# QRCode Generator Attack Vector from the Social-Engineer Toolkit (SET)

**Execution Steps:**

1. **Launched SEToolkit:**
   - `sudo su.`
   - `Setoolkit`
   - `[1] Social-Engineering Attacks`
   - `[8] QRCode Generator Attack Vector`
   - `Opening the root folder contents`

## ***STEPS:***

1. **Launch Toolkit:**
   Open terminal → `sudo su` → `setoolkit`

2. **Navigate Menus:**
   Select → `[1] Social-Engineering Attacks` → `[8] QRCode Generator Attack Vector`

3. **Enter Phishing URL:**
   Provide a fake login page URL (e.g., Instagram clone via SET's Credential Harvester)

4. **QR Code Generated:**
   File saved at `/root/.set/reports/qrcode_attack.png`

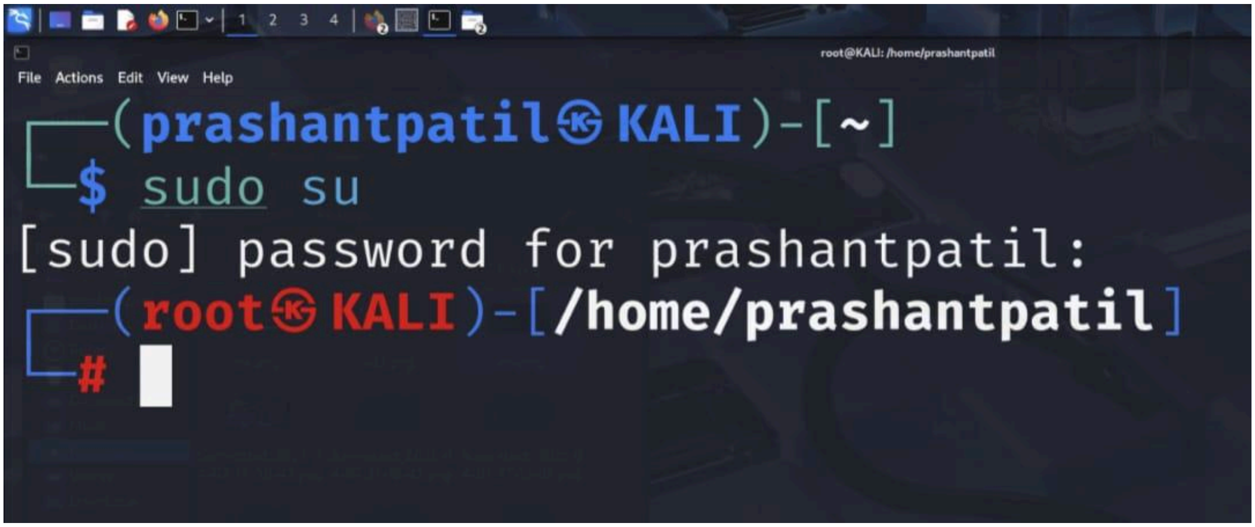
5. **Access QR Code:**
   Use `cd /root/.set/reports/` → Open with `sudo open qrcode_attack.png`

6. **Deploy QR Code:**
   Embed in posters (e.g., “Free Wi-Fi”) to attract users

7. **Result:**
   On scanning, user is redirected to a realistic phishing site, capturing login details

