Social Engineering Tollkit

Toolkit es una herramienta open-source en Python destinada para pruebas de penetración en el ámbito de la ingeniería social.

Desarrollo:

Debemos de tener dos máquinas una que será la máquina donde haremos el ataque y otra que será la víctima, nuestra máquina donde haremos el ataque tiene la dirección IP **192.168.1.71** y una dirección MAC **08:00:27:7a:1a:c2** como se muestra en la figura 1 y la máquina víctima tiene la dirección IP **192.168.1.67** y le haremos un ping para ver que se ven una a otra como se muestra en la figura 2.

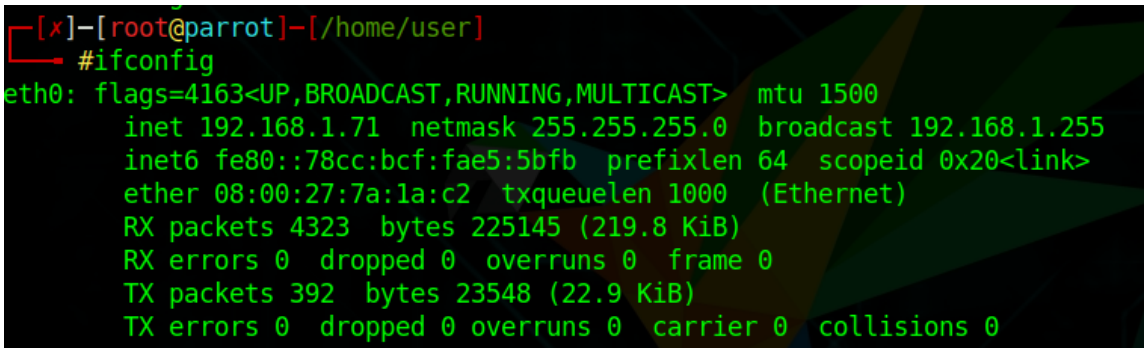

Figura 1. Dirección IP del atacante.

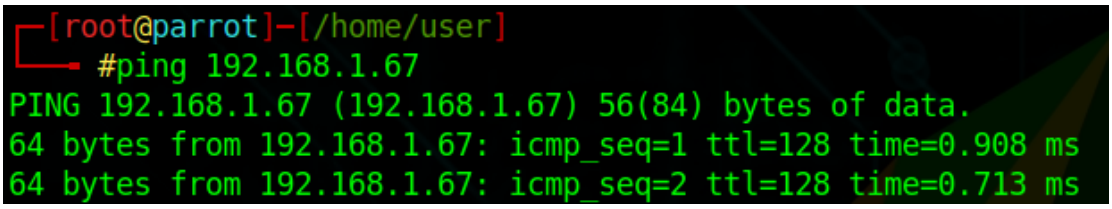

Figura 2. Comunicación entre el atacante y la víctima.

Procedemos a iniciar la herramienta setoolkit, como se muestra en la figura 3 y 4.

Figura 3. Inicio de la herramienta setoolkit.

