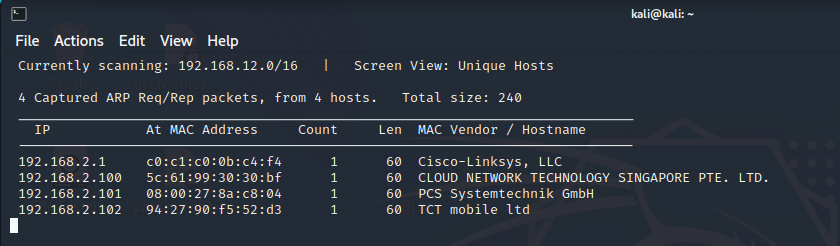
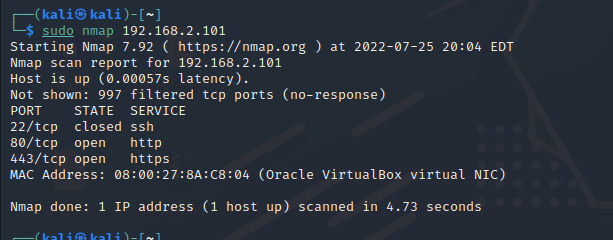
**ANALISIS MAQUINA MR.ROBOT**

**Objetivo:** Realizar pentesting a la maquina vulnerable Mr.Robot y encontrar 3 claves ocultas.

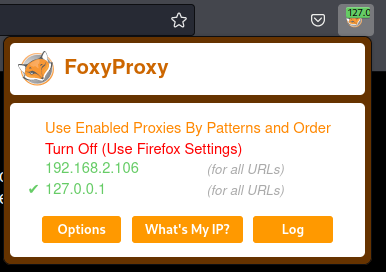
Lo primero que hacemos es analizar la red para identificar la dirección IP de la maquina Mr.Robot y lo hacemos con el comendo **sudo netdiscover**



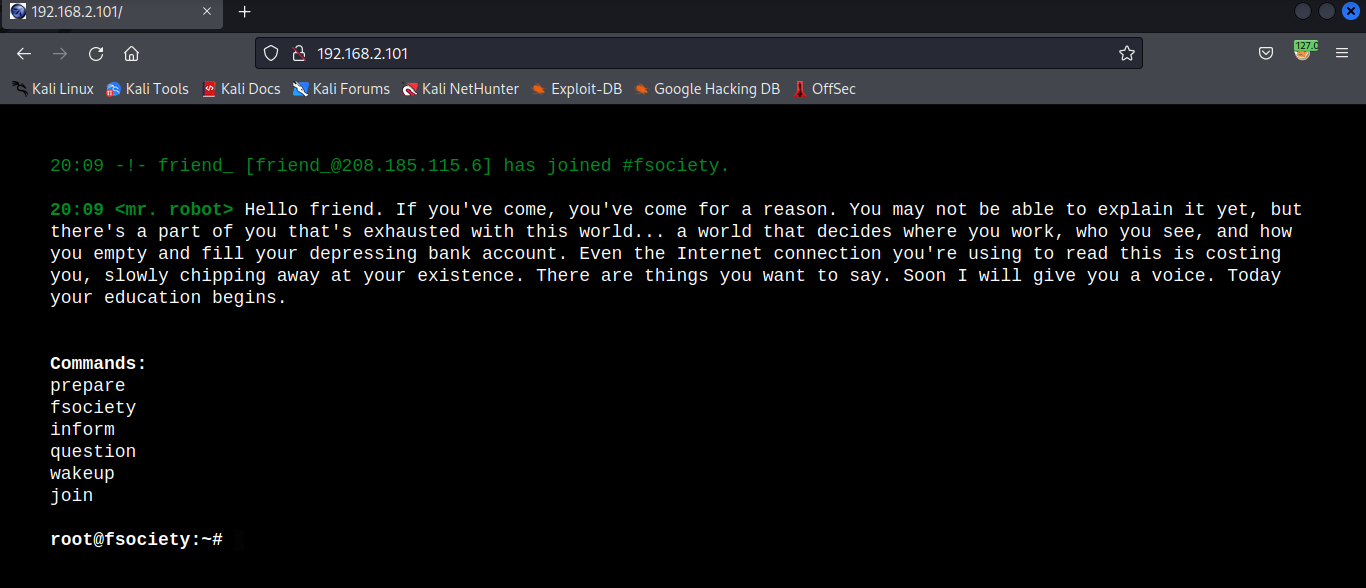
Identificamos que la dirección IP que corresponde a la maquina vulnerable es **192.168.2.101,** ahora procederemos a analizar la máquina virtual con **sudo nmap 192.168.2.101** para ver los servicios y puertos abiertos.



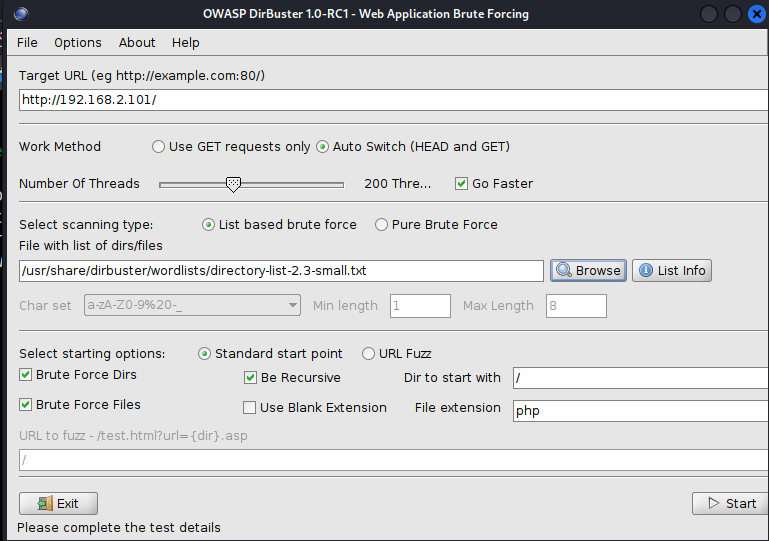
Observamos que los puertos abiertos son 80 y 443 del servicio http lo cual tendremos que ir a un navegador y colocar la dirección ip en la URL 192.168.2.106 y analizar la página web con las herramientas burpsuite o dirbuster, en este caso utilizaremos los dos usando el proxy para comunicar ambas herramientas.