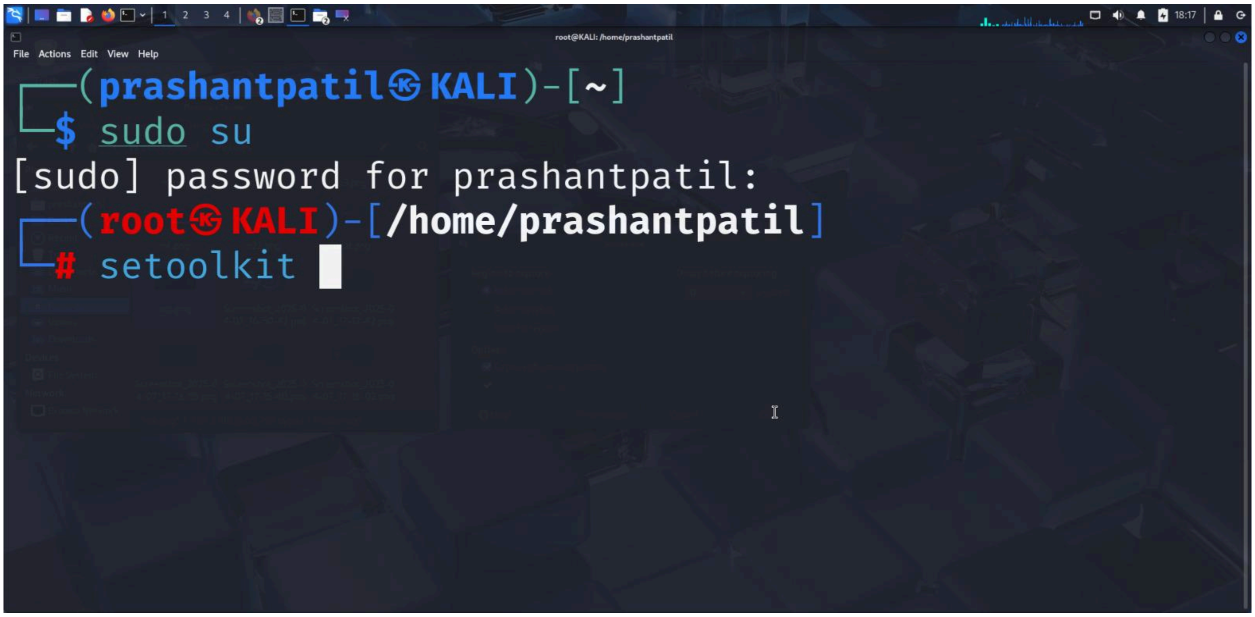
***Step 1:***

a) Using sudo su elevates you to the root user, giving you full administrative privileges in a single session. This saves time by eliminating the need to type sudo before every command.



```
┌──(prashantpatil㉿KALI)-[~]
└─$ sudo su
[sudo] password for prashantpatil:
┌──(root㉿KALI)-[/home/prashantpatil]
└─#
```

b) When you type setoolkit and hit enter, the Social-Engineer Toolkit initializes and displays a banner with tool credits and warnings. You're then presented with a numbered main menu offering different social engineering attack vectors.

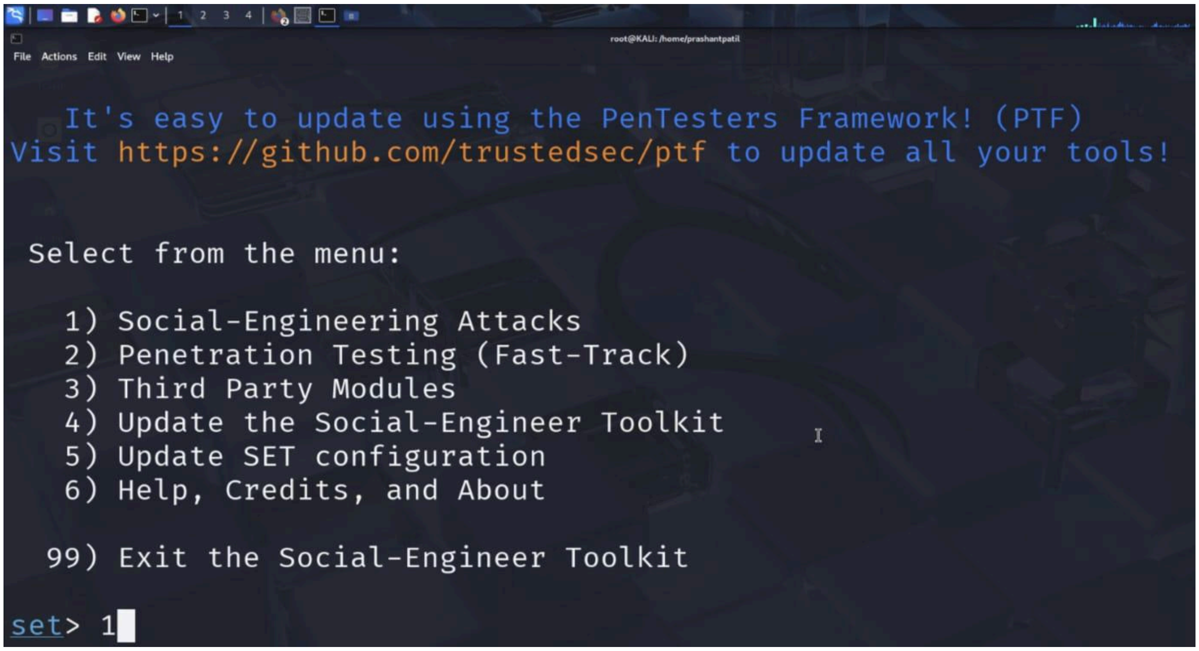


```
┌──(prashantpatil㉿KALI)-[~]
└─$ sudo su
[sudo] password for prashantpatil:
┌──(root㉿KALI)-[/home/prashantpatil]
└─# setoolkit
```

