

CYBER THREAT INTELLIGENCE & INCIDENT RESPONSE

PRACTICAL - 9

DATE: 11-04-2025

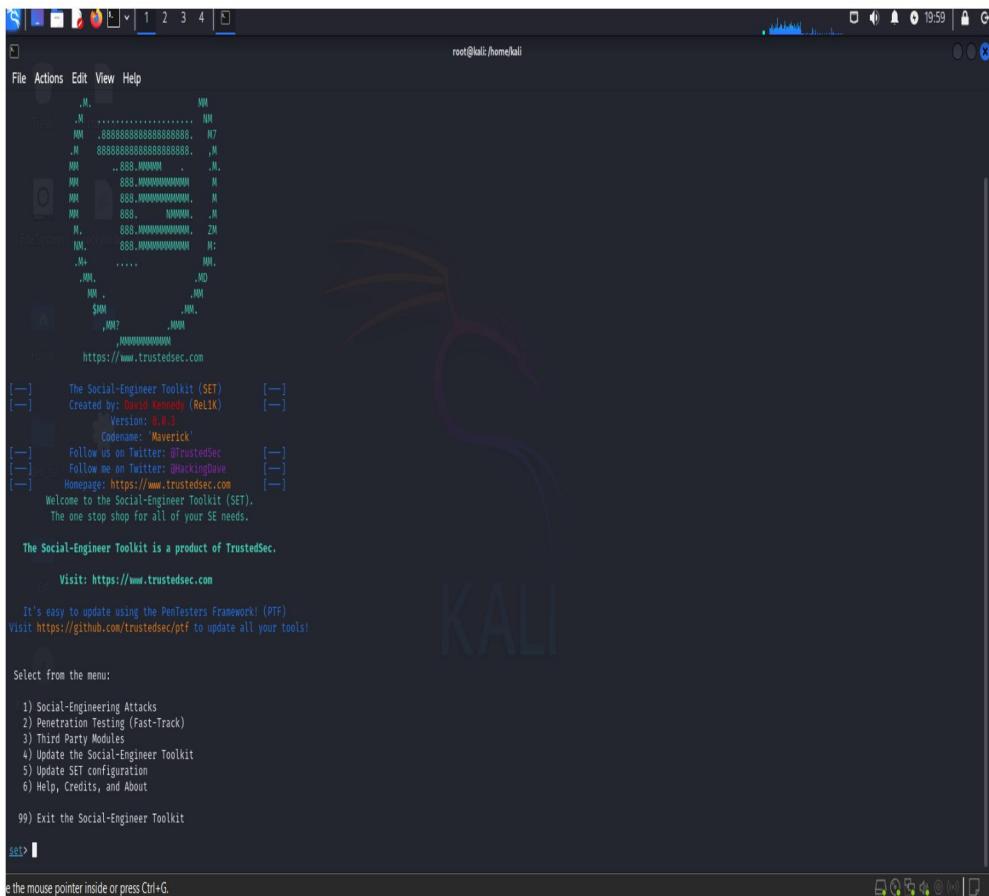
AIM: Conducting a social engineering attack and analyzing the results to identify vulnerabilities - II.

Steps:-

1: - Open Social Engg attack toolkit
Setoolkit

2:- Select From the menu
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



CYBER THREAT INTELLIGENCE & INCIDENT RESPONSE

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.