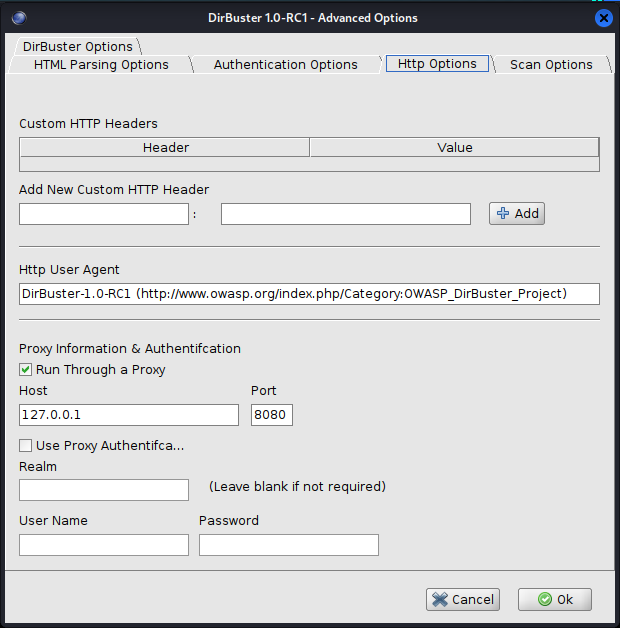


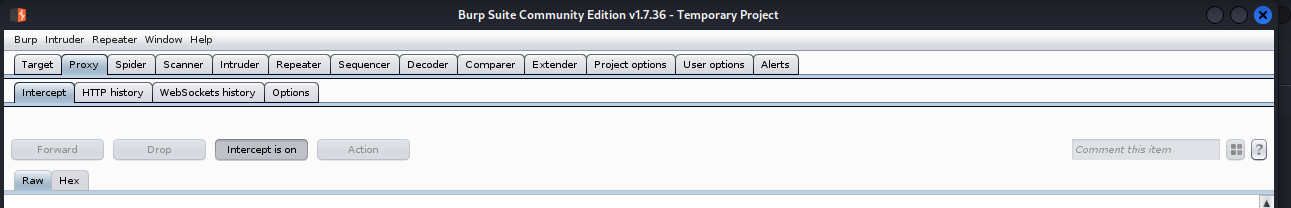
Usamos FoxyProxy



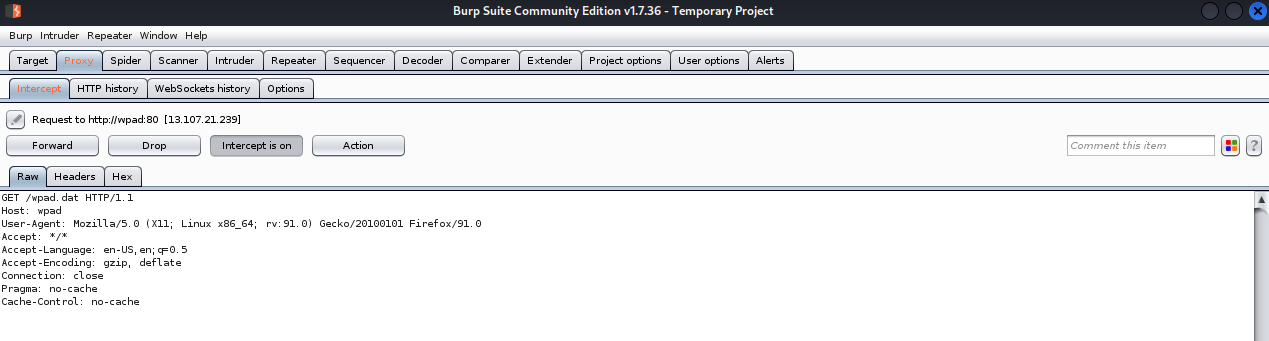
CONFIGURACION DIRBUSTER



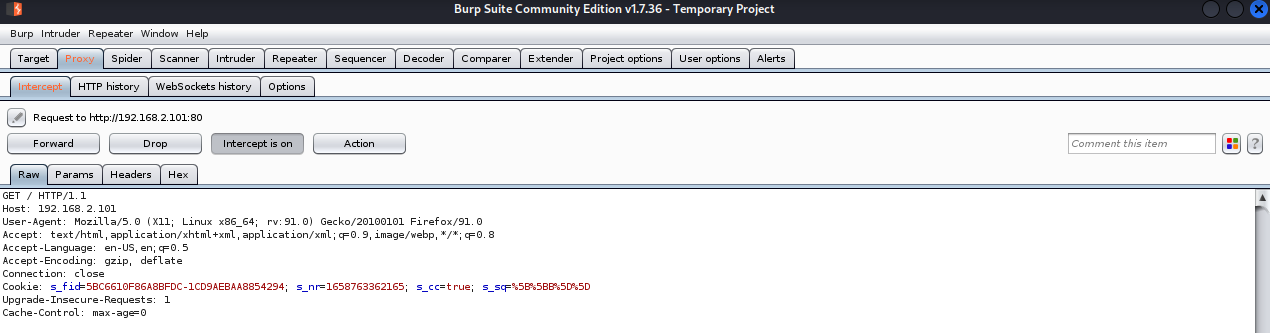
En opciones avanzadas y en http options configuramos el proxy

