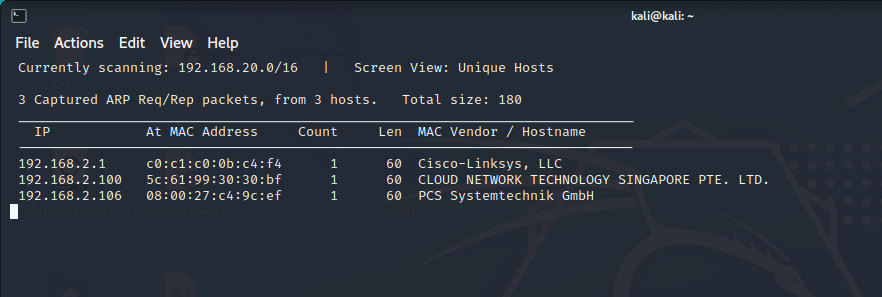
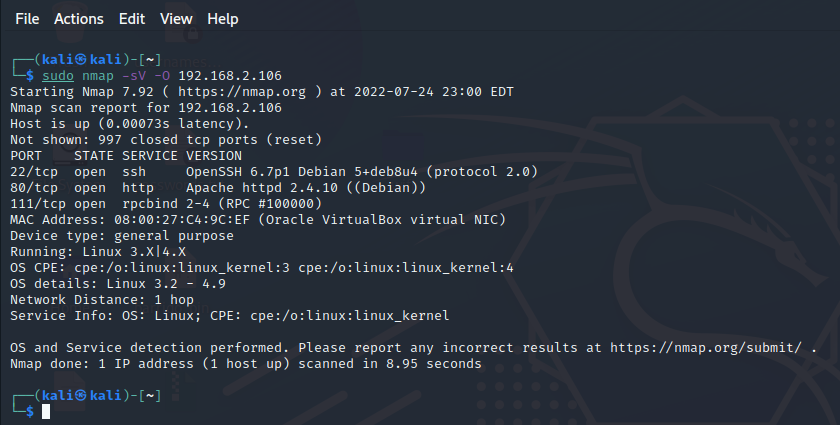
ANALISIS MAQUINA VULNERABLE TOPPO

Usamos netdiscovery para analizar la red teniendo como resultado

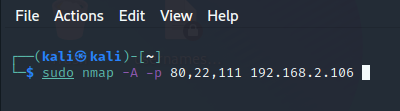


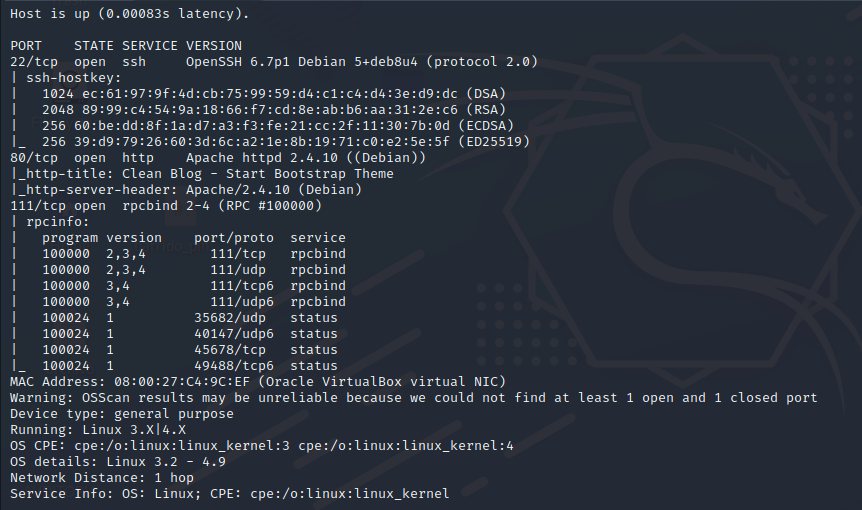
Identificamos que la red vulnerable es la maquina con IP 192.168.20.26

