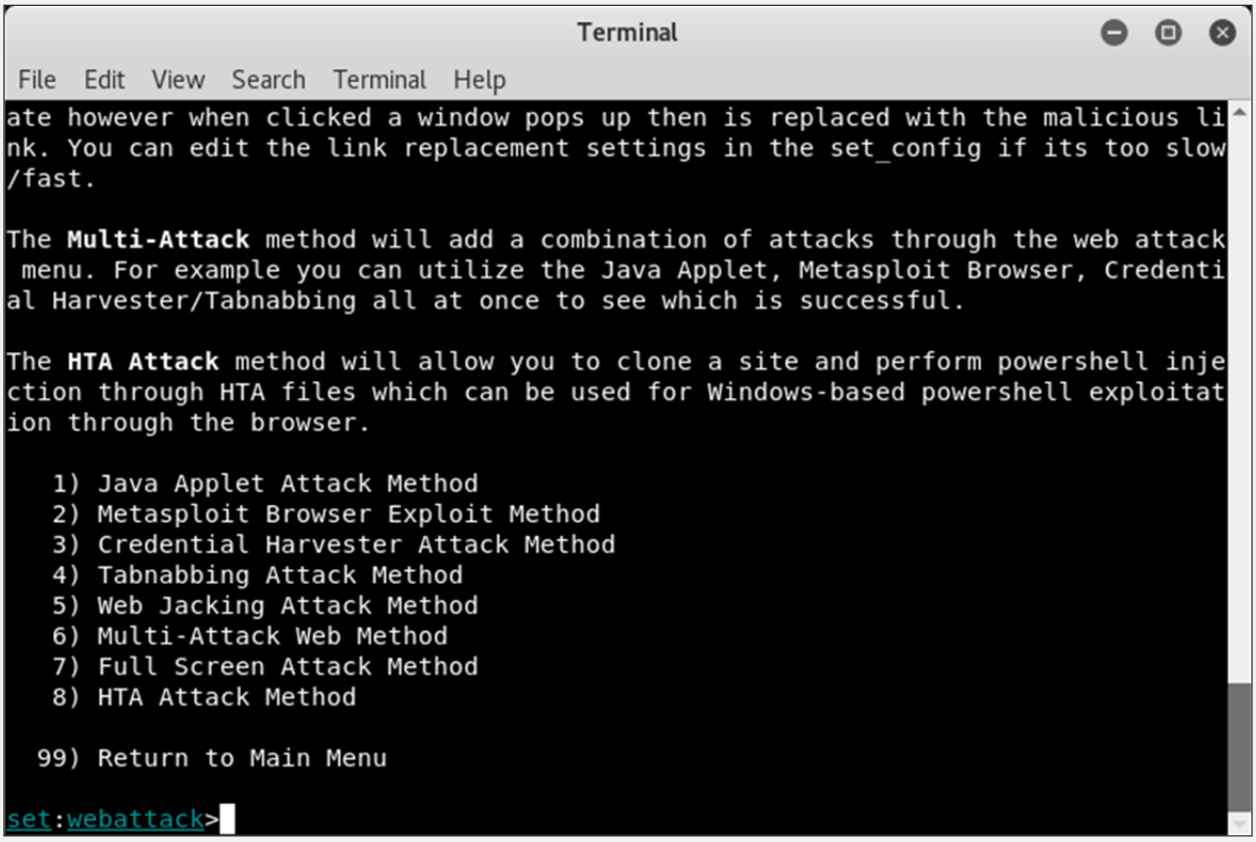



*Figure 9-11 Website Attack Vector Options*

9. Type "2" for Site Cloner

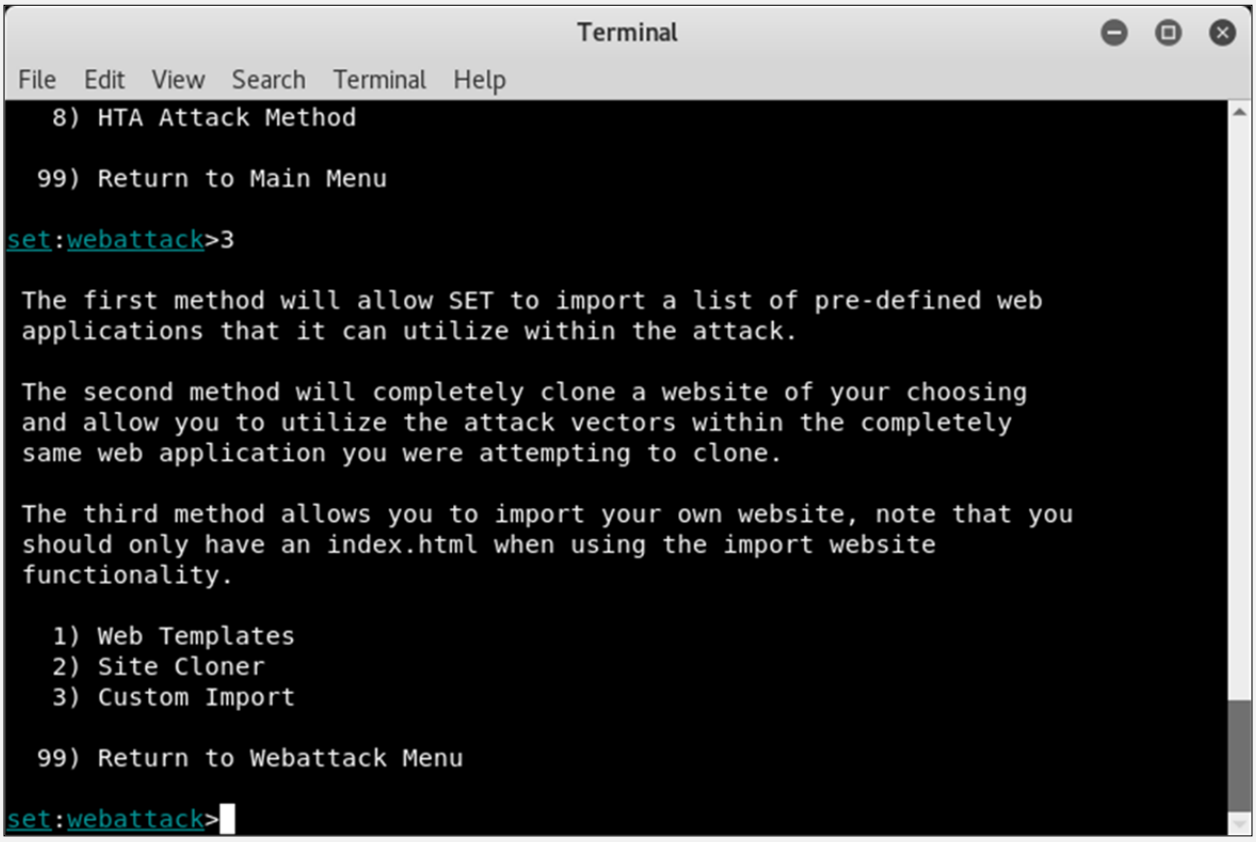



*Figure 9-12 Credentials harvester attack method*

10. Type IP address of Kali Linux machine ( 10.10.50.200 in our case).

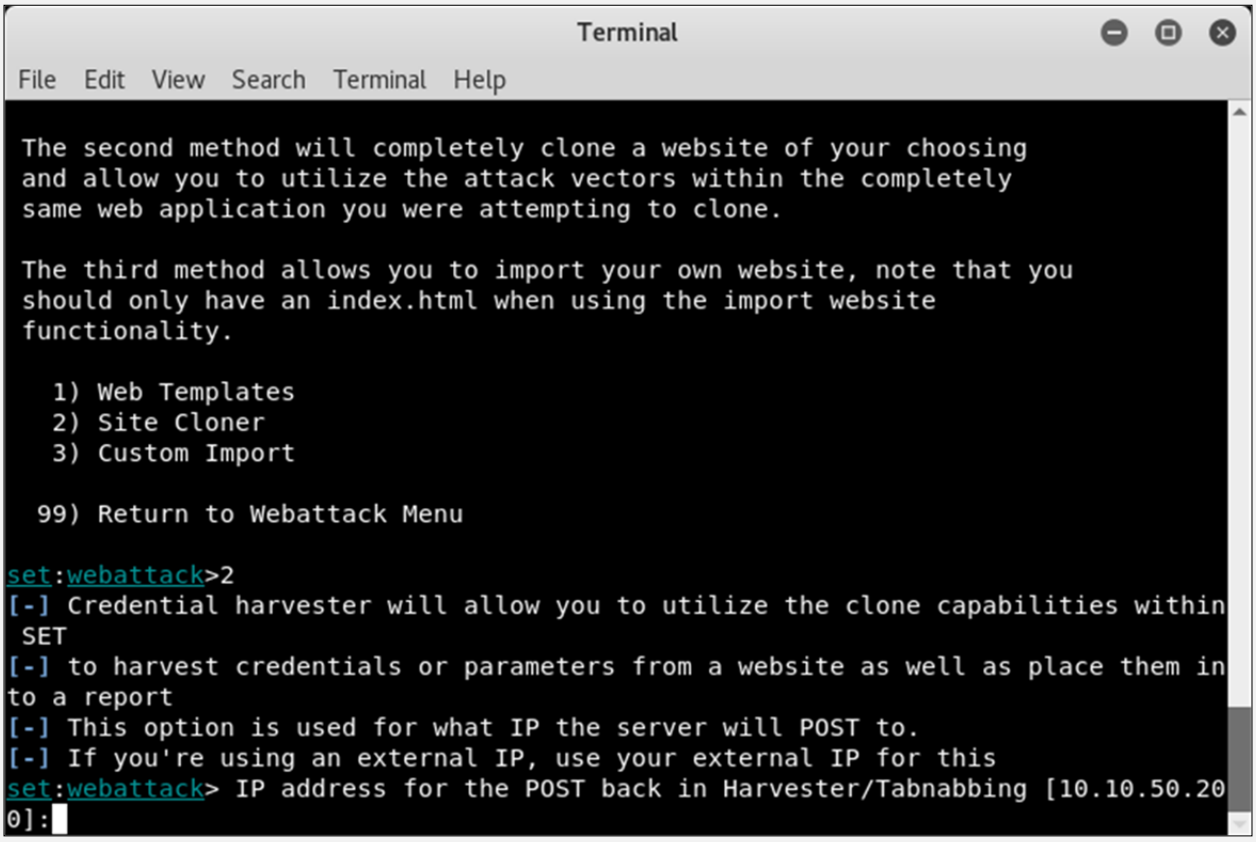