CONFIGURACION BURPSUITE  


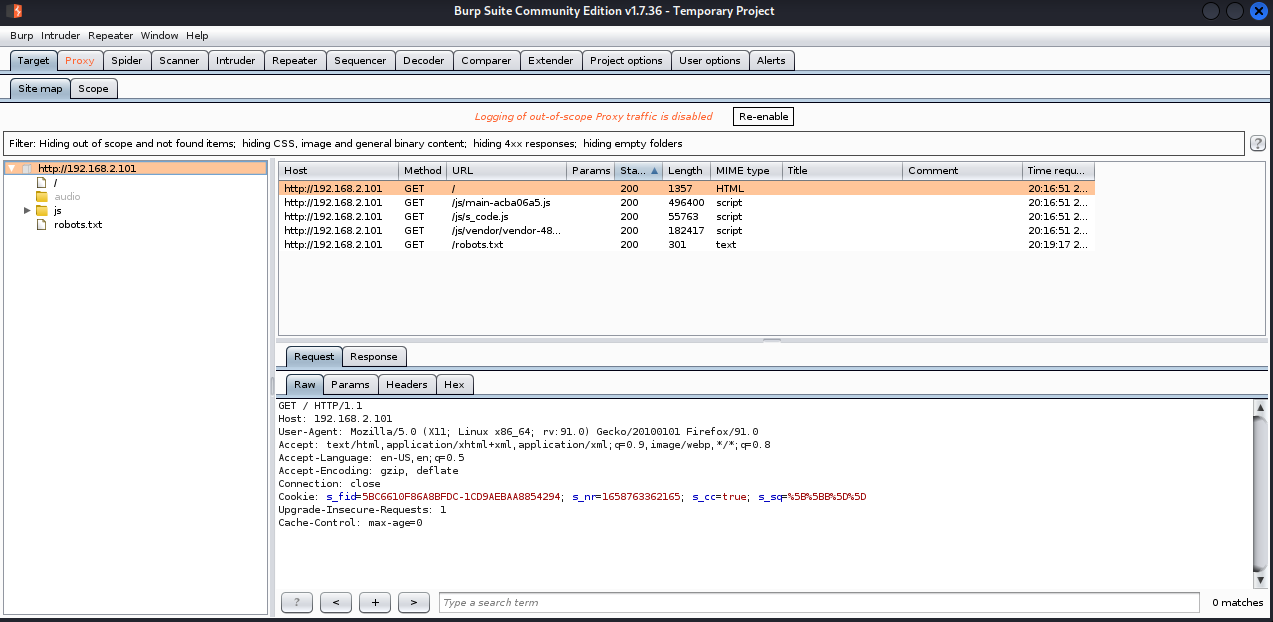
Y nos vamos al navegador y refrescamos página para capturar el trafico



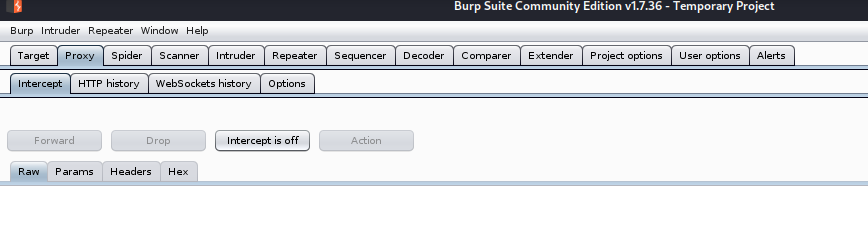
Damos forward varias veces para seguir



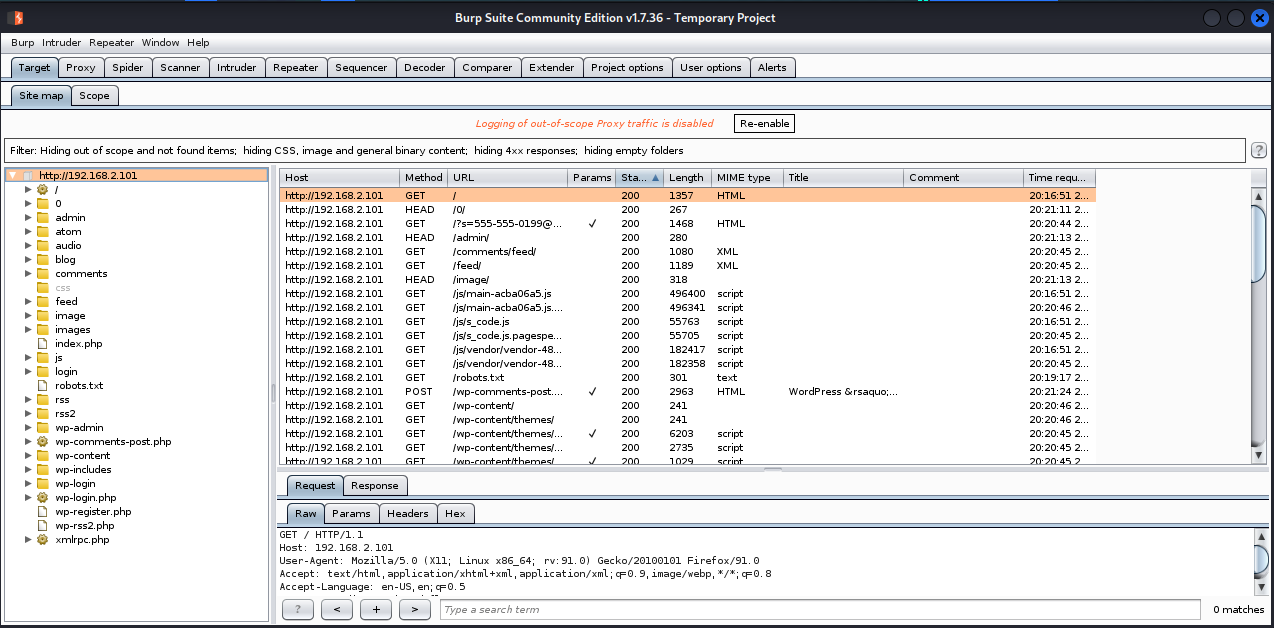
Vamos a la viñeta target y allí le damos clic derecho a <http://192.168.2.101/> y elegimos **add to scope** y después volvemos a dar clic derecho y le damos al spider to host para ver los directorios que tiene la página.



