INGENIERÍA SOCIAL

Jordi Masó Pla

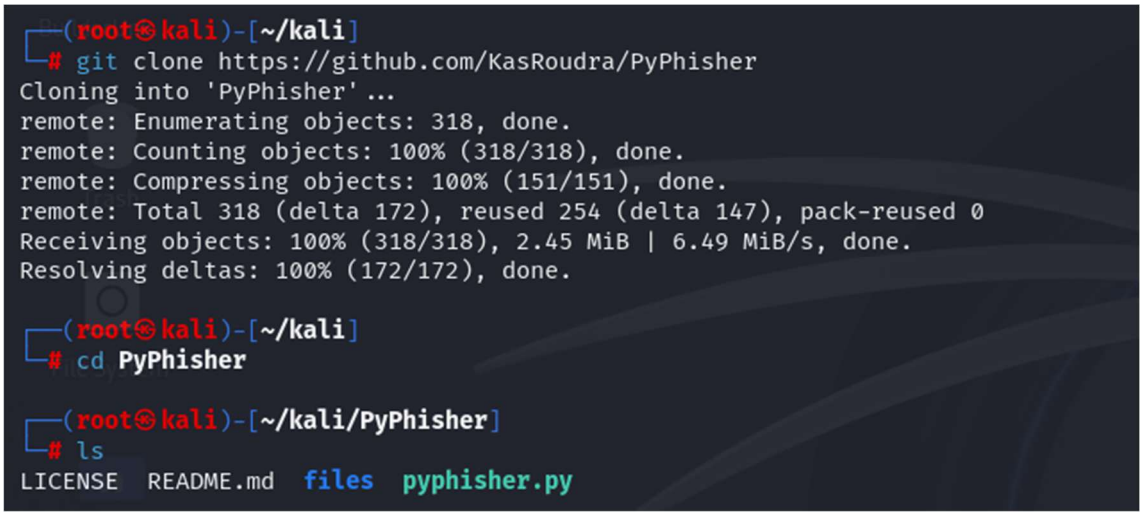
ÍNDICE

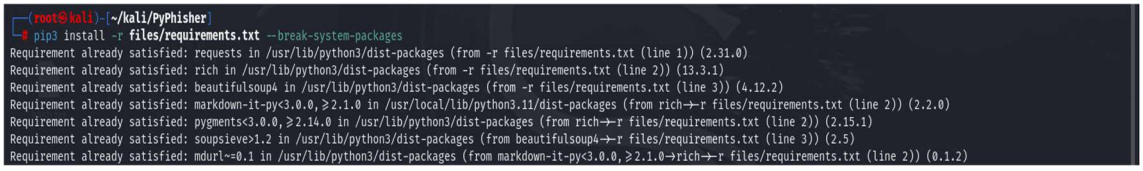
1 DESCRIPCIÓN

En este ejercicio realizaremos un ataque de ingeniería social creando RogueAP con portal cautivo, con la herramienta PyPhisher.