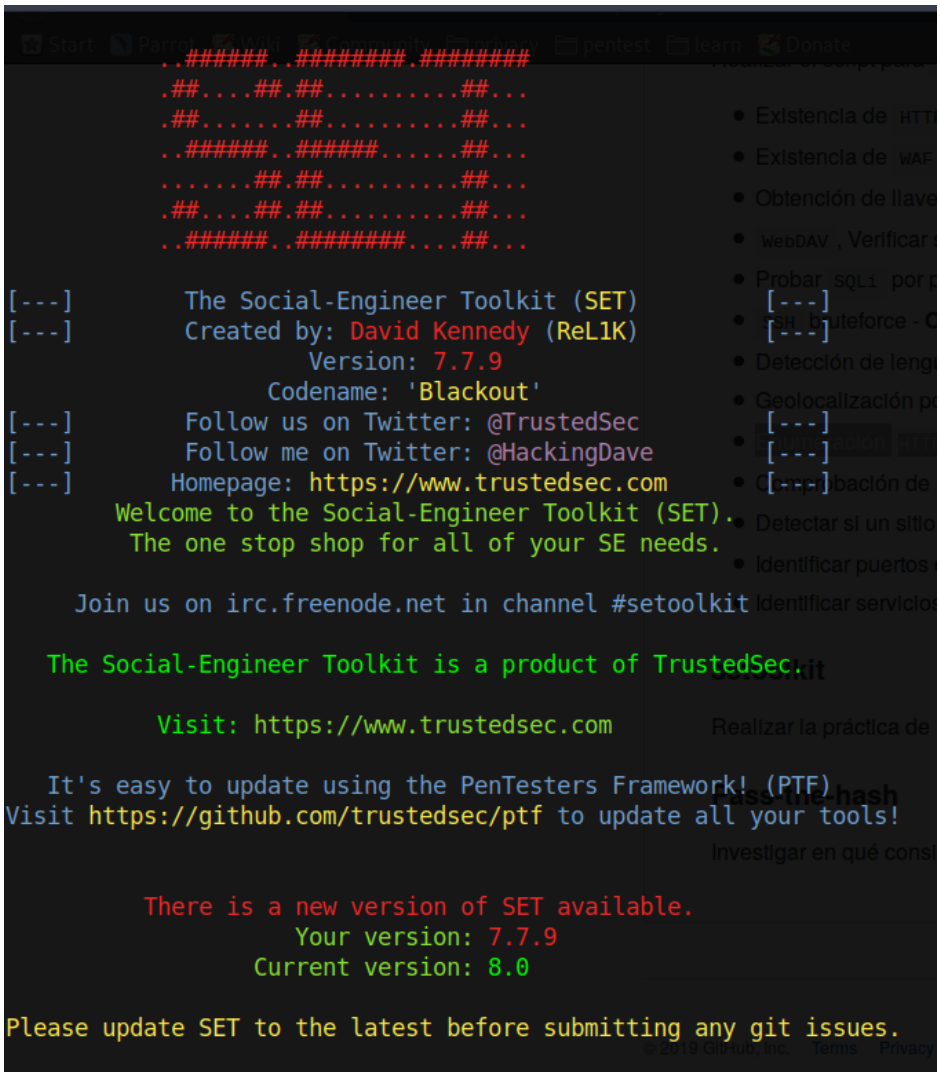

Figura 4. Inicio de la herramienta setoolkit.

Una vez iniciada seleccionamos la opción 1 Social-Engineering Attacks como se muestra en la figura 5.

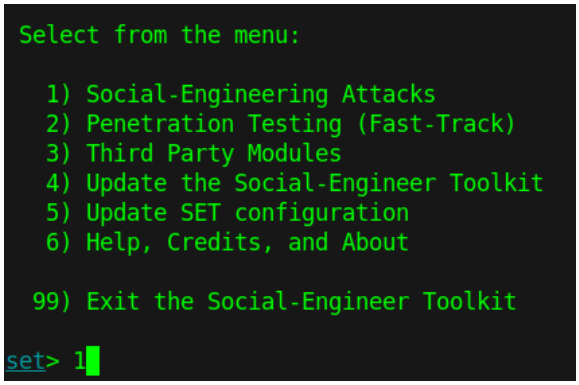

Figura 5. Selección de Social-Engineering Attacks.

Nos mostrará otro menú y seleccionamos la opción 2 Website Attack Vectors como se muestra en la figura 6.