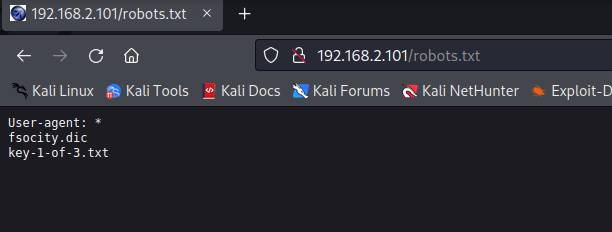
Le damos start al dirbuster para que trabaje a la par con burpsuite pero antes hay que apagar el proxy de burpsuite



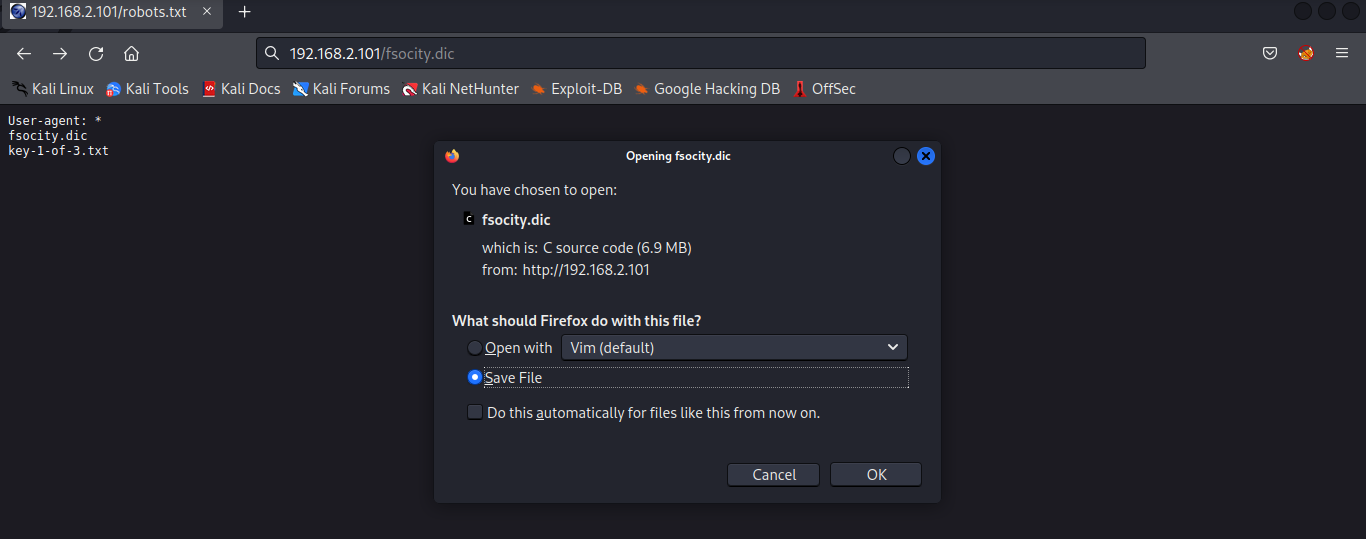
Ya ejecutados los dos programas podemos ver el resultado de los directorios



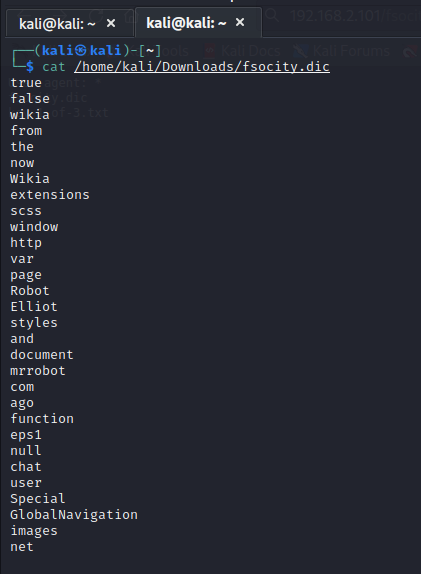
Y podemos observar un dato interesante **robots.txt** esta activo en esta pagina el cual nos puede dar información muy importante, el cual colocamos en el navegador <http://192.168.2.101/robots.txt>, pero primero ya podemos cerrar las herramientas ya que tenemos listado los archivos y directorios de la pagina web, también desactivamos el foxyProxy.

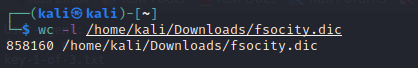


Y nos da 2 archivos lo cual para abrirlos colocamos el archivo en la URL



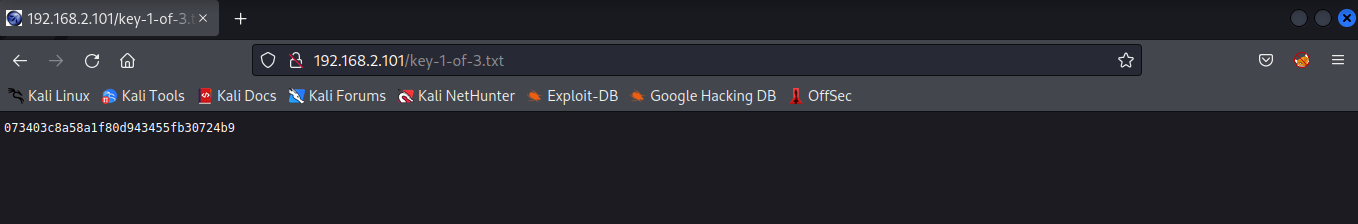
El cual guardamos el archivo y lo revisamos con **cat /home/kali/Download/fsocity.dic**