Haremos un escaneo con nmap

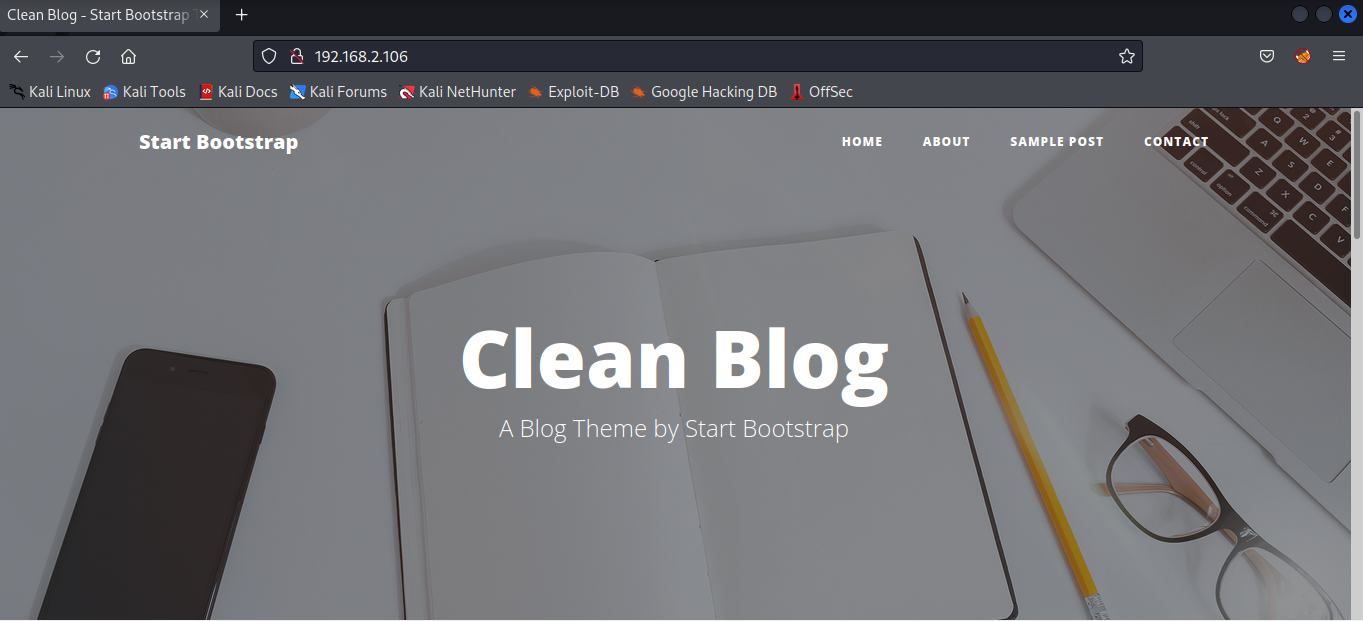


Haremos otro escaneo mas profundo para obtener las versiones y mas información de los puertos del anterior escaneo