1.1 INSTALACIÓN

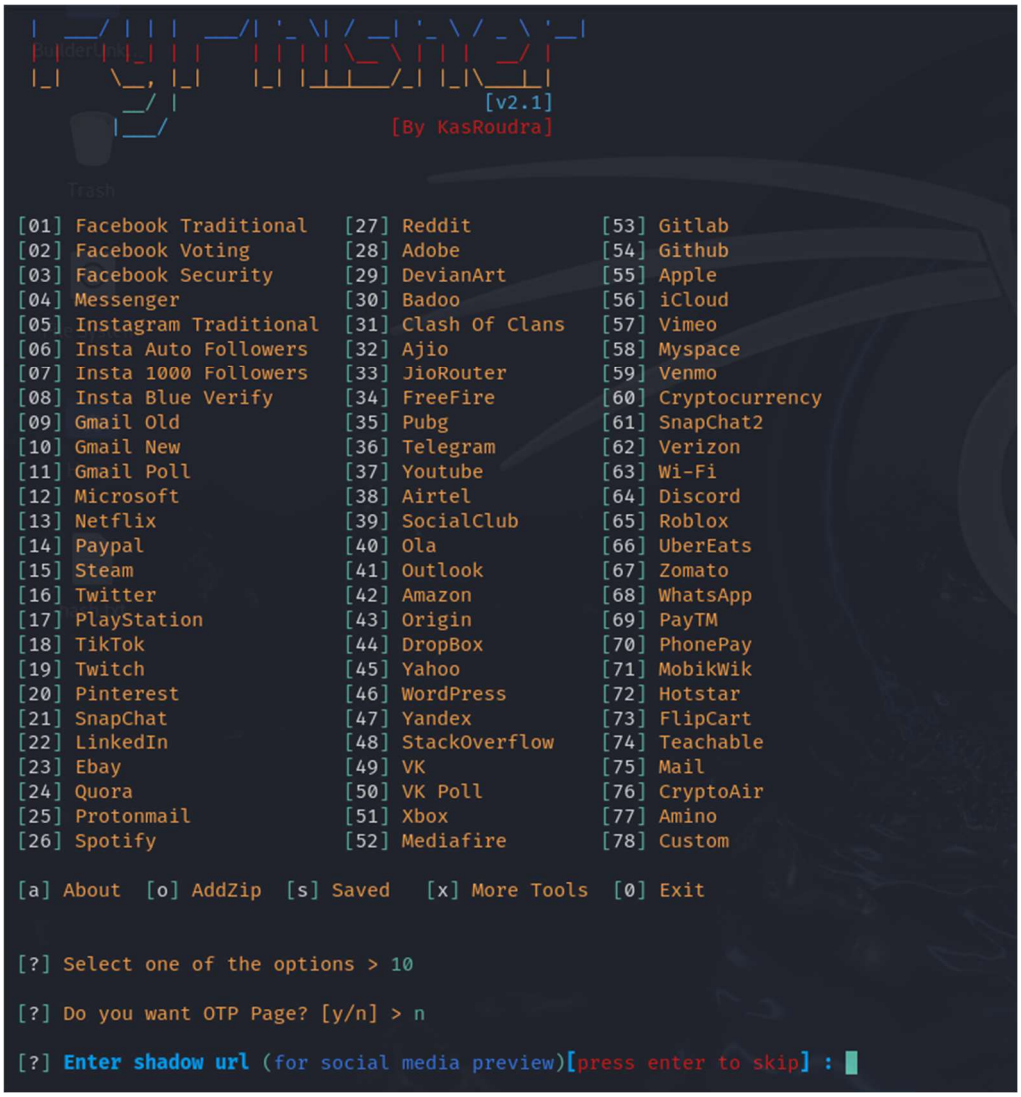
Para instalar la herramienta de PyPhisher lo aremos desde el repositorio de GitHub. Primero instalamos las dependencias requeridas con el comando “sudo apt install git python3 python3-pip php openssh-client -y”, el siguiente comando es descargar el programa con “git clone https://github.com/KasRoudra/PyPhisher.git”. Accedemos al fichero de PyPhisher e instalamos la herramienta con el comando “pip3 install -r files/requirements.txt --break-system-packages”. Con esto ya podemos ejecutar la herramienta, con el comando “python3 pyphisher.py”.





1.2 CONFIGURACIÓN DEL ATAQUE

Esta herramienta tiene un entorno guiado en la consola. Una vez dentro del programa seleccionamos el portal que queremos suplantar, en este caso será la opción 10 que es el portal de login de Proto mail.

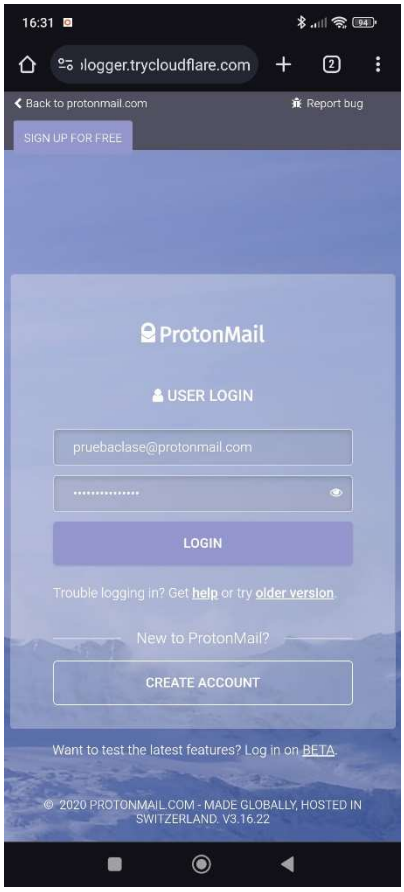


Nos pregunta si queremos una pagina OPT le indicamos que no y si queremos introducir una url oculta para las redes sociales, indicamos que no.

