Alumno: Rodrigo Vila

Experto Universitario en Hacking Ético

Final 1

Herramienta 1:

Nombre de la tool: Social Engineering Toolkit (SET)

Función de la misma: SET es una herramienta muy popular que permite realizar diversas técnicas de ingeniería social, como ataques de phishing, suplantación de identidad y la creación de sitios web falsos, entre otros.

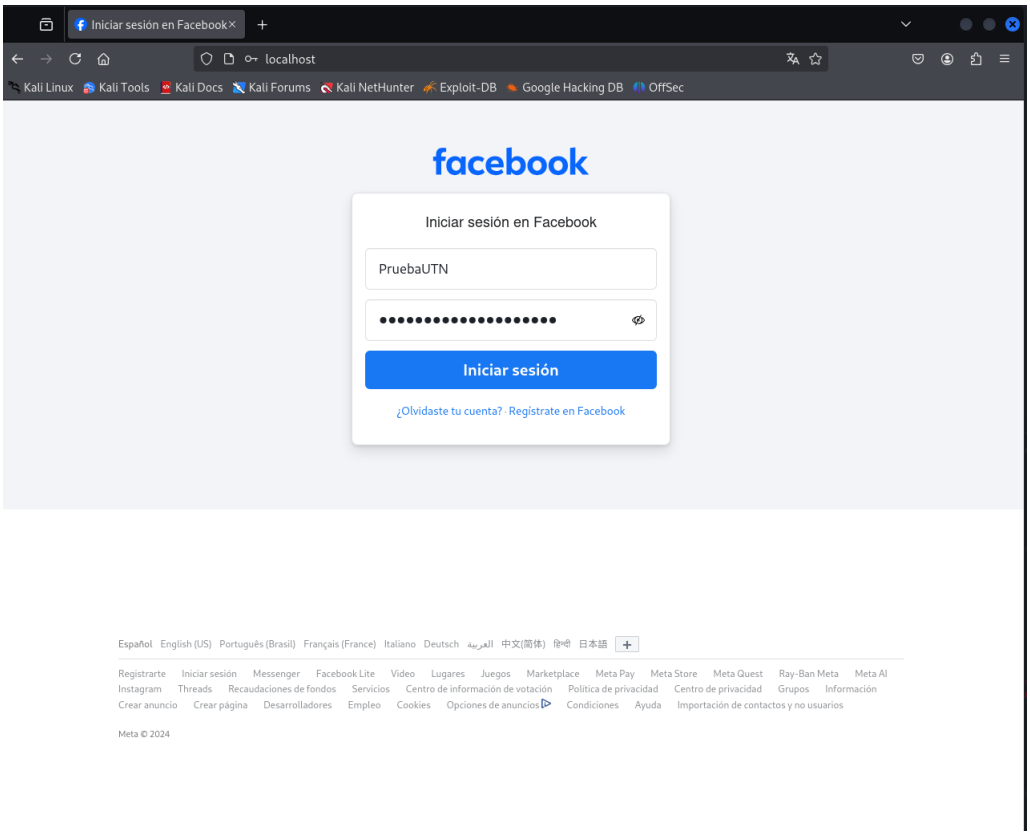
Opinión personal de uso: Es una herramienta muy útil con una gran variedad de utilidades. En lo que respecta a la clonación de sitios web de logins documento el proceso a continuación:

Screenshots:

Portada:

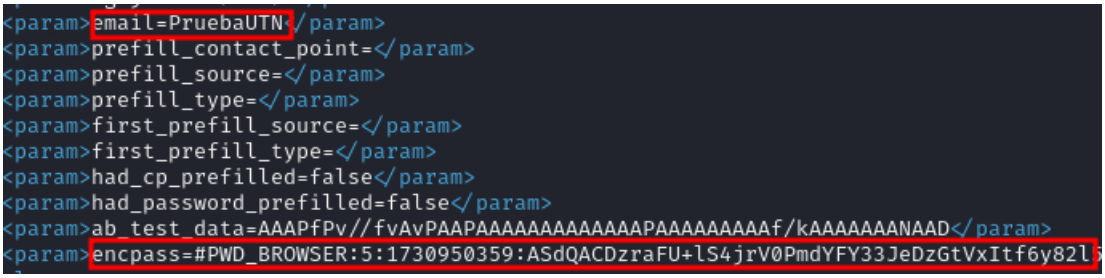
Herramienta Credential Harvester (SET):

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

──────────────────────────────────────────────────────────────────────────
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://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.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```



Cloné como demostración el login de Facebook y lo hice correr localmente en vez de abrir el servidor a internet. En resultado de captura se crea un archivo log con las credenciales capturadas, ésto es muy útil teniendo en cuenta que es una tool

que corre sola y no tenemos que estar monitoreandola todo el tiempo en tiempo real, solo con revisar los logs podemos ver cuantas “presas” hemos capturado.