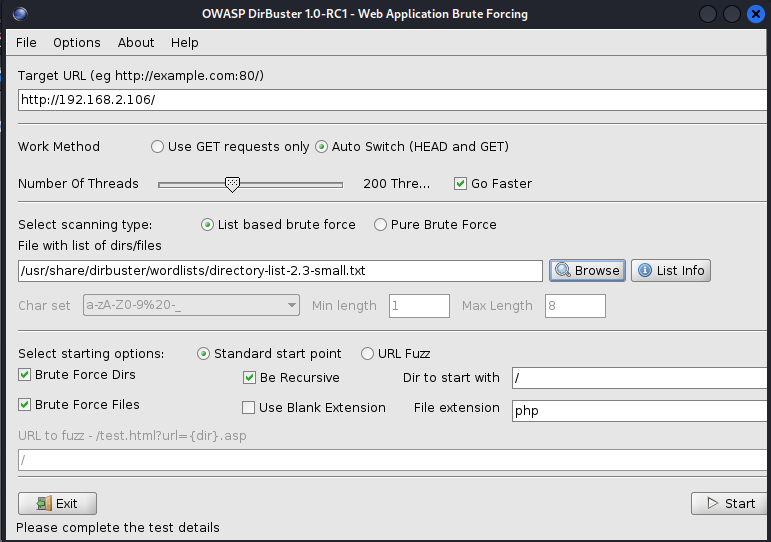




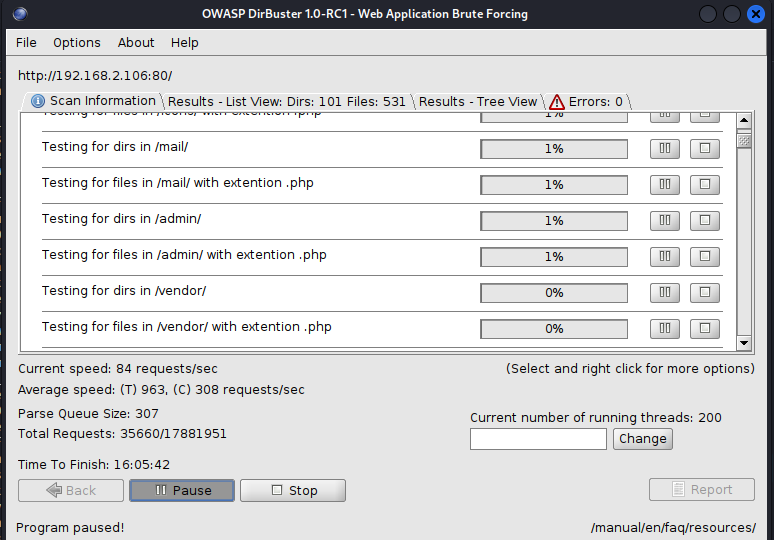
Probamos explotar la vulnerabilidad en el puerto 80 entonces en el navegador colocamos la dirección IP de la maquina TOPPO

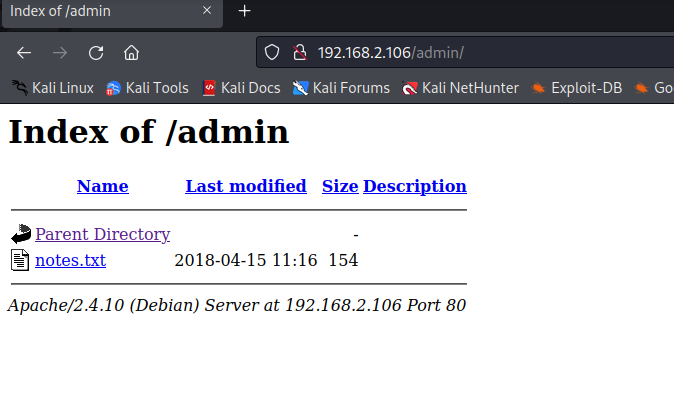


Usaremos la herramienta Dirbuster para analizar la pagina y encontrar informacion. Y configuramos la herramienta colocando el link de la pagina, usaremos diccionario de datos para realizar una fuerza bruta, usaremos el que trae por default Dirbuster

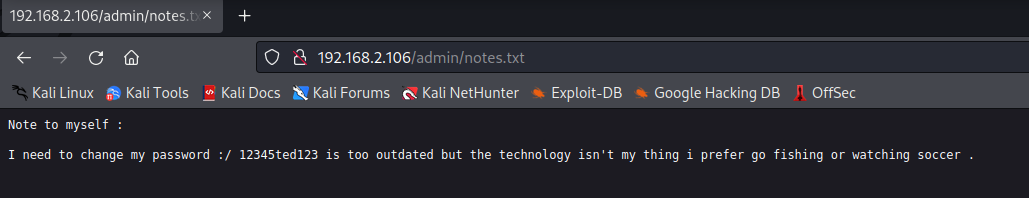


Podemos ver que los resultados nos va arrojando varios directorios los cuales podríamos ir probando en la URL de la página, normalmente el más interesante siempre es empezar por admin