Acto seguido empieza a levantar un servidor php y el túnel a las direcciones. Esta herramienta muestra tres direcciones una es un CloudFlared, localhost y serveo. Nos pregunta si queremos personalizar el link.

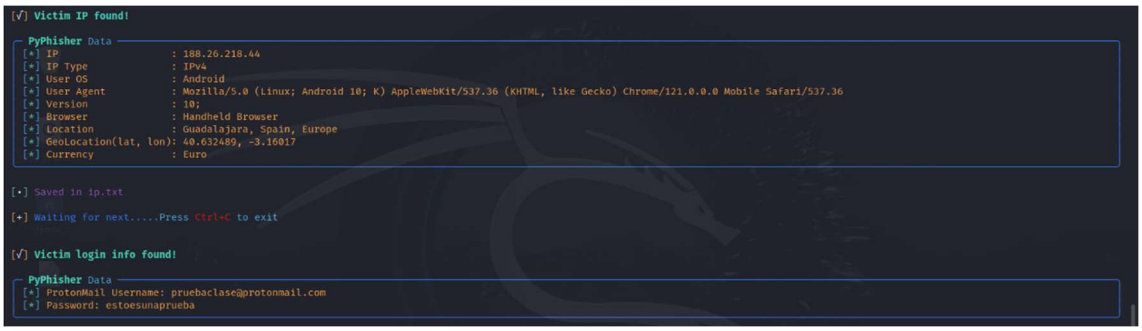
1.3 COMPROBACIÓN DEL ATAQUE

Accedemos desde el teléfono móvil para iniciar sesión en la web de Proton mail, accedemos a una web de inicio e introducimos las credenciales de inicio de sesión.



1.4 OBTENCIÓN DE LAS CREDENCIALES

Comprobamos como la herramienta a capturado el inicio de sesión del teléfono y las credenciales introducidas en el portal.



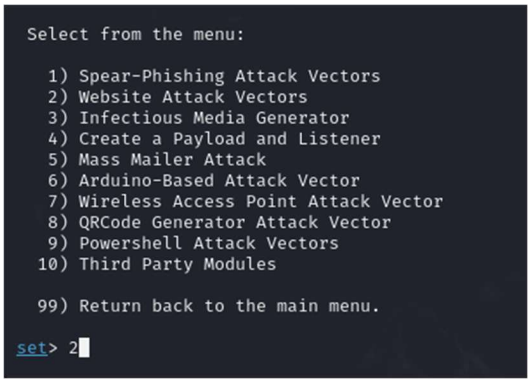
Esta herramienta a capturado la dirección ip del terminal, el sistema operativo, la versión del navegador, la geolocalización del dispositivo y las credenciales introducidas.

2 ENVENENAMIENTO ARP Y USO DE SET

2.1 PREPARACIÓN DE SET

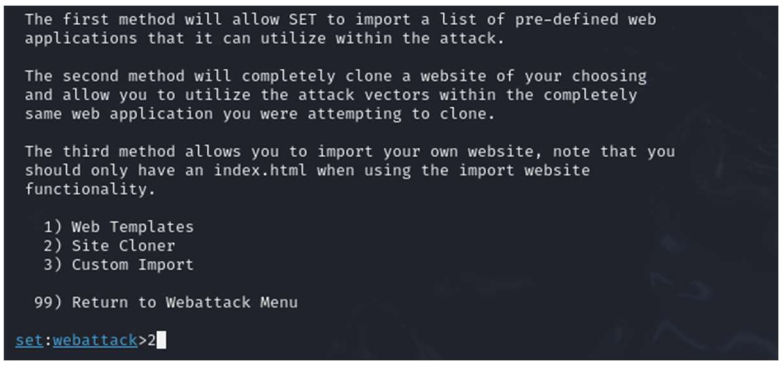
The Social-Engineer Toolkit es una herramienta ya instala en Kali Linux para realizar ataques de ingeniería social. En esta ocasión realizaremos un ataque para conseguir credenciales de inicio de sesión de una página web.

Una vez arrancada la herramienta seleccionamos la opción 1, en el siguiente menú la opción 2 vector de ataque a sitio web.



El siguiente menú escogemos la opción 3 método de ataque de recolección de credenciales.

El ultimo menú escogemos la opción 2 que es clonar un sitio web, en este caso Twitter. Introducimos la ip de nuestra maquina atacante, el ataque corre sobre nuestra ip al puerto 80.