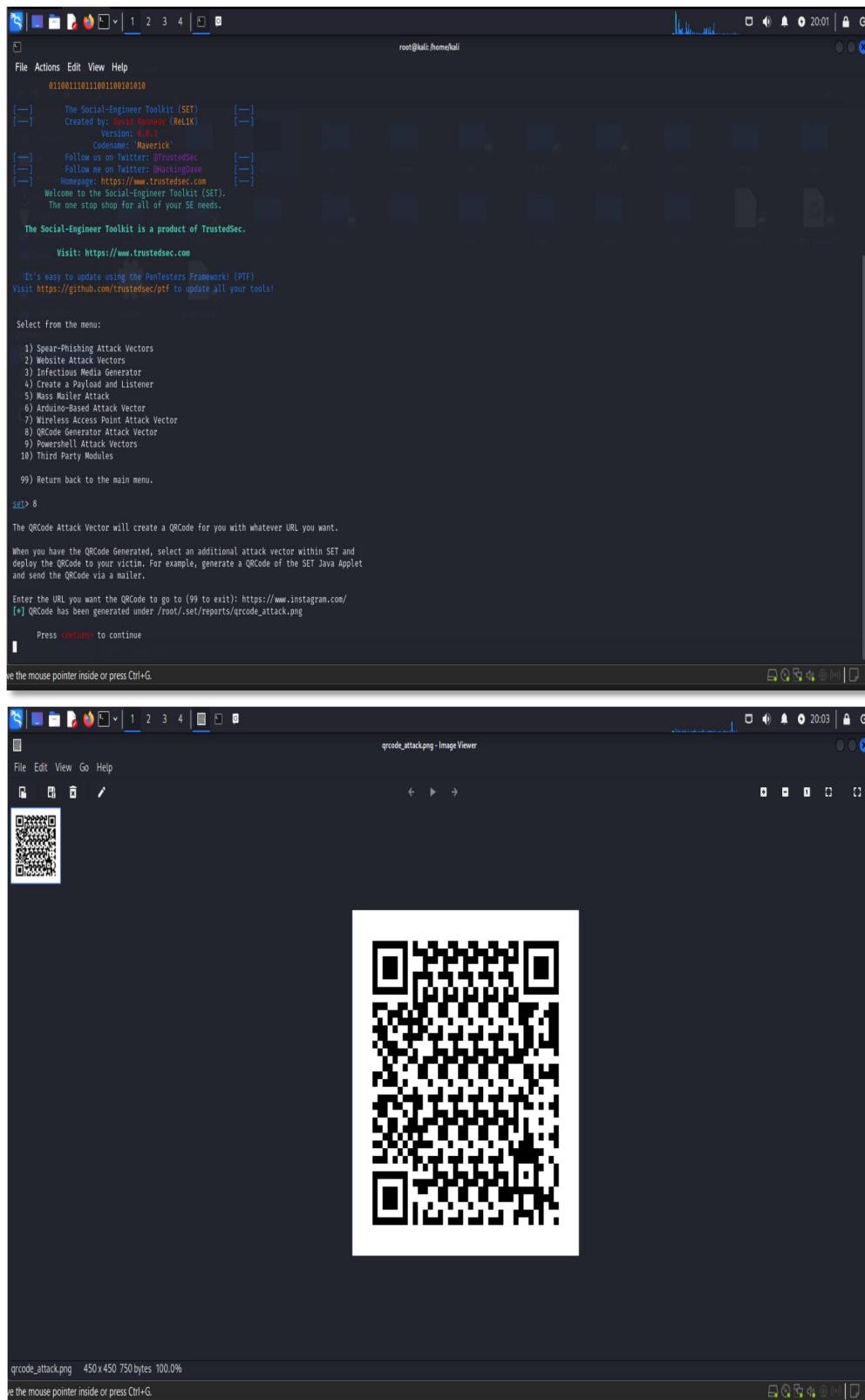
The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar indicates the session is root@kali:~/. The window displays the Social-Engineer Toolkit (SET) interface, which includes a binary string at the top, followed by the toolkit's logo and name, and various configuration options and links. Below this, there is a "Select from the menu:" prompt and the same list of attack vectors as the previous slide. The bottom of the window shows a command-line prompt (set>) and a status message about moving the mouse or pressing Ctrl+G.

```
0110000101101110011000011100110001000  
000011010010101010010010000000101  
0100011010000110000010101100110010101  
110011001000000110001200101011101010010  
0010000011101010111001010100010101  
1001100111001000000111001000110000010  
0100001000000100010101011001000010101  
01000101100000101011000001010101000101  
01100110011001101010010101011001001  
01010001011100100000010101000101001010  
1110011011110101011000101010100010100101  
110100001000000010101010100001110101  
011001110110101010101010101010101010101  
The Social-Engineer Toolkit (SET)  
Created by: David Kennedy (ReL1K)  
Version: 0.0.3  
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>
```

CYBER THREAT INTELLIGENCE & INCIDENT RESPONSE

4:- Select Number 8 QRcode Generator Attack Vector

Enter The Url That Embedd in QRcode Scanner



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.