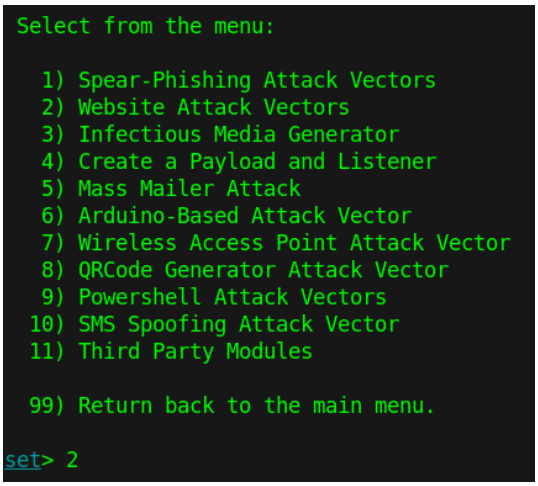

Figura 6. Selección de Website Attack Vectors.

Se nos mostrará otro menú y ahora seleccionamos la opción 3 Credential Harvester Attack Method, como se muestra en la figura 7.

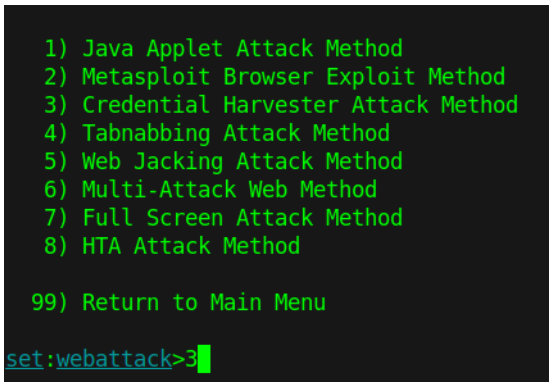

Figura 7. Selección de Credential Harvester Attack Method.

Por último, nos aparecerá un menú y seleccionamos la opción 2, Site cloner como se muestra en la figura 8.

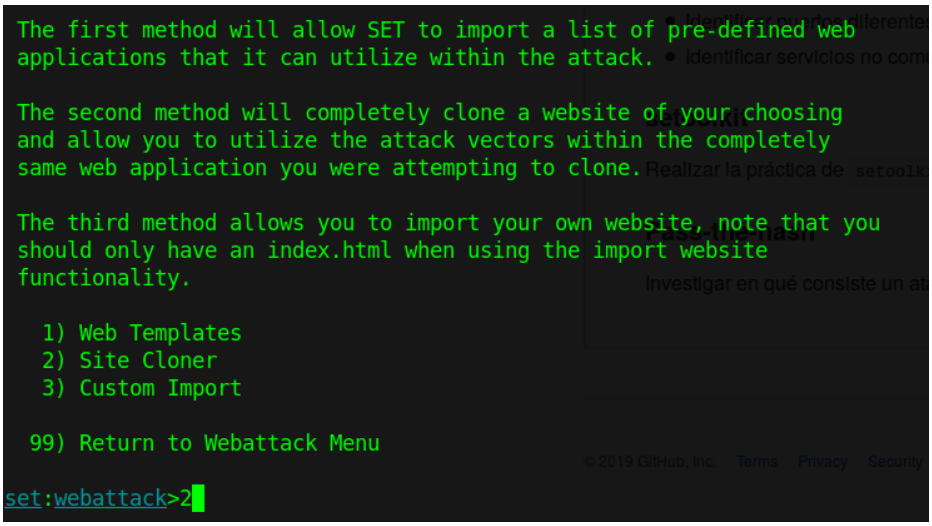

Figura 8. Selección de Site cloner.

Ahora nos pedirá que ingresemos la url la cual clonaremos, en este caso será el sitio de Facebook, la cual tiene la dirección https://www.facebook.com, la ingresamos como se muestra en la figura 9, el sitio original se muestra en la figura 10.

Figura 9. Ingreso del sitio web a clonar.