Una excelente práctica que podemos observar, es que la web clonada utiliza cifrado en el lado cliente en su formulario de inicio de sesión. Esto evita que las contraseñas se envíen como texto plano. SET puede capturar lo que el usuario envía, pero, si el sitio usa cifrado, el valor capturado estará codificado.

Herramienta 2:

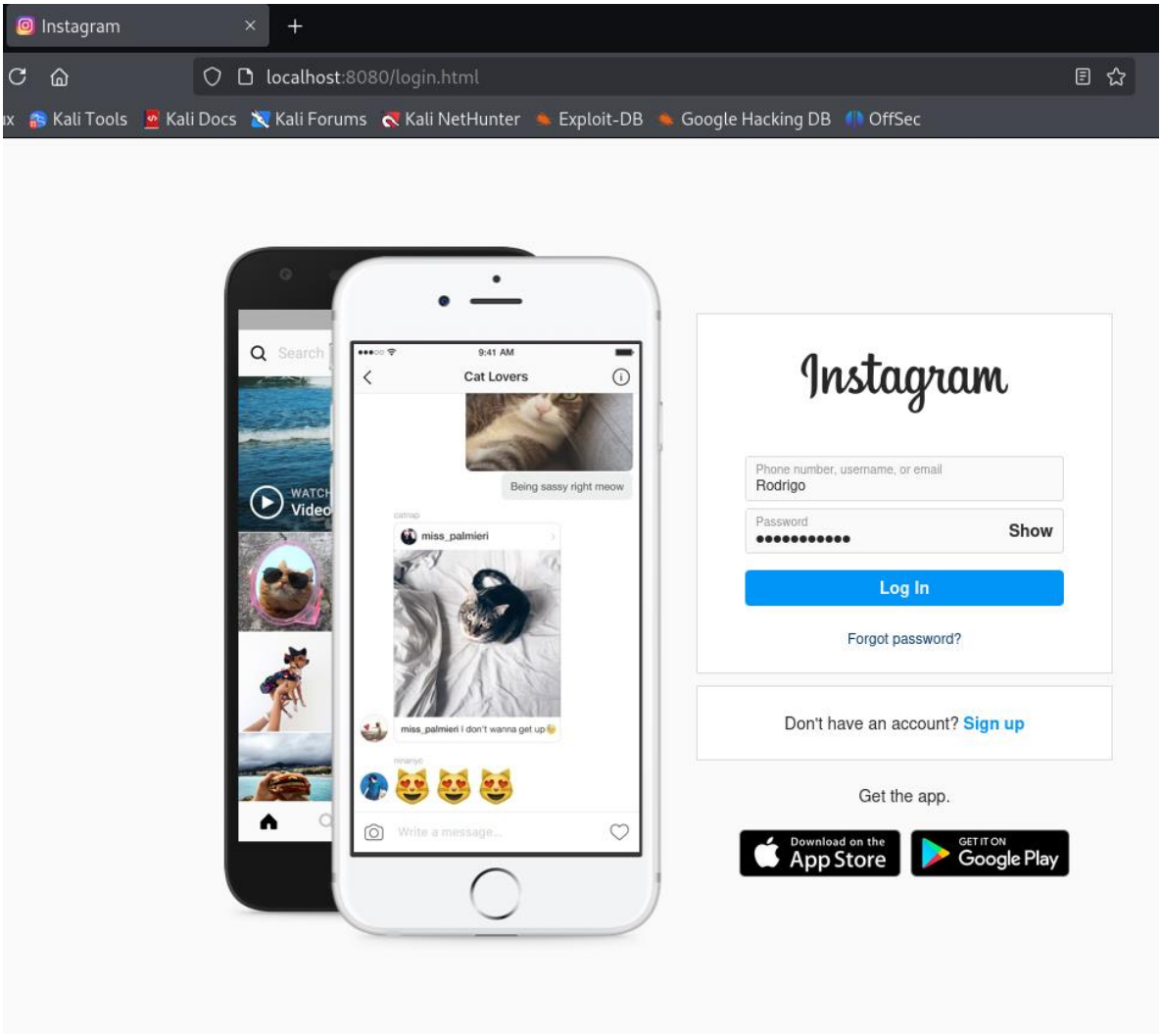
Nombre de la tool: ZPhisher

Función de la misma: La función de ZPhisher es clonar sitios de inicio de sesión populares para capturar credenciales *en entornos controlados, facilitando la simulación de ataques de phishing para capacitación en ciberseguridad.*