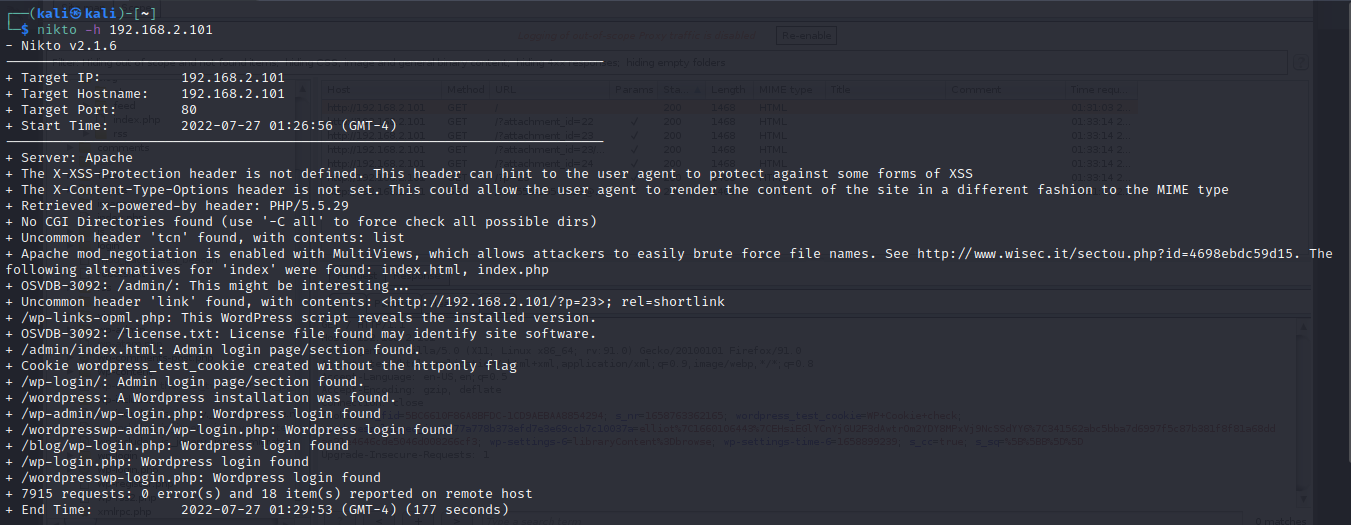
El cual es un diccionario de claves

Probamos con el otro archivo



Y obtenemos la primera clave **073403c8a58a1f80d943455fb30724b9**

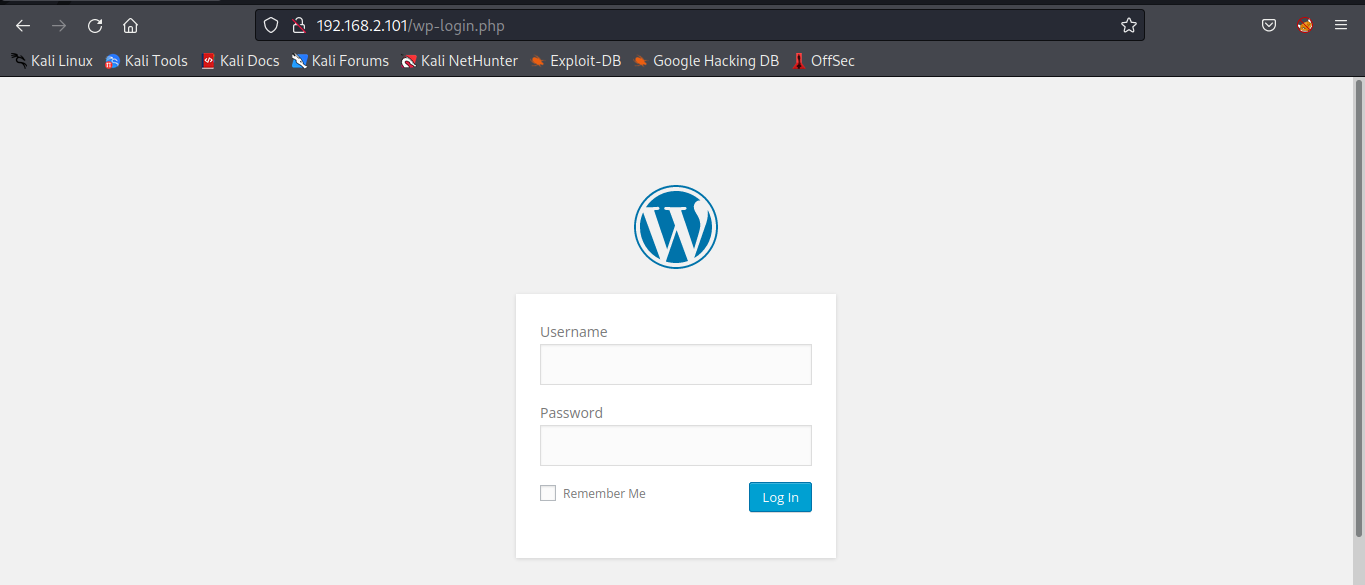
Tambien pudimos usar la herramienta nikto para buscar alguna vulnerabilidad o mala configuración.



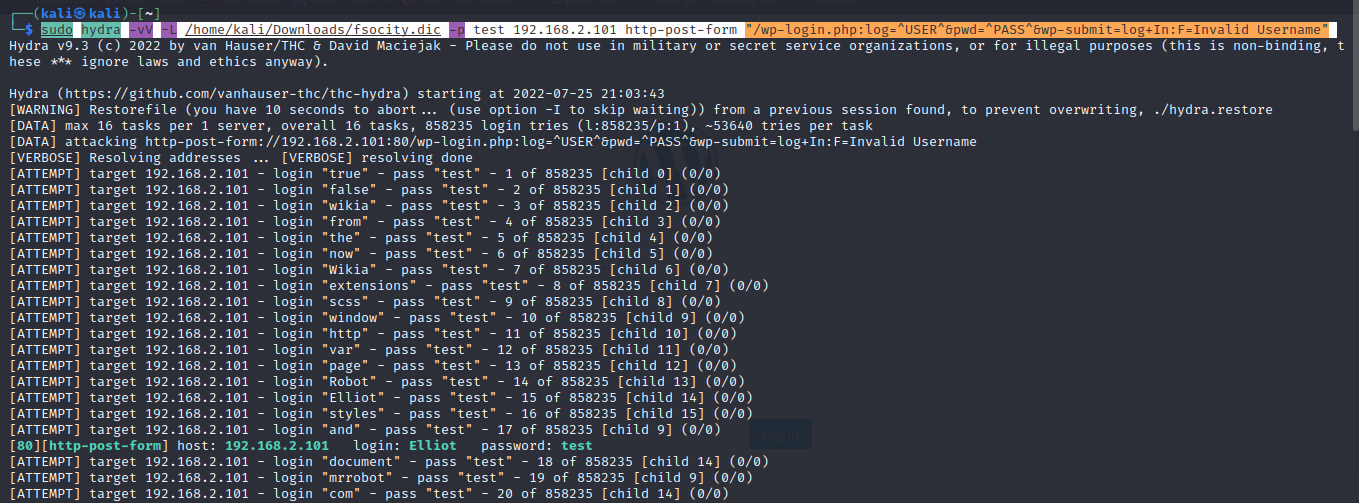
Y lo interesante de este resultado es que encontramos

