

3:- select type of attack
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.



The screenshot shows a Kali Linux terminal window with the Social-Engineer Toolkit (SET) interface. The terminal title is 'root@kali: ~/homekali'. The menu is displayed as follows:

```
File Actions Edit View Help
01100001011011100110010001110011001000
00001110100010110100101001001000000101
0100011010000110000101101110011010101
1100110010000001100110011011101110010
001000000110101011001101101001011011
1001100111001000000110100011010000110
0101001000000101001101101110110000101
101001011000010101100001011010000101
011011100110011011010100010110110011001
01011001011100100110000001010000110
111010111011011000101011010101000101
1101000100000001010100110100001110101
0110011011001100101010
[+] 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) 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> |
```

4:- Select Number 8 QRcode Generator Attack Vector

Enter The Url That Embedd in QRcode Scanner

```

root@kali: /home/fail
File Actions Edit View Help
01100110110011001100101010

[+] The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 3.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @hackingbase
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> 8

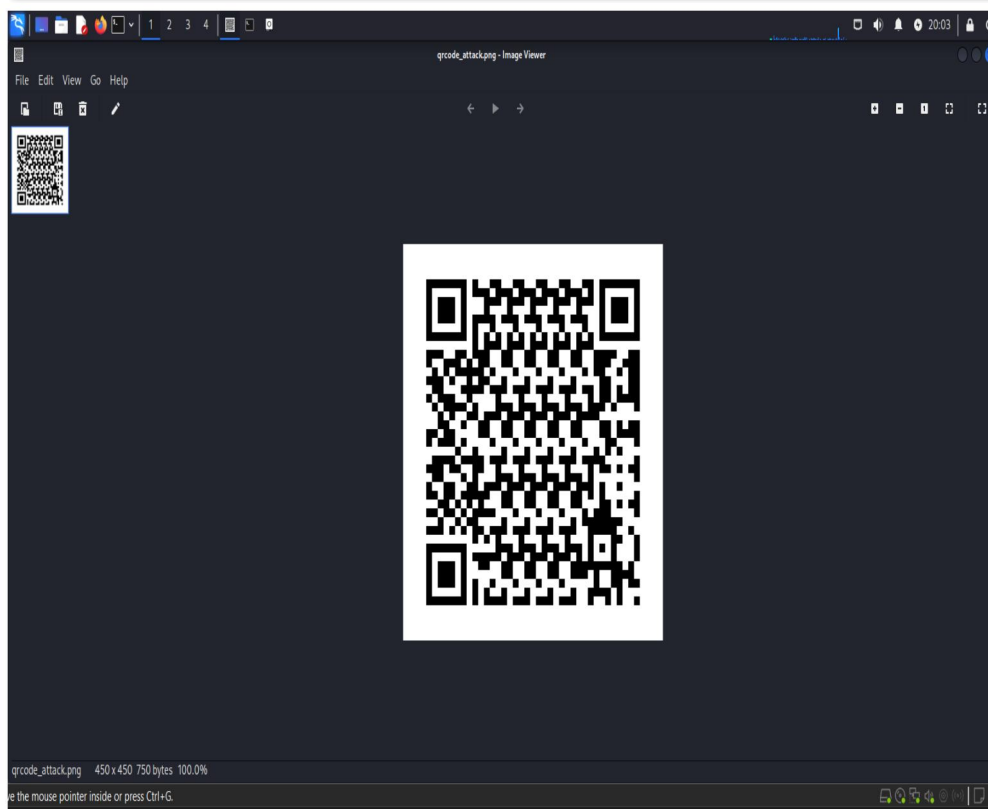
The QRCode Attack Vector will create a QRcode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within 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 <ret> to continue

```



CYBER THREAT INTELLIGENCE & INCIDENT RESPONSE

- After Generating the QRcode When Victim Scan the QRcode it will redirect to the URL That you insert in the QRcode.

Conclusion:

- The conducted social engineering attack successfully highlighted several critical vulnerabilities in human behavior and organizational security protocols. Through simulated phishing emails, pretexting scenarios, and other manipulation techniques, it was evident that even well-established systems can be compromised through human error or lack of awareness.