***Step2:***

a) After launching SEToolkit, selecting `”Social-Engineering Attacks”` from the main menu opens.

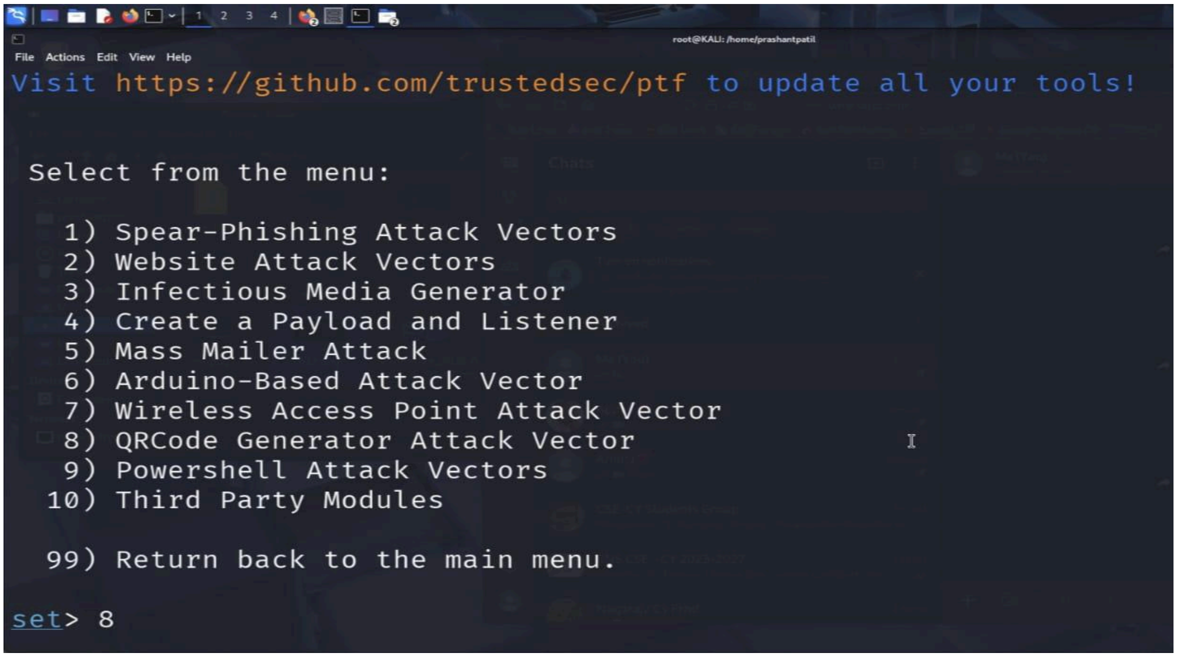
a list of powerful attack methods like *phishing, website cloning, and QR code generation*. This section is designed to simulate real-world scenarios that target human behavior.



```
   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
```