*Figure 9-13 Site Cloner*

11. Type target URL

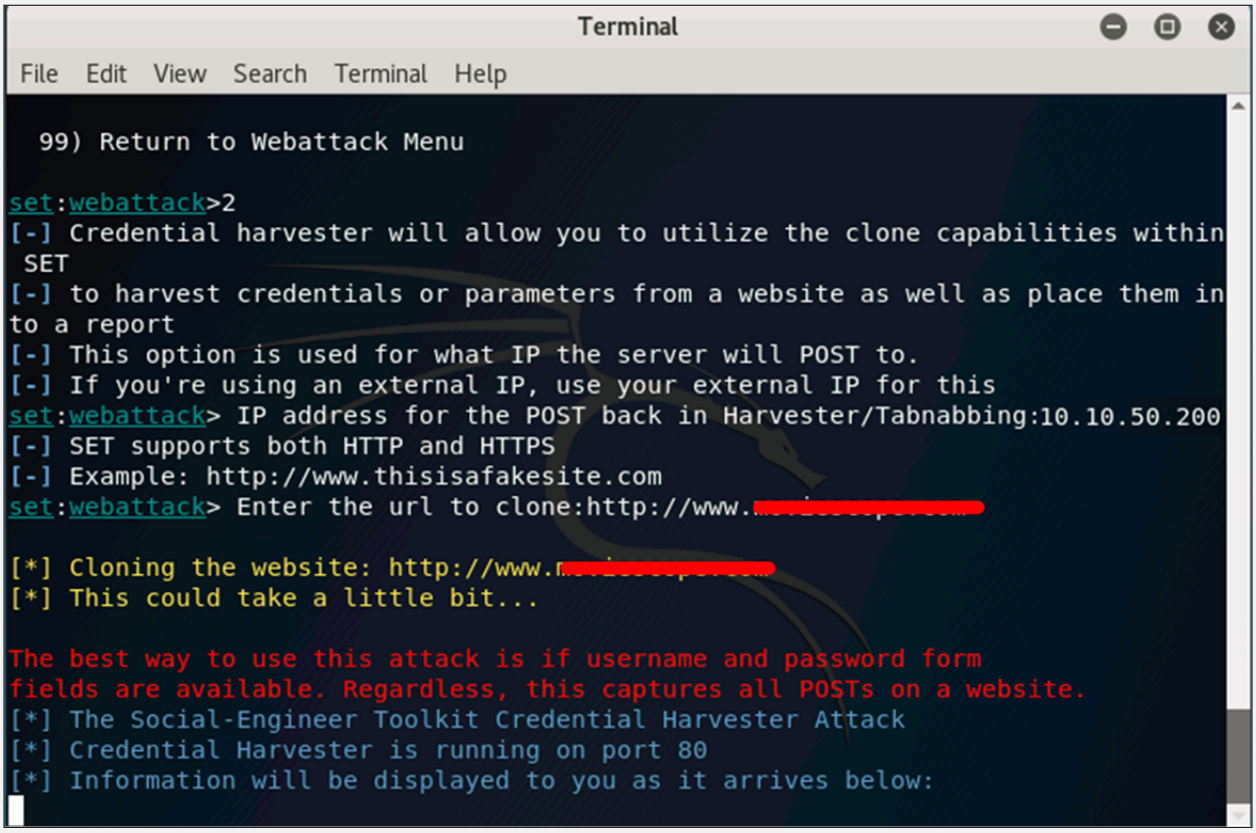



*Figure 9-14 Cloning*

12. Now, http://10.10.50.200 will be used. We can use this address directly, but it is not an effective way in real scenarios. This address is hidden in a fake URL and forwarded to the victim. Due to cloning, the user could not identify the fake website unless he observes the URL. If he accidentally clicks and attempts to log in, credentials will be fetched to Linux terminal. In the figure below, we are using http://10.10.50.200 to proceed.
13. Login using username and Password

