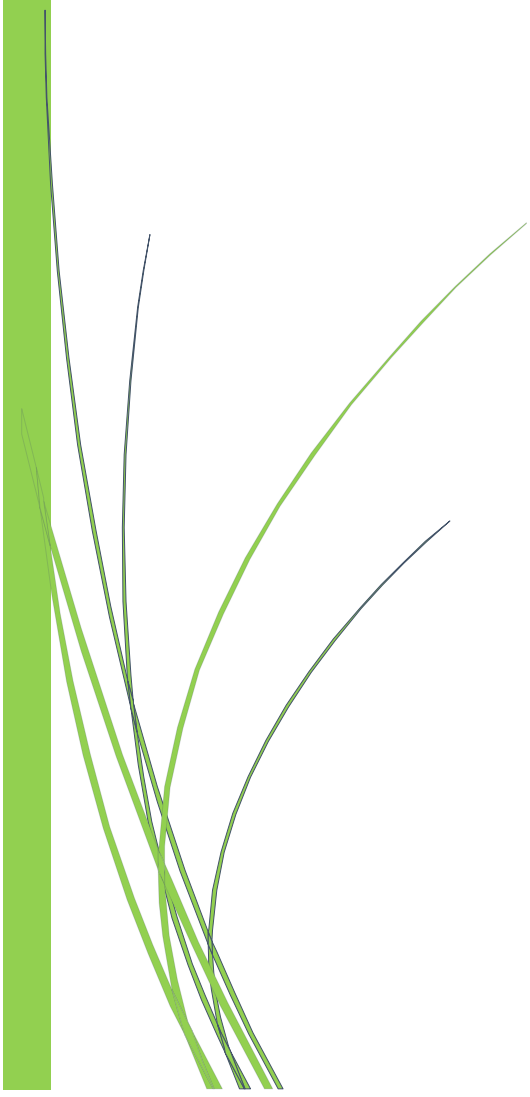
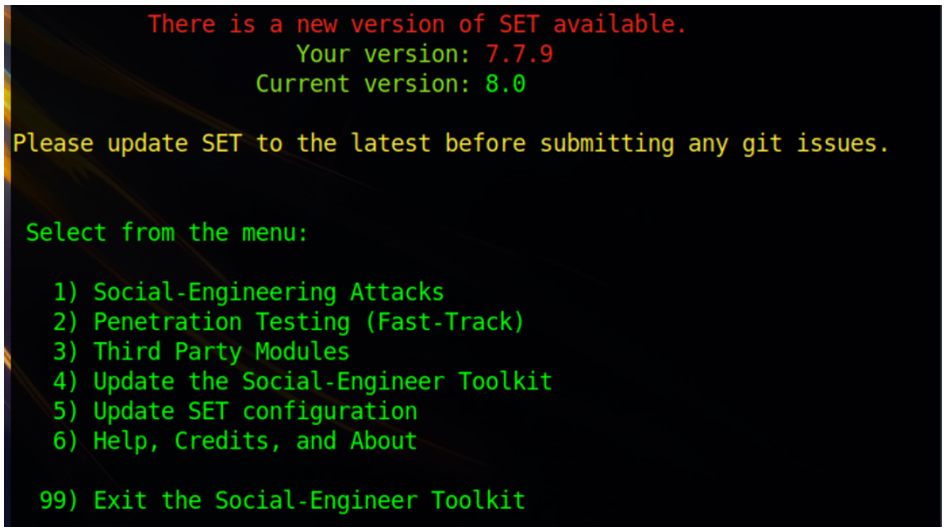
Pruebas de pentración

Práctica 14: SOCIAL ENGINEERING TOOLKIT.