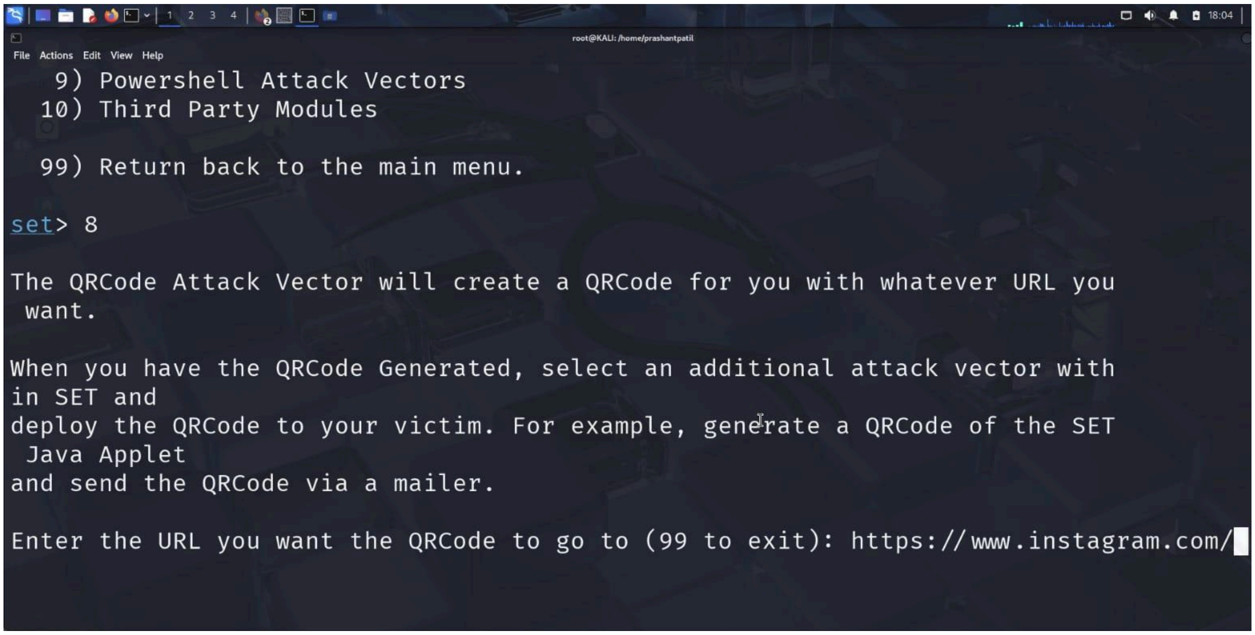
***Step3:***

a) Upon selecting the **`[8] QRCode Generator Attack Vector`** from the Social-Engineering Attacks menu, SET prompts you to input a URL that the QR code should redirect to.



```
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> 8
```