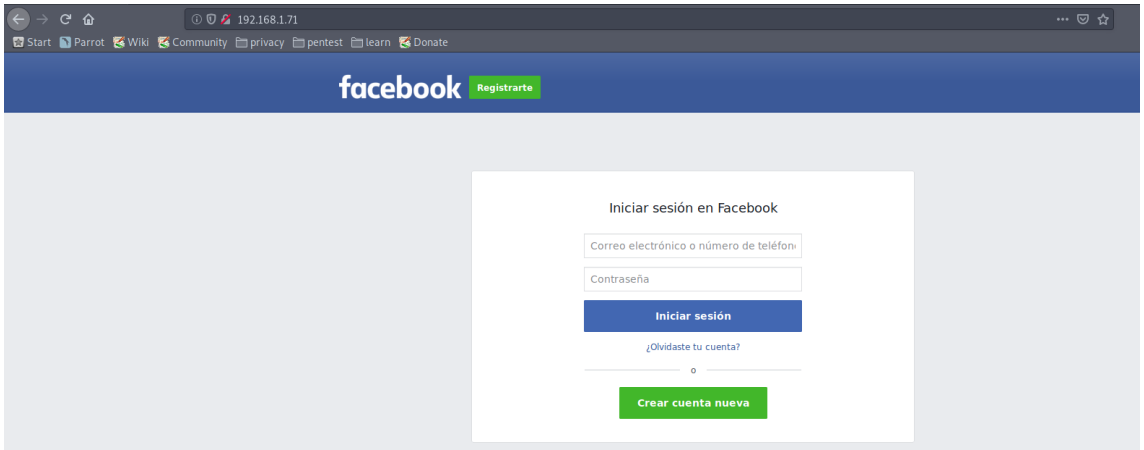

Figura 10. Sitio original

Ahora abrimos otra terminal y procedemos a realizar un ARP spoofing y un DNS spoofing, para esto es necesario editar el archivo etter.dns el cual se encuentra en /etc/ettercap/etter.dns, como se muestra en la figura 11.

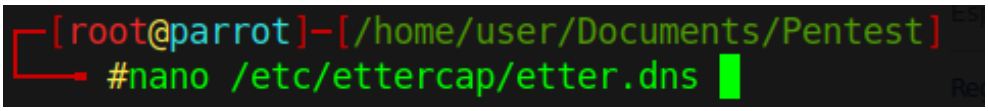

Figura 11. Ubicación del archivo etter.dns.

Una vez localizado se procede a agregar lo siguiente:

facebook.com A 192.168.1.71

Como se muestra en la figura 12, esto lo realizamos para que resuelva el sitio de facebook.com y lo redirija a nuestro sitio que previamente hemos clonado.