OSVDB-3092: /license.txt : el cual podemos probar en el navegador pero no encontramos nada

Ahora con el diccionario de datos que obtuvimos haremos fuerza bruta con la herramienta **hydra** para conseguir el nombre del usuario y contraseña para tener las credenciales ya que vemos en los directorios wp-login.php que pertenece a paginas de wordpress

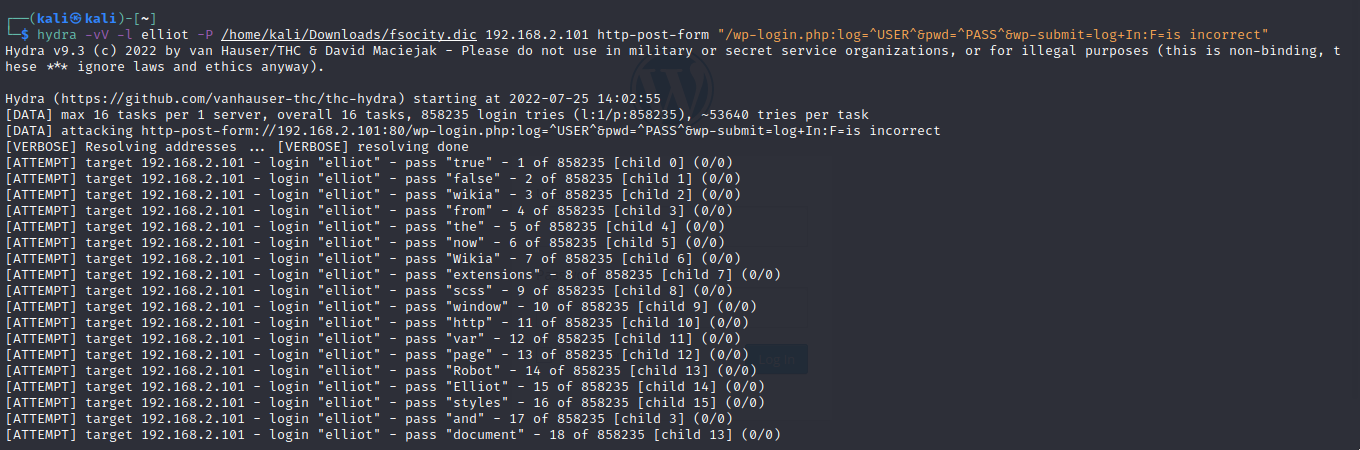


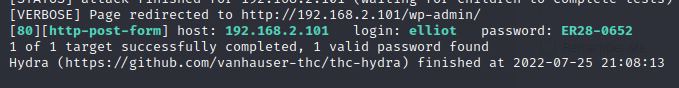
Usamos el comando **sudo hydra -vV -L /home/kali/Downloads/fsocity.dic -p test 192.168.2.101 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=log+In:F=Invalid Username"** para conseguir el usuario con el diccionario de datos que descargamos.



Y obtenemos el usuario: Elliot

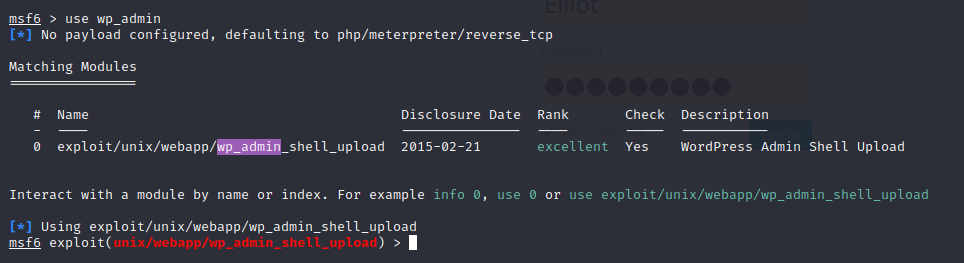
Ahora usamos el comando sudo **hydra -vV -l elliot -P /home/kali/Downloads/fsocity.dic 192.168.2.101 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=log+In:F=is incorrect"** para obtener el password



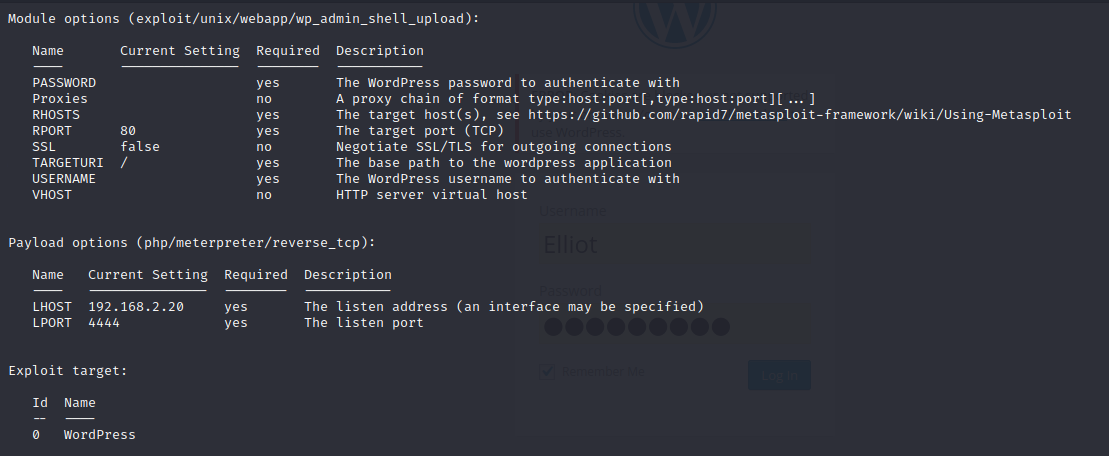


Y obtuvimos la contraseña: **ER28-0652**

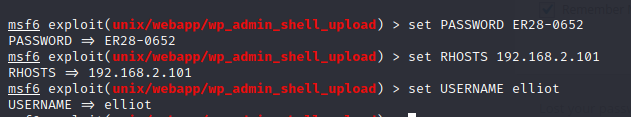
Ahora que tenemos las credenciales usaremos metasploit para lanzar un payload que instale un plugin en el wordpress y con ello nos permita crear una Shell. Usamos el comando **sudo msfconsole**  y buscamos el exploit que nos ayudara a subir la Shell.