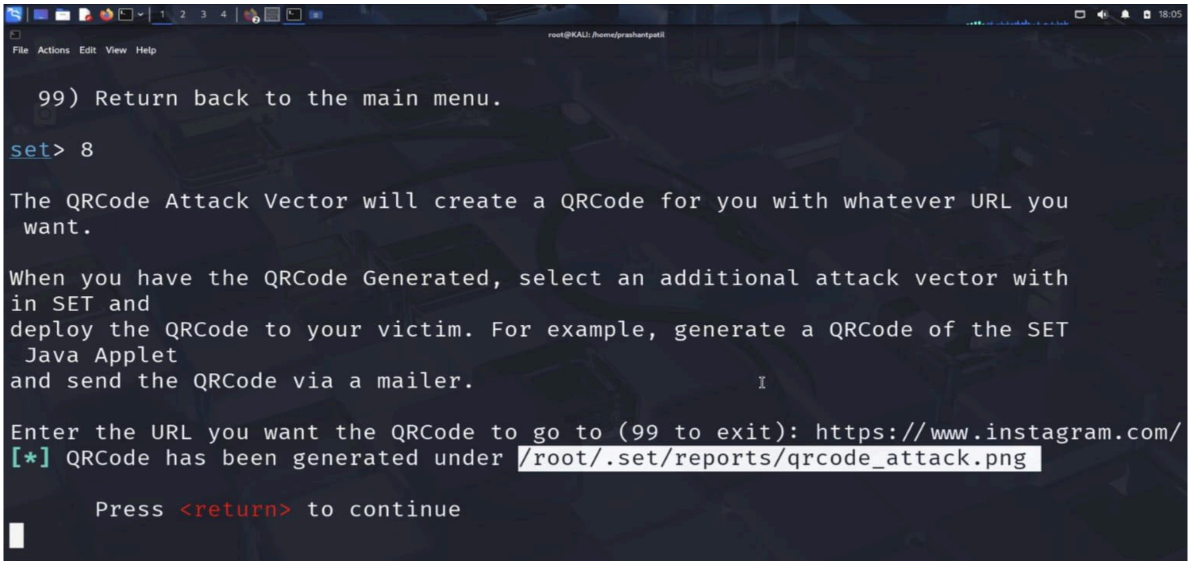
b) In this case, the Instagram URL is being entered for demonstration purposes. To utilize the tool effectively, a fake website URL must be provided—one that is specifically designed for phishing simulation. This website should closely replicate the appearance and functionality of the original Instagram site to increase the likelihood of user interaction.



```
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 8

The QRCode Attack Vector will create a QRCode for you with whatever URL you
 want.

When you have the QRCode Generated, select an additional attack vector with
in SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET
 Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): https://www.instagram.com/
```

***Step5:***

a) After generating the QR code, SEToolkit saves the file in a root directory that isn't directly accessible through the file explorer. Due to permission restrictions, the folder must be accessed via the terminal using elevated privileges. Users can either view the file with sudo or move it to a user-accessible location for easier access.