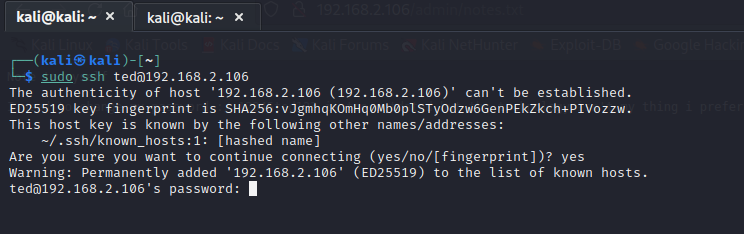


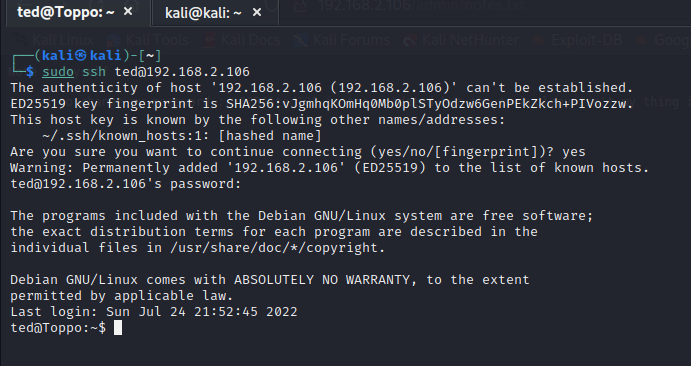


Podemos observar que pudimos ingresar al colocar admin en la URL y podemos observar un archivo notes.txt solo damos doble clic para ver si hay información relevante.

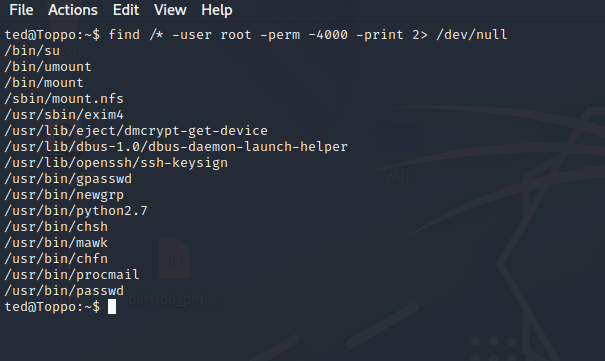


Nos muestra una contraseña y un posible usuario la cual probaremos con el servicio de SSH



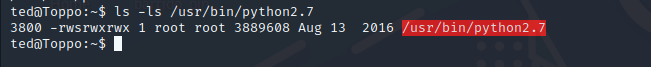
Y colocamos la contraseña 12345ted123  


Y tuvimos acceso a la maquina y comprobamos que el usuario se llama ted. Ahora comprobaremos que aplicaciones o servicios son root con el comando: find /\* -user root -perm -4000 -print 2> /dev/null



Y podemos observar que entre los servicios con privilegios root tenemos a Python el cual nos permitirá usar script para abrir cualquier tipo de Shell

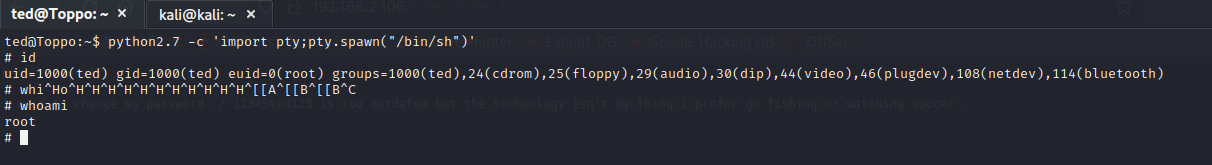
Comprobamos los permisos de Python usando el comando ls -ls /usr/bin/python2.7