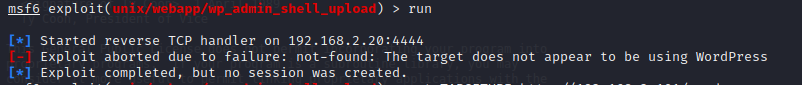
Con show options vemos las configuraciones



Y usamos los siguientes comandos



Una vez configurado el exploit usamos el comando run o exploit para ejecutar el ataque



Lastimosamente nos encontramos con un error, y según lo investigado el problema es en el código fuente del exploit lo cual editaremos para poder corregir usando el comando **sudo** **gedit /usr/share/metasploit-framework/modules/exploits/unix/webapp/wp\_admin\_shell\_upload.rb**

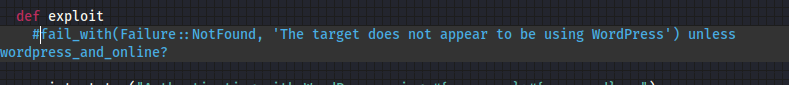


Buscaremos el codigo

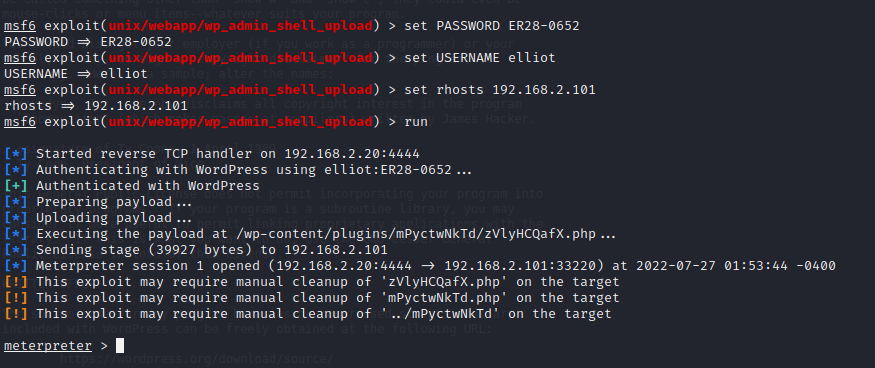
def exploit

#fail\_with(Failure::NotFound, 'The target does not appear to be using WordPress') unless wordpress\_and\_online?

Y le colocaremos un signo de numeral # para desactivarlo y guardamos cambios



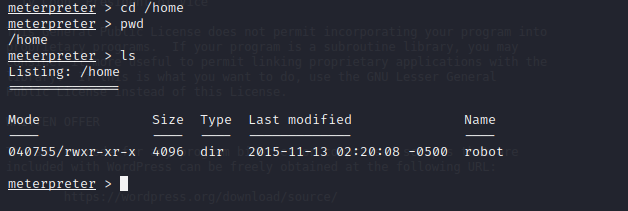
Y volvemos a probar el exploit



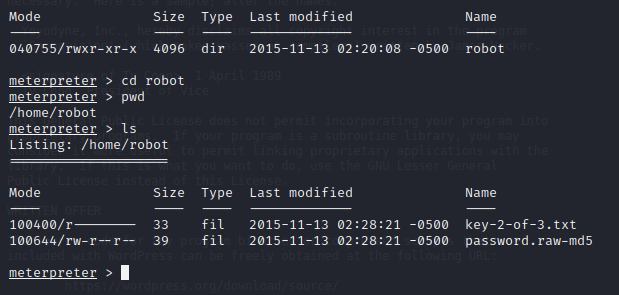
Y ahora si obtenemos el meterpreter que es una Shell con esteroides, probamos con pwd para ver la ubicación donde estamos



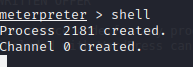
Nos desplazaremos al home para ver que archivos se encuentran en la raíz del sistema operativo de la maquina virtual, y damos el comando ls para ver que archivos tiene.



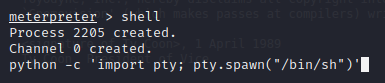
Observamos que hay una carpeta con nombre robot, ingresamos a ella con el comando cd y damos ls nuevamente para ver que contiene la carpeta robot

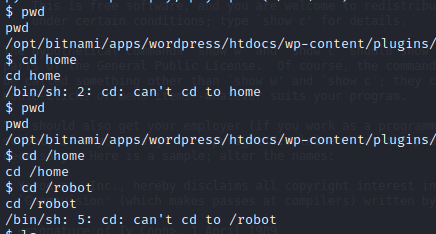


Podemos ver que hay 2 archivos interesantes, la llave 2 y un password md5, pero antes de continuar si nos molesta desplazarnos con el meterpreter podemos llamar la Shell de linux usando el comando Shell

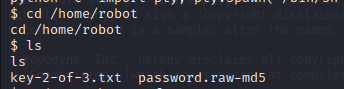


Y escribimos el comando python -c 'import pty; pty.spawn("/bin/sh")'