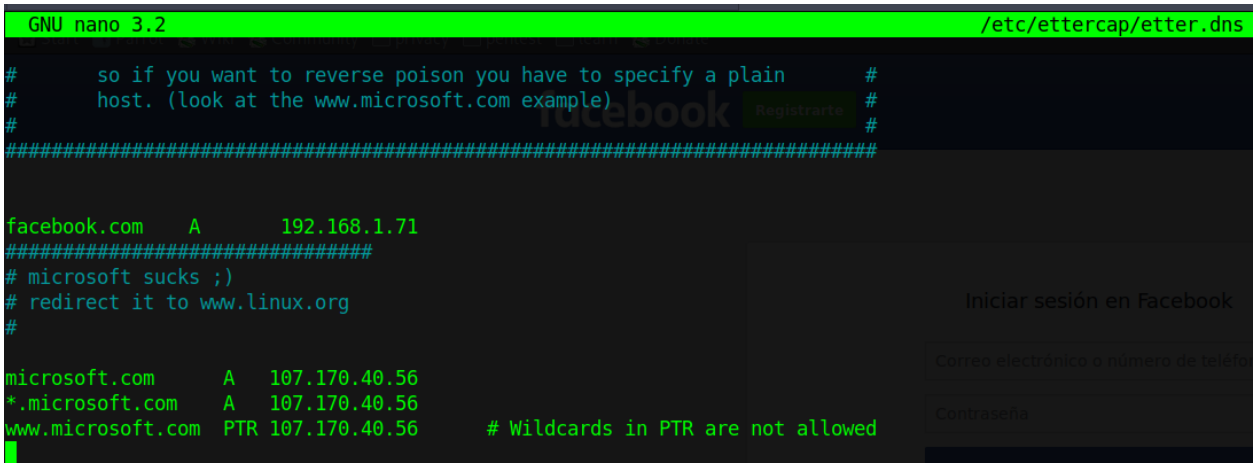

Figura 12. Agregar el registro A del sitio clonado.

Ahora procedemos a realizar el ataque ARP spoofing y DNS spoofing con el siguiente comando:

ettercap –T –q –i eth0 –P dns_spoof –M arp ///

El comando anterior en la terminal se vera de la siguiente manera, como se muestra en la figura 13, al ejecutar el comando tendremos la siguiente salida como la que se muestra en la figura 14.

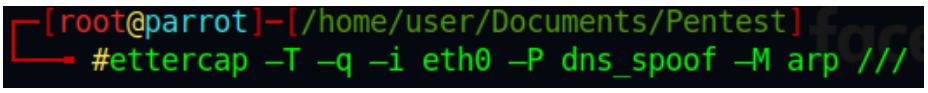

Figura 13. Ataque ARP y DNS spoofing.

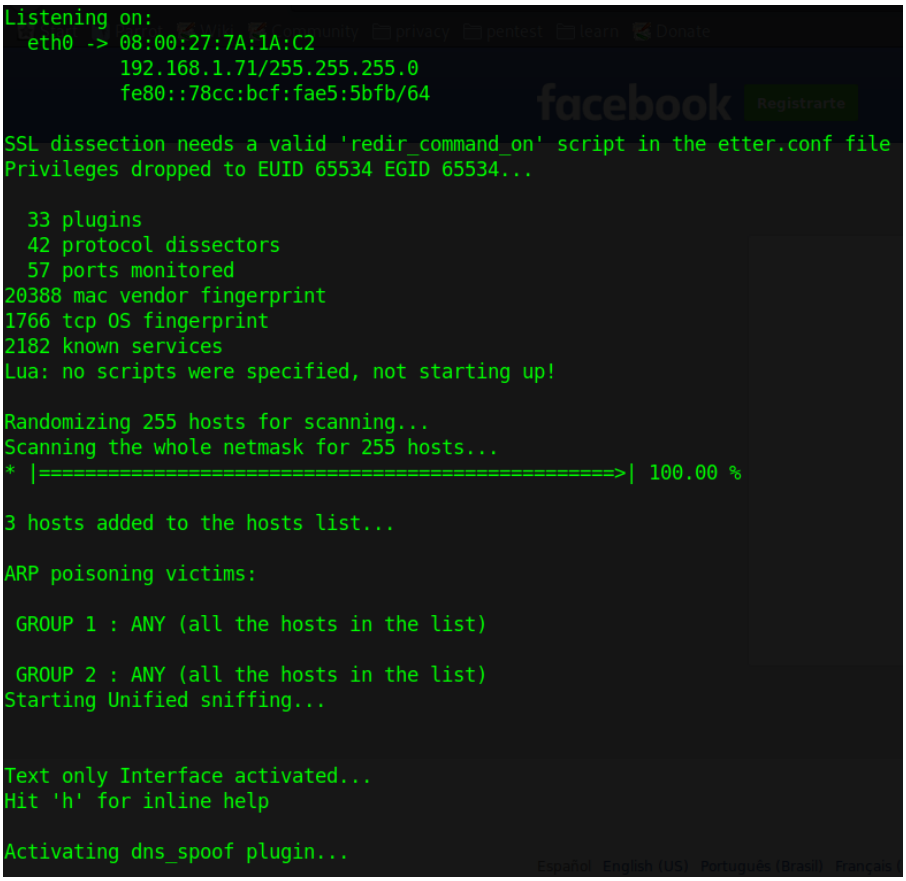

Figura 14. Ejecución del comando.