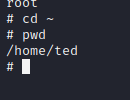
METODOS PARA EJECUTAR SHELL

Metodo 1: Con Python

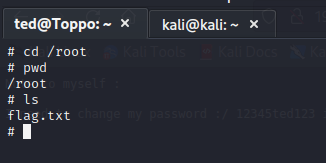
Usamos el comando **python2.7 -c 'import pty;pty.spawn("/bin/sh")'** para obtener la shell



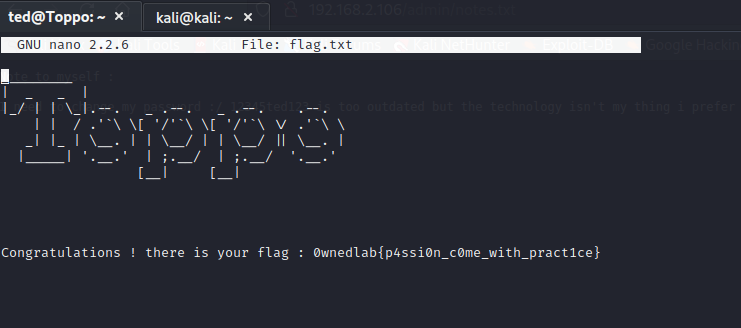
Ahora revisaremos los archivos que se encuentran en la raíz con cd ~ y con pwd confirmamos



Ahora nos dirigimos a cd /root y comprobamos con pwd y listamos archivos con ls

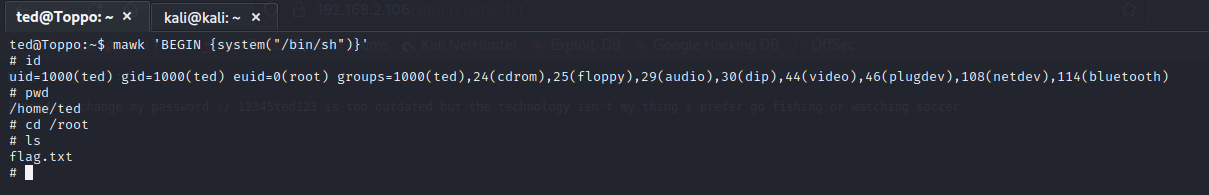


Encontramos un archivo con nombre flag.txt y abrimos el archivo con nano flag.txt



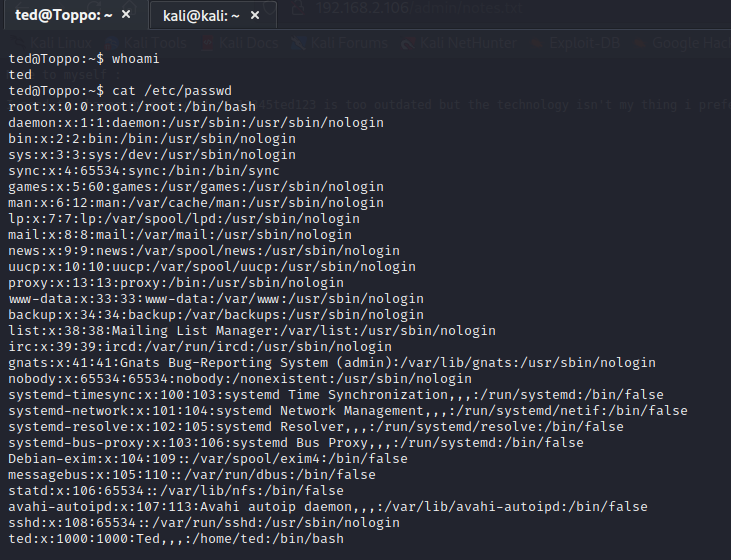
METODO 2: Usando Mawk

Al ejecutar el siguiente podemos utilizar mawk para devolver una Shell intectativa con privilegios de root. Usamos el comando **mawk 'BEGIN {system("/bin/sh")}'**