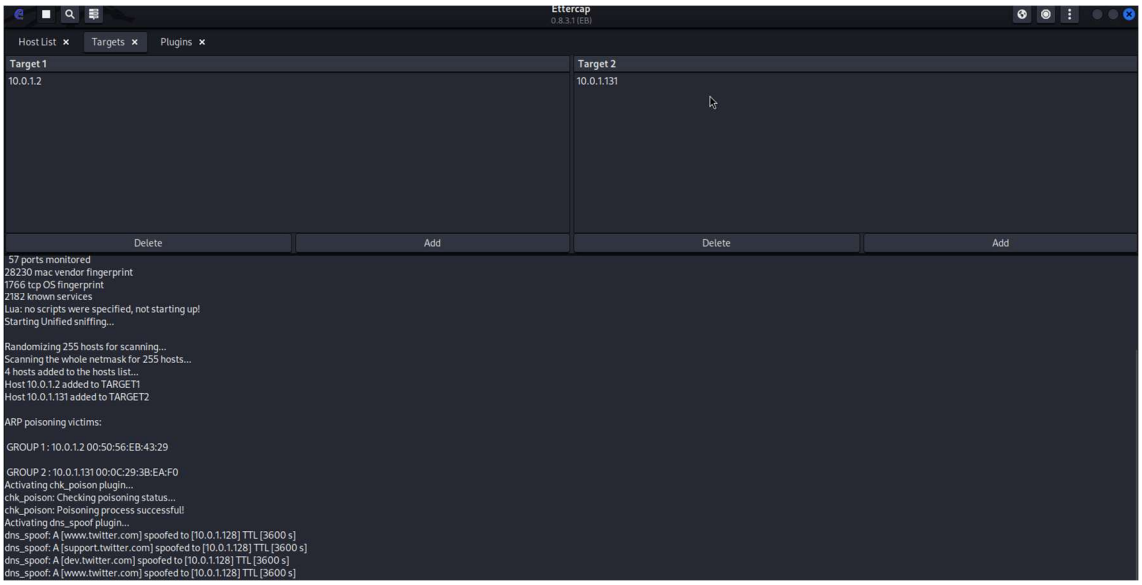
```
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

2.2 Envenenamiento ARP

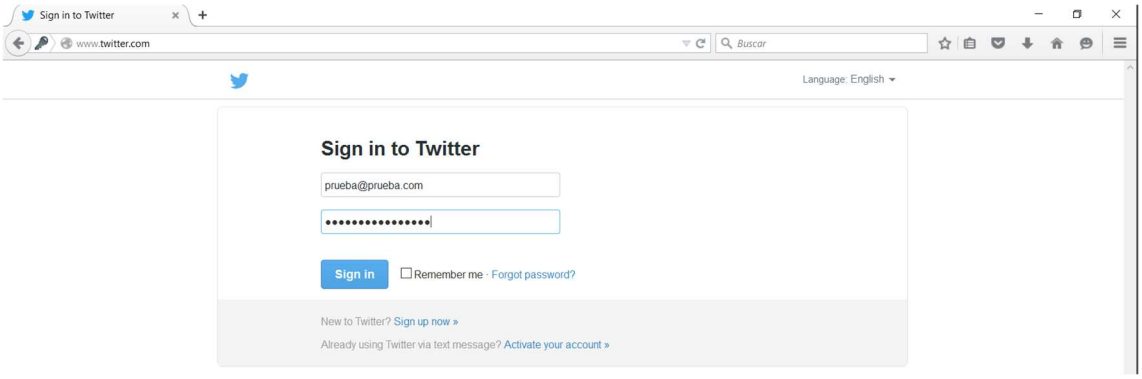
Con la herramienta Ettercap realizaremos el envenenamiento ARP y el dns spoofing para que todo el trafico de red y al que se dirige a la puerta de enlace para por nosotros y poder interceptar-lo.

Con la previa configuración de los ficheros de etter.conf y etter.dns ya podemos ejecutar Ettercap poner el envenenamiento ARP y el dns spoofing en marcha.



2.3 COMPROBACIÓN DEL ATAQUE

Desde nuestro Windows 10 accedemos a la web de Twitter y ponemos las credenciales para acceder al servició de esta web.



En la maquina Kali comprobamos como el envenenamiento ARP y el dns spoofing esta funcionando correctamente, el acceso se ha dirigido a nuestra maquina iniciándose en el portal de la herramienta SET, cazando las credenciales de inicio de sesión