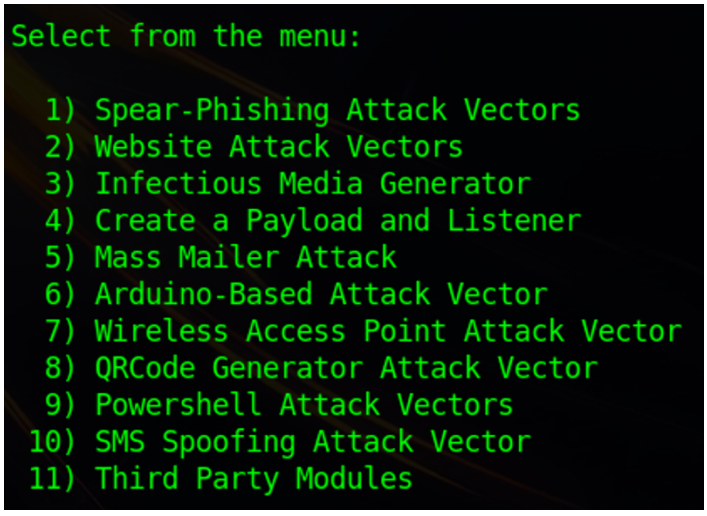


Rodríguez Gallardo Pedro Alejandro

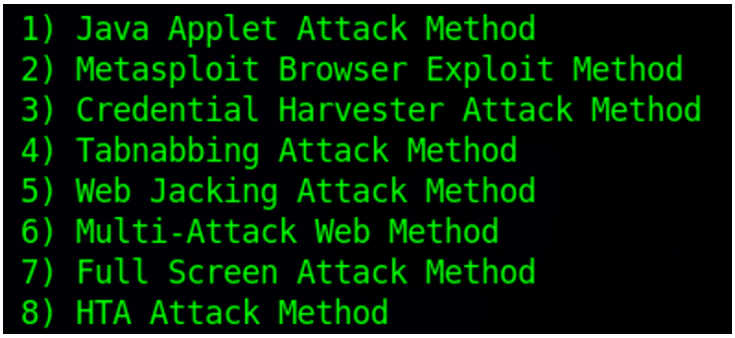
Ejecución de herramienta setoolkit:



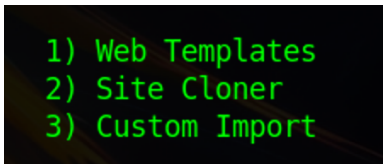
Social-Engineering Attacks



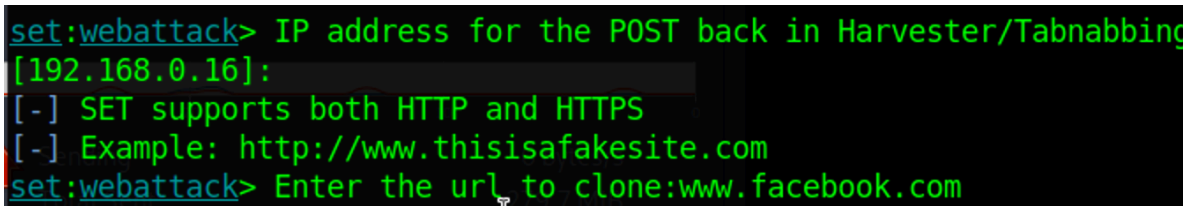
Website Attack Vector



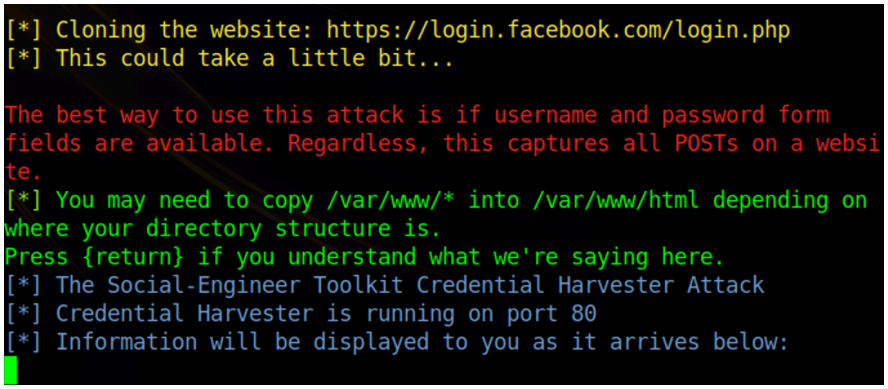
Credential Harvester Attack Method



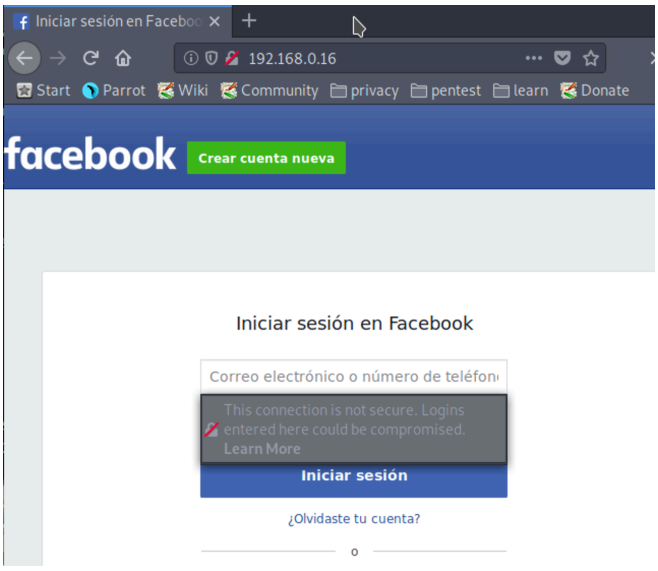
Site Cloner



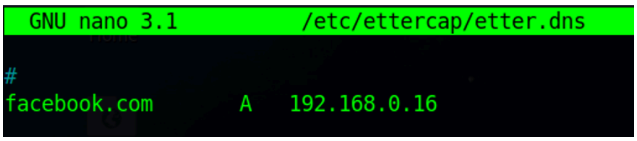
Especificación de pagina web que se clonara.



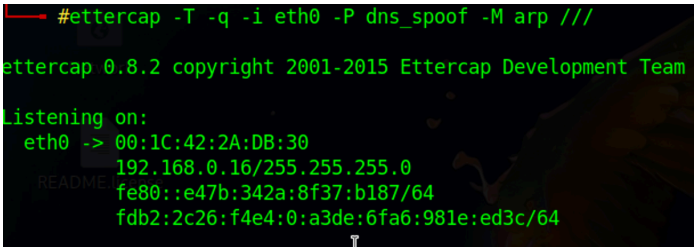
Proceso de clonación del sitio de facebook.com



Prueba del sitio falso.

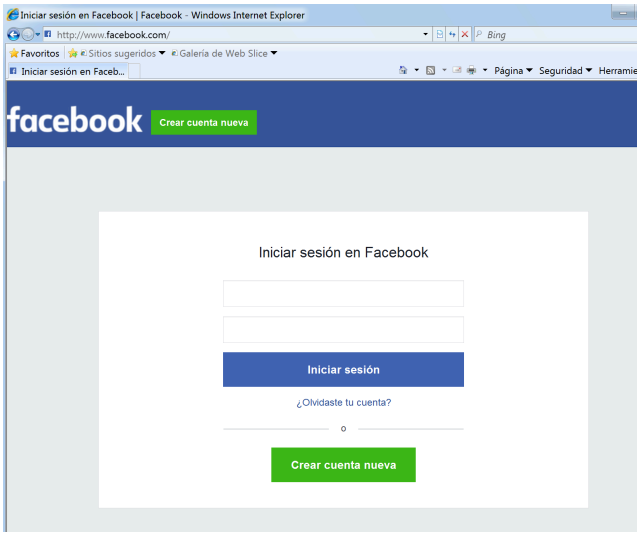


DNS spoofing



ARP poisoning y DNS spoofing.

Tabla ARP de la victima con MAC atacante.



Victima ingresa a la página falta de Facebook.

```
DHCP: [192.168.0.1] ACK : 192.168.0.16 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "localdomain"
DHCP: [00:1C:42:B2:C6:10] REQUEST 192.168.0.28
```

La victima es redirigido a la pagina falsa donde ingresa sus credenciales las cuales son capturadas por el atacante.