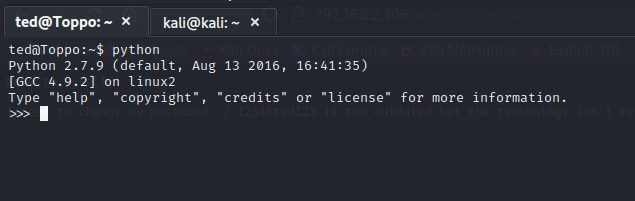


**METODO 3: Creando un usuario**

Verificamos con whoami el usuario y con cat /etc/passwd los usuarios que tiene creada la maquina



Vamos a ejecutar el comando Python para que nos aparezca su terminal



Escribimos el siguiente código para agregar el usuario

>>> import crypt

>>> username = "hacker"

>>> password = "hacker"

>>> salt = "hacker"

>>> cryp\_hash = crypt.crypt(password, salt)

>>> print(cryp\_hash)

ha2TYUFs4D5oM

>>> user\_line = "%s:%s:0:0:root:/root:/bin/bash" % (username, cryp\_hash)

>>> print(user\_line)

hacker:ha2TYUFs4D5oM:0:0:root:/root:/bin/bash

>>>

>>> file = "/etc/passwd"

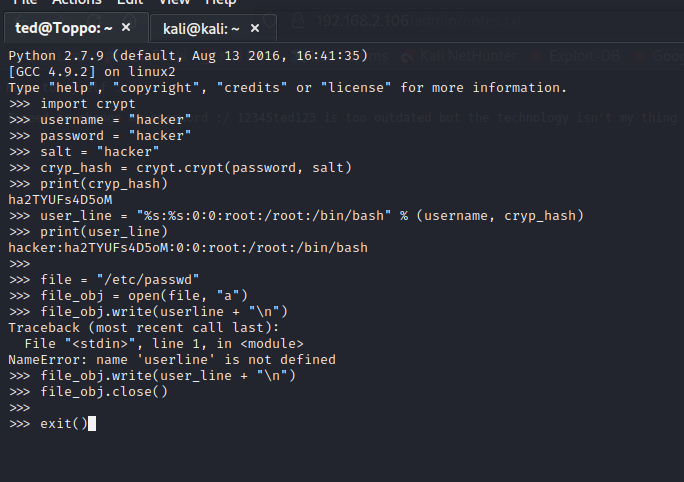
>>> file\_obj = open(file, "a")

>>> file\_obj.write(user\_line + "\n")

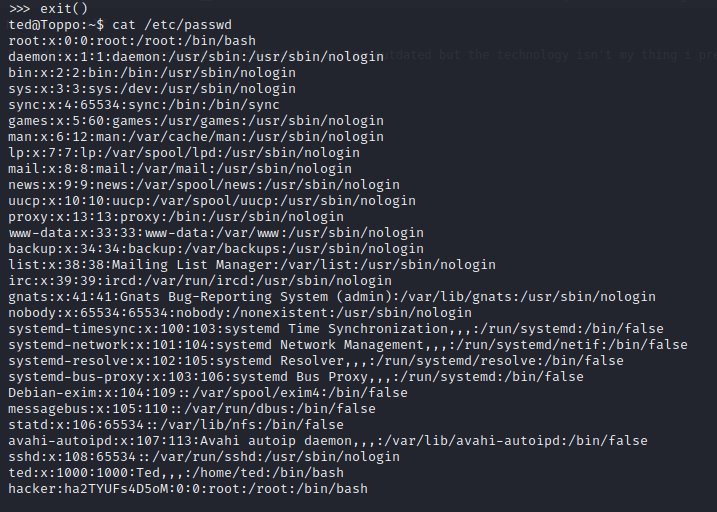
>>> file\_obj.close()

>>>

>>> exit()



Ahora comprobamos si el usuario fue creado con el comando cat /etc/passwd



Y para finalizar probamos a salirnos de la sesión y probamos a conectarnos con el usuario creado

Nota: Cambiamos de red ya que con la que trabajamos anteriormente tuvo problemas.