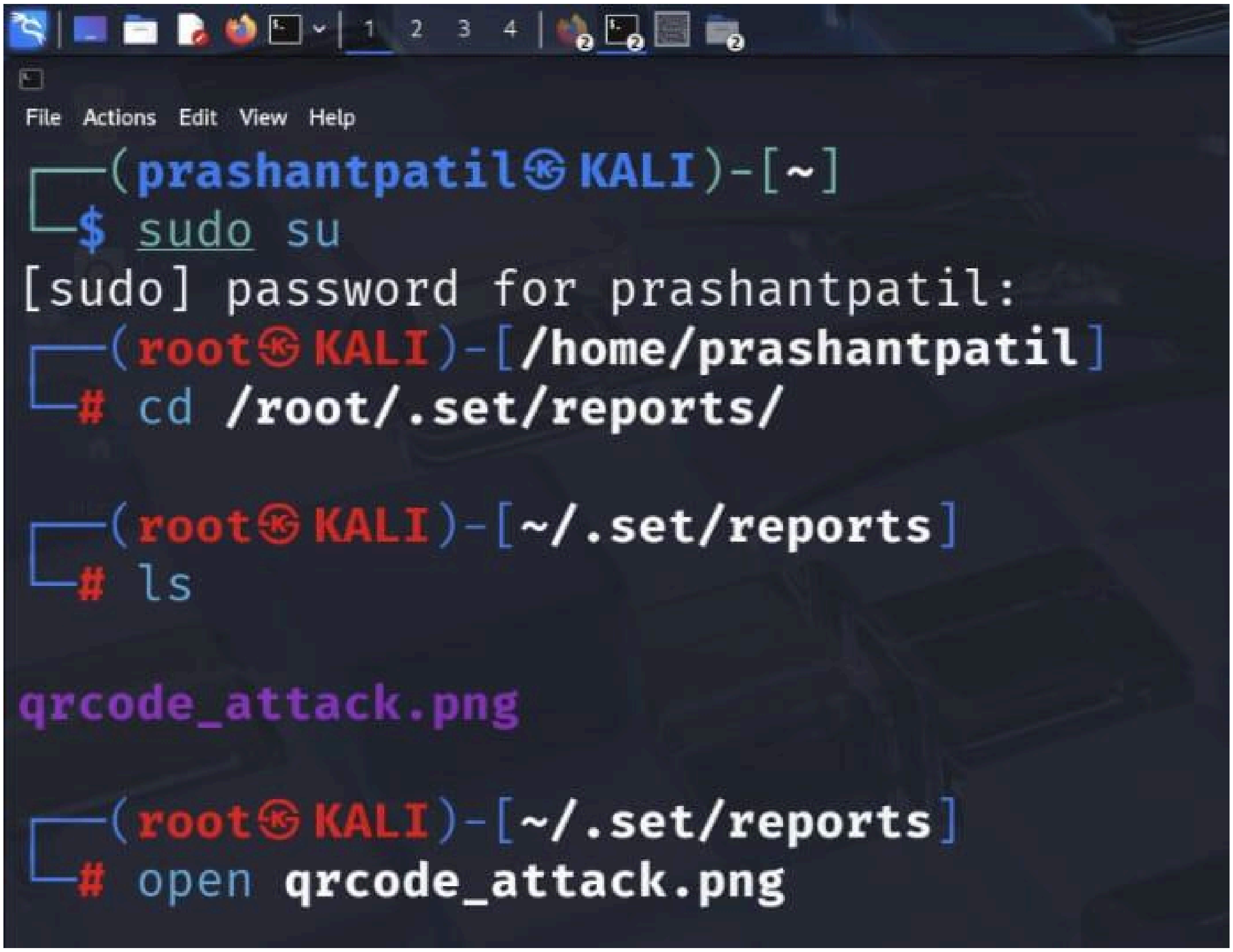


```
  99) Return back to the main menu.

set> 8

The QRCode Attack Vector will create a QRCode for you with whatever URL you
 want.

When you have the QRCode Generated, select an additional attack vector with
in SET and
deploy the QRCode to your victim. For example, generate a QRCode of the SET
 Java Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to (99 to exit): https://www.instagram.com/
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png

      Press <return> to continue
```

b) In this case, the generated QR code is saved at the path `/root/.set/reports/qrcode_attack.png`. It is important to note down both the directory path `/root/.set/reports/` and the file name `qrcode_attack.png` separately. This allows for accurate navigation and retrieval of the file using terminal commands with root privileges

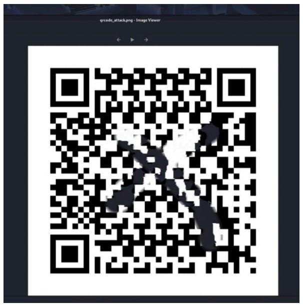
***Step6:*** *open new terminal again*

a) To access the generated QR code, navigate to the directory using the command `cd /root/.set/reports/` in the terminal. Since this is a root-protected path, elevated privileges are required. Once inside the directory, you can open `qrcode_attack.png` using an image viewer like `open` by running `open qrcode_attack.png`(if you are in root already,if not



```
┌──(prashantpatil㉿KALI)-[~]
└─$ sudo su
[sudo] password for prashantpatil:
┌──(root㉿KALI)-[/home/prashantpatil]
└─# cd /root/.set/reports/

┌──(root㉿KALI)-[~/.set/reports]
└─# ls

qrcode_attack.png

┌──(root㉿KALI)-[~/.set/reports]
└─# open qrcode_attack.png
```

Once the command is executed, the QR code image `qrcode_attack.png` will open in the system's default image viewer. This confirms that the file has been successfully generated and is ready for deployment in a phishing simulation. The QR code can now be scanned using any mobile device, redirecting the user to the embedded URL


qrcode_attack.png - Image Viewer