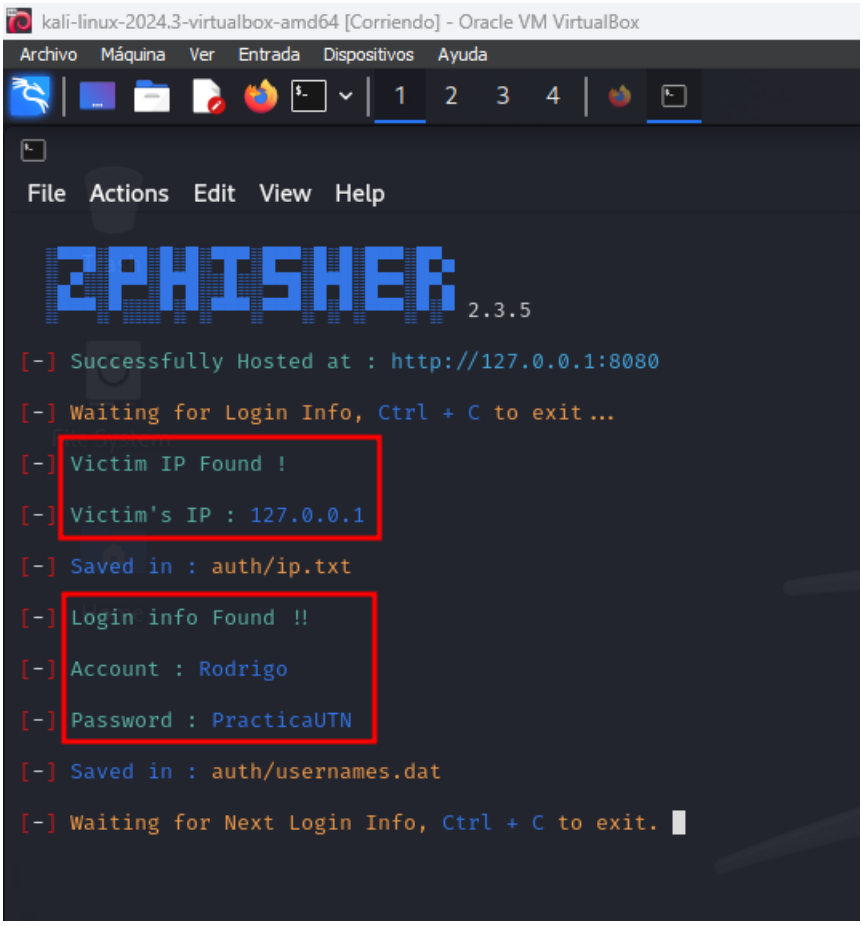
Opinión personal de uso: A diferencia de SET, ésta herramienta tiene una gran variedad de plantillas preinstaladas de sitios web con formulario de inicio de sesión como redes sociales, entre otras webs. El uso es mucho mas simple y mas enfocado en exclusiva al Phishing a diferencia de SET que tiene un abanico mas amplio de utilidades. Además que a diferencia de SET no clona la web objetivo sino que utiliza una plantilla, ósea que la información que se introduce en los campos de formulario por defecto no se encontrará cifrada.

Screenshots:

Acá podemos observar una plantilla de Instagram corriendo en este caso también en nuestro localhost:



En la terminal podemos ver en tiempo real la IP, el usuario y la contraseña introducida, así también como el archivo log:



Herramienta 3:

Nombre de la tool: Hydra

Función de la misma: Hydra es una herramienta de fuerza bruta que permite realizar ataques de diccionario o combinaciones en múltiples protocolos y servicios, como SSH, FTP, HTTP, y otros. Es ampliamente utilizada en pruebas de penetración para evaluar la seguridad de contraseñas, ya que puede realizar intentos rápidos y automatizados de autenticación utilizando una lista de nombres de usuario y contraseñas.

Opinión personal de uso: Para variar un poco de las herramientas de phishing, en este caso Hydra es una excelente herramienta de fuerza bruta que utiliza diccionarios para intentar vulnerar accesos débiles o por defecto.

Para utilizar Hydra lo mas importante es tener en cuenta los parámetros, ya que el “case sensitive” como vimos en la última clase, es muy importante.

Si queremos especificar un usuario por defecto se utiliza “-l user” y si queremos que Hydra utilice un listado de usuarios de un diccionario “-L ruta/de/diccionario.txt”

Lo mismo pasa con la contraseña: se utiliza “-L ruta/de/diccionario.txt” o “-l Contraseña123”.

Después y por último *(mentira)*, para no extenderme demasiado, está el parámetro “-C”, que sirve tanto para que Hydra pruebe usuarios y contraseñas del mismo diccionario, siempre que el formato del texto en el archivo sea del tipo “usuario:contraseña”.