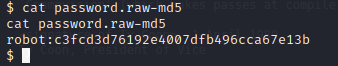
Nosotros seguiremos con meterpreter



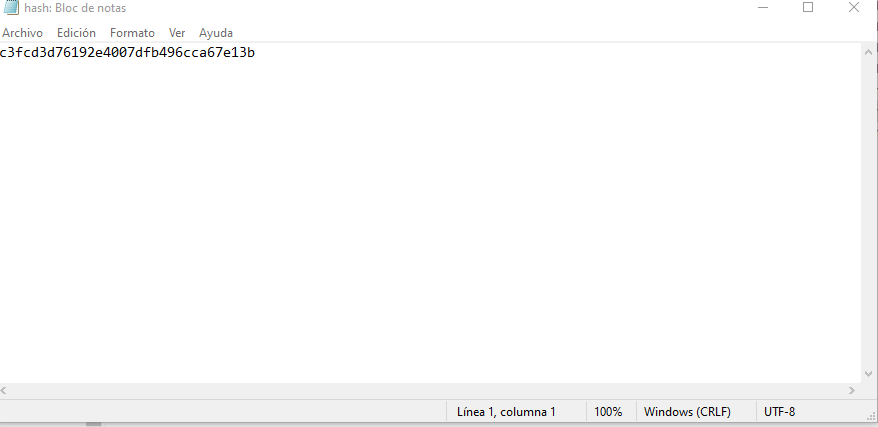
Veremos el contenido del primer archivo con el comando sudo cat nombreArchivo



Pero nos pide una contraseña para ver el archivo, por lo cual veremos el otro archivo

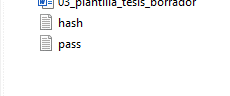


Creamos un archivo con la contraseña c3fcd3d76192e4007dfb496cca67e13b en D:/pass.txt en windows

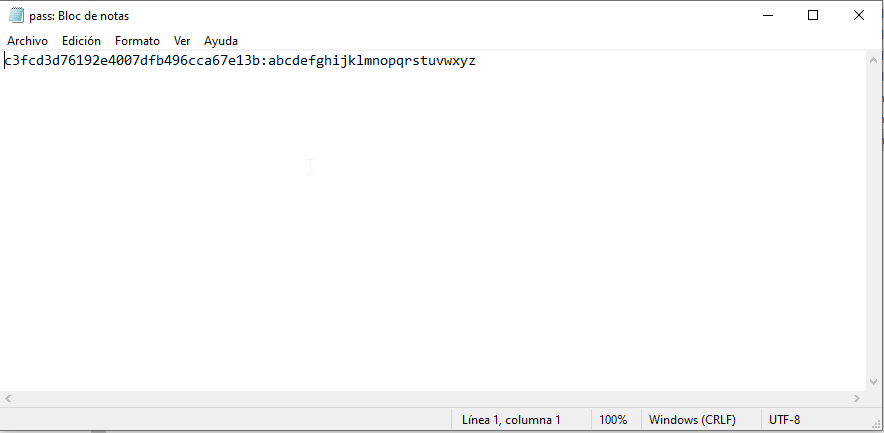


Ahora para descifrar la contraseña md5 usaremos la herramienta hashcat en windows con el comando  **hashcat -a 0 -m 0 D:\hash.txt C:\rockyou.txt -o D:\pass.txt**



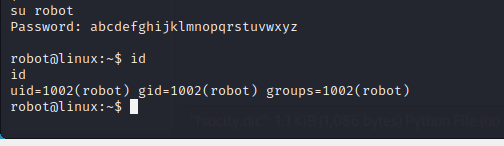


Y en pass encontramos la contraseña descifrada por hashcat

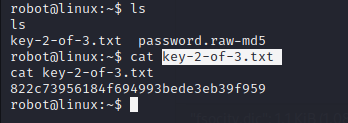


Ahora en la Shell escalamos privilegios con **su robot** e ingresamos la contraseña que obtuvimos



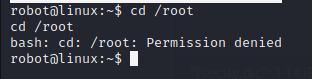


Y ya tenemos privilegios siendo el usuario robot y con ello ingresamos el comando cat key-2-of-3.txt



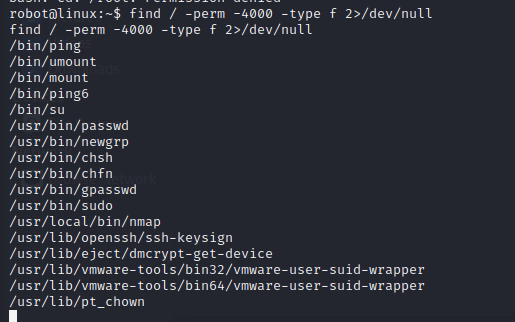
Y así obtenemos la segunda clave 822c73956184f694993bede3eb39f959

Ahora tratamos de ver si tenemos permisos para ver los archivos de la ubicación root

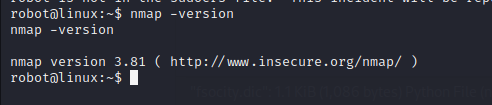


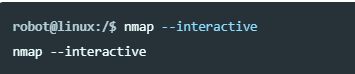
No tenemos permisos por lo cual tenemos que realizar nuevamente una escalada de privilegios por lo cual usaremos una técnica con el comando

**find / -perm -4000 -type f 2>/dev/null:** Comando que nos enlistara una gama de programas que pueden tener o generar problemas o errores si están mal configurados

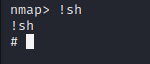


Usaremos la aplicacion nmap y principalmente nmap –interactive un programa que tiene permisos root y es una aplicación de versiones antiguas de nmap

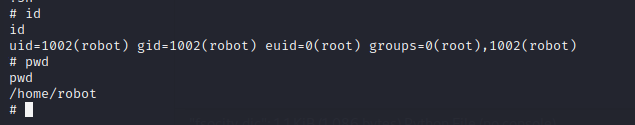




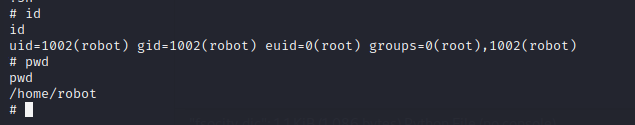
Usamos el comando !sh para llamar la shell



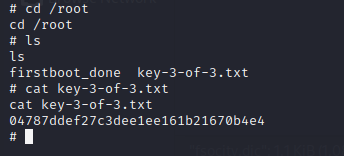
Verificamos los permisos



Y nos ubicamos en root



Y ahora si podemos ingresar a la raíz y damos ls para ver archivos



Y encotramos la ultima clave 04787ddef27c3dee1ee161b21670b4e4