Tablas de resolución para Facebook de la victima.

```
Connections list:

     192.168.0.2:0     -    192.168.0.28:0       idle    TX: 0 RX: 0
     192.168.0.1:0     -    192.168.0.28:0       idle    TX: 0 RX: 0
     192.168.0.2:0     -     192.168.0.1:0       idle    TX: 0 RX: 0
  fdb2:2c26:f4e4:0:6548:6677:d61:47a4:0     - ff02::1:ff00:18:0       killed  TX: 0 RX: 0
  fdb2:2c26:f4e4::1:0     - fdb2:2c26:f4e4:0:6548:6677:d61:47a4:0       idle    TX: 0 RX: 0
  fdb2:2c26:f4e4:0:6548:6677:d61:47a4:49285 - 2a03:2880:f135:83:face:b00c:0:25de:443   T opening TX: 0 RX: 0
     192.168.0.2:17500 -   192.168.0.255:17500 U idle    TX: 1253 RX: 0
    192.168.0.28:49286 -    192.168.0.16:443   T killed  TX: 0 RX: 0
  fdb2:2c26:f4e4:0:6548:6677:d61:47a4:49287 - 2a03:2880:f135:83:face:b00c:0:25de:443   T opening TX: 0 RX: 0
  fe80::21c:42ff:fe00:18:0      -         ff02::1:0       killed  TX: 0 RX: 0
  fe80::e47b:342a:8f37:b187:0      -         ff02::16:0       idle    TX: 0 RX: 0
    192.168.0.28:49284 -  148.245.185.75:80    T killed  TX: 0 RX: 0
    192.168.0.28:49282 -  148.245.185.75:80    T killed  TX: 0 RX: 0
    192.168.0.28:49283 -  148.245.185.75:80    T killed  TX: 0 RX: 0
    192.168.0.28:49274 -  148.245.185.90:80    T killed  TX: 0 RX: 0
    192.168.0.28:49288 -     31.13.89.35:443   T killed  TX: 508 RX: 1455
     192.168.0.2:5353  -     224.0.0.251:5353  U idle    TX: 668 RX: 0
```

Lista de conexiones, hay conexiones en Windows 7 hacia direcciones públicas que no se deberían de crear si es que es una prueba de concepto.

```
C:\Users\pter>netstat -a

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            :0                     LISTENING
  TCP    0.0.0.0:445            :0                     LISTENING
  TCP    0.0.0.0:49152          :0                     LISTENING
  TCP    0.0.0.0:49153          :0                     LISTENING
  TCP    0.0.0.0:49154          :0                     LISTENING
  TCP    0.0.0.0:49155          :0                     LISTENING
  TCP    0.0.0.0:49156          :0                     LISTENING
  TCP    192.168.0.28:139       :0                     LISTENING
  TCP    192.168.0.28:49230     edge-star-mini-shv-01-qro1:https  ESTABLISH
  TCP    192.168.0.28:49231     xx-fbcdn-shv-01-qro1:https  ESTABLISHED
  TCP    192.168.0.28:49233     xx-fbcdn-shv-01-qro1:https  ESTABLISHED
  TCP    192.168.0.28:49234     xx-fbcdn-shv-01-qro1:https  ESTABLISHED
  TCP    192.168.0.28:49235     xx-fbcdn-shv-01-qro1:https  ESTABLISHED
  TCP    192.168.0.28:49236     xx-fbcdn-shv-01-qro1:https  ESTABLISHED
  TCP    192.168.0.28:49237     xx-fbcdn-shv-01-qro1:https  ESTABLISHED
  TCP    [::]:135               PEDRORODRIG6DBA:0      LISTENING
  TCP    [::]:445               PEDRORODRIG6DBA:0      LISTENING
  TCP    [::]:49152             PEDRORODRIG6DBA:0      LISTENING
  TCP    [::]:49153             PEDRORODRIG6DBA:0      LISTENING
  TCP    [::]:49154             PEDRORODRIG6DBA:0      LISTENING
  TCP    [::]:49155             PEDRORODRIG6DBA:0      LISTENING
  TCP    [::]:49156             PEDRORODRIG6DBA:0      LISTENING
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:52102        *:*
  UDP    127.0.0.1:56964        *:*
  UDP    127.0.0.1:61988        *:*
  UDP    192.168.0.28:137       *:*
  UDP    192.168.0.28:138       *:*
  UDP    192.168.0.28:1900      *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:61987            *:*
  UDP    [fe80::c1ba:788:f94b:fb26%11]:1900  *:*
```

Conclusión:

No pude obtener las cuenta y contraseña a pesar de tener la configuración apropiada, en la practica podemos ver como conjuntar dos ataques para causar un mayor daño, es importante concientizar a los usuario de este tipo de ataques para que puedan tener un mayor cuidado sobre las paginas que estos revisar y evitar que se conviertan en victimas.

Al igual, encontramos algunas conexiones que fueron creadas a direcciones publicas sospechosas, las cuales no deberían de haberse creado a mi parecer.