Un ejemplo de un ataque de fuerza bruta con Hydra a un servidor ssh utilizando el famoso archivo “rockyou” seria:

hydra -C /usr/share/wordlists/rockyou.txt ssh://ip_del_objetivo

Un ataque de fuerza bruta puede demorar muchísimo en tener éxito o dejarnos en la incertidumbre de la espera durante largos periodos de tiempo, dependiendo la longitud de los diccionarios que utilicemos. Por eso, otro parámetro importante a tener en cuenta es “-t” el cual especifica el número de intentos simultáneos que ejecutamos.

Los intentos simultáneos en Hydra, configurados mediante la opción “-t”, controlan la cantidad de conexiones paralelas que Hydra realiza mientras prueba las contraseñas. Cuanto mayor sea el número de intentos simultáneos, más rápido se ejecutará el ataque, ya que Hydra podrá probar múltiples combinaciones de usuario y contraseña al mismo tiempo.

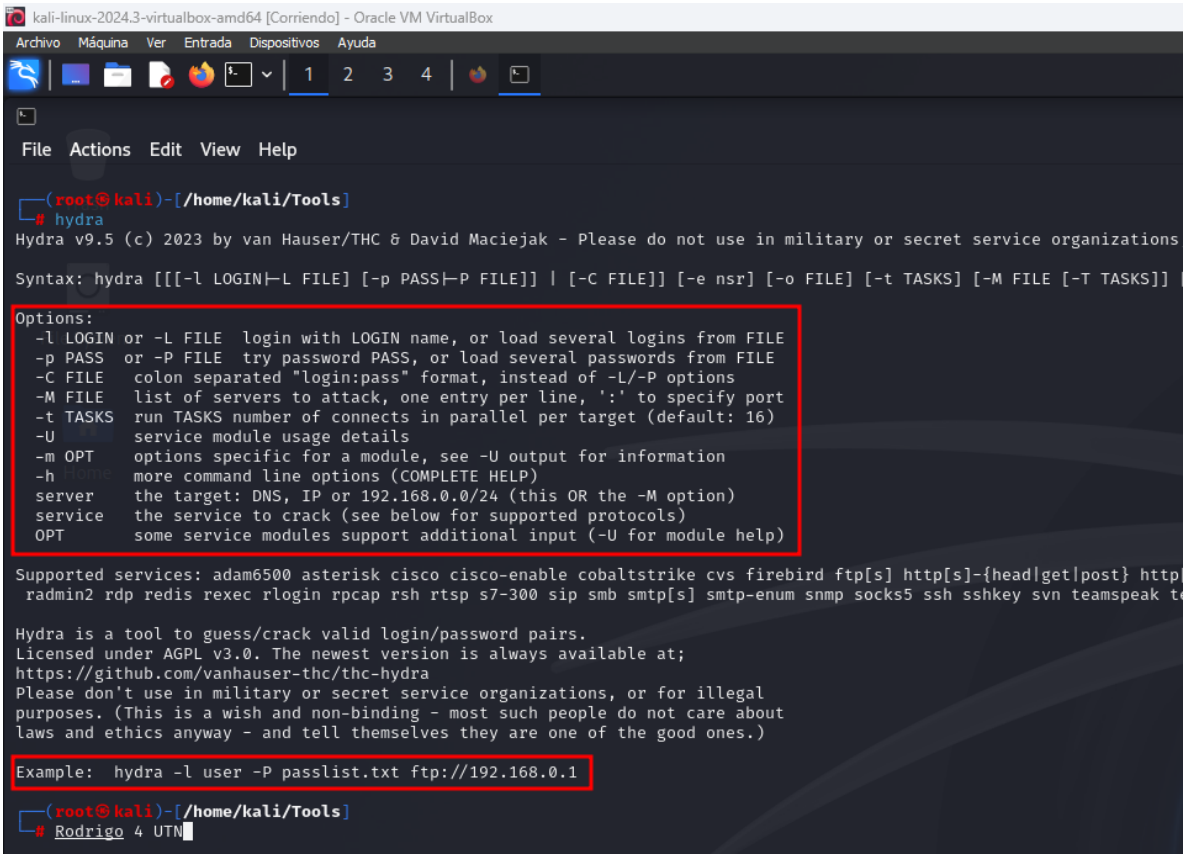
Si estableces un valor bajo para “-t”, Hydra probará las combinaciones de una en una, mientras que un valor alto acelera el proceso, pero también podría generar más tráfico en la red y sobrecargar el servidor objetivo si no tiene un límite de intentos o protección activa.

Por ejemplo:

hydra -L usuarios.txt -P contraseñas.txt -t 10 ssh://ip_del_objetivo

En este caso, Hydra intentará realizar 10 intentos de conexión simultáneamente por cada combinación de usuario y contraseña. Esto significa que probará 10 combinaciones diferentes al mismo tiempo, lo que puede aumentar considerablemente la velocidad del ataque.

Screenshot:



Rodrigo Vila.-