Username: admin

Password: Admin@123

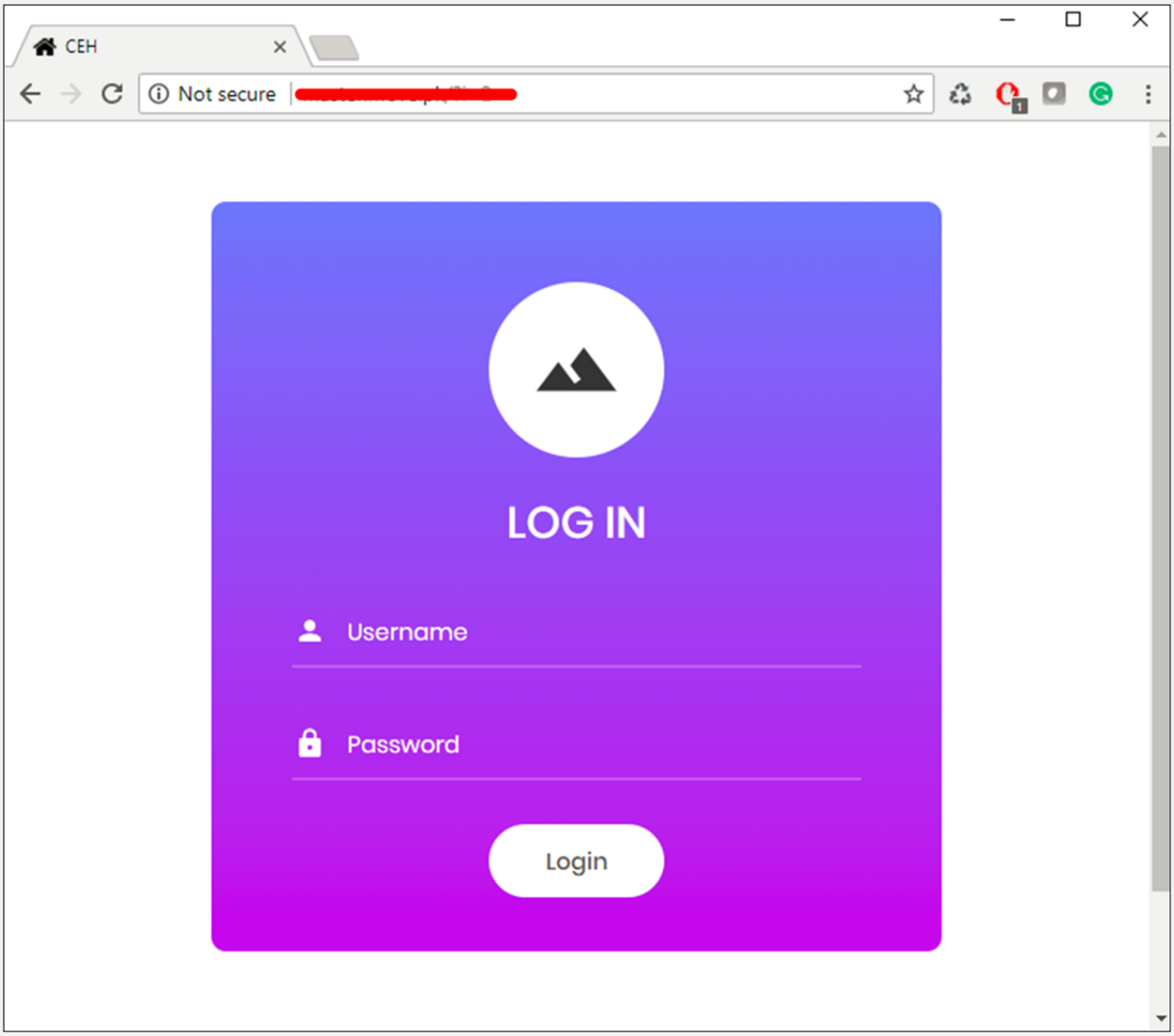



*Figure 9-15 Logging into the cloned website*

14. Go back to Linux terminal and observe.

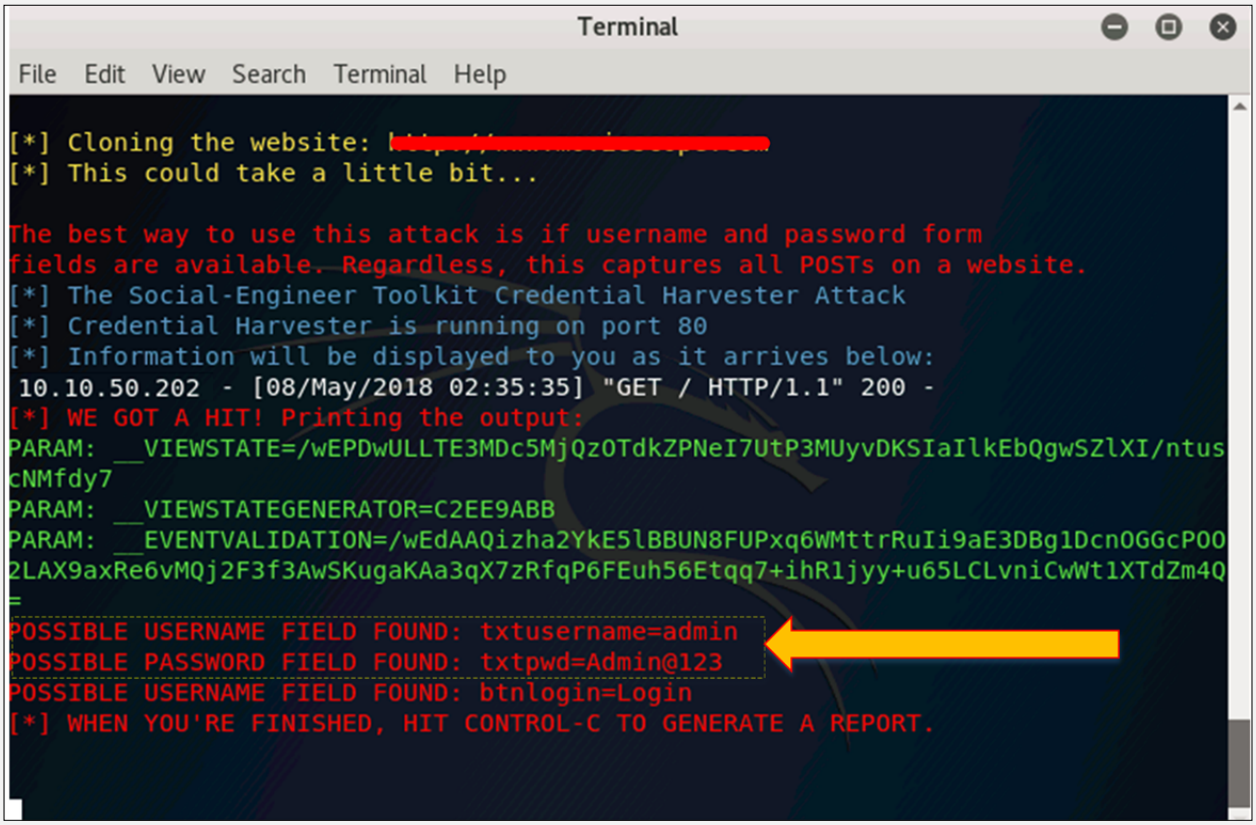



*Figure 9-16 Extracted Credentials*

Username admin and password is extracted. If the user types it correctly, exact spelling can be used. However, you will get the closest guess of user ID and password. The victim will observe a page redirect, and he will be redirected to a legitimate site where he can re-attempt to log in and browse the site.