Ahora nos dirigimos a la computadora victima y abrimos una terminal y ejecutamos el comando arp -a, para ver su tabla arp y observamos que se modifico y que los quipos tienen la dirección MAC de la máquina atacante, como se muestra en la figura 15.

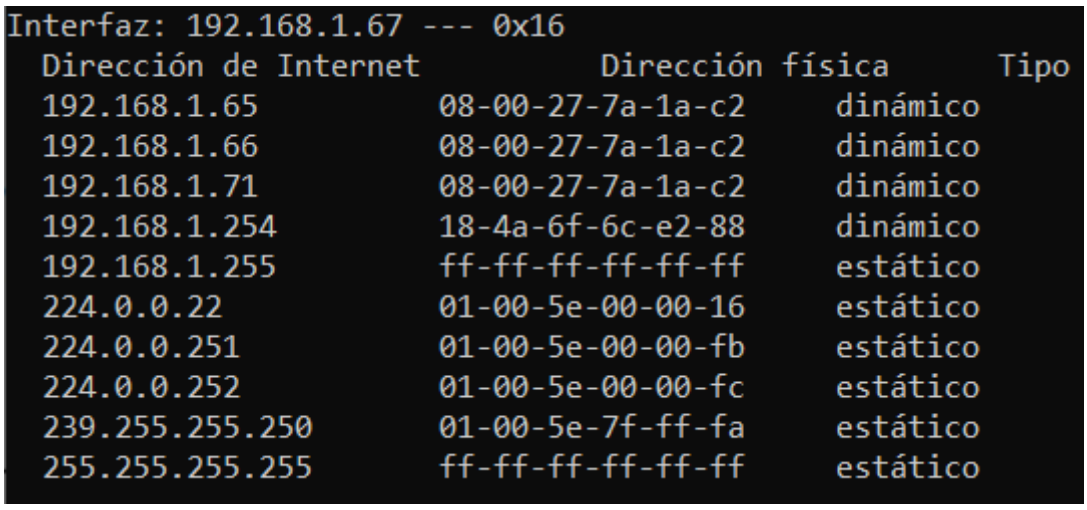

Figura 15. Tabla ARP modificada en la víctima.

Ahora desde la computadora víctima abrimos un navegador e ingresamos a Facebook, ponemos nuestro nombre de usuario y nuestra contraseña e ingresamos, como se muestra en la figura 16.

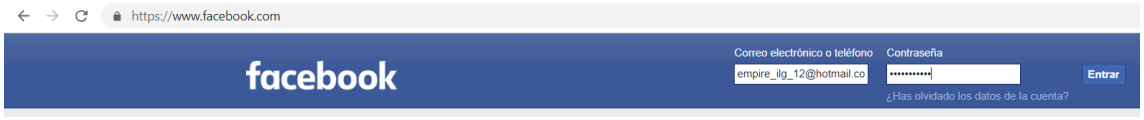

Figura 16. Ingreso a Facebook desde la máquina víctima.

Regresamos a la máquina atacante y observamos que se tiene el nombre de usuario y la contraseña ingresada, como se muestra en la figura 17, las cuales son las que ingresamos en la máquina víctima, las cuales corresponden a nuestras credenciales.

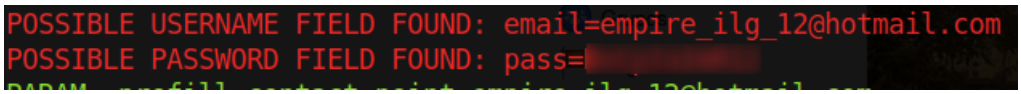

Figura 17. Usuario y contraseña obtenida.