APLICANDO HERRAMIENTAS A LAS CVE

Giancarlo Soto

Docente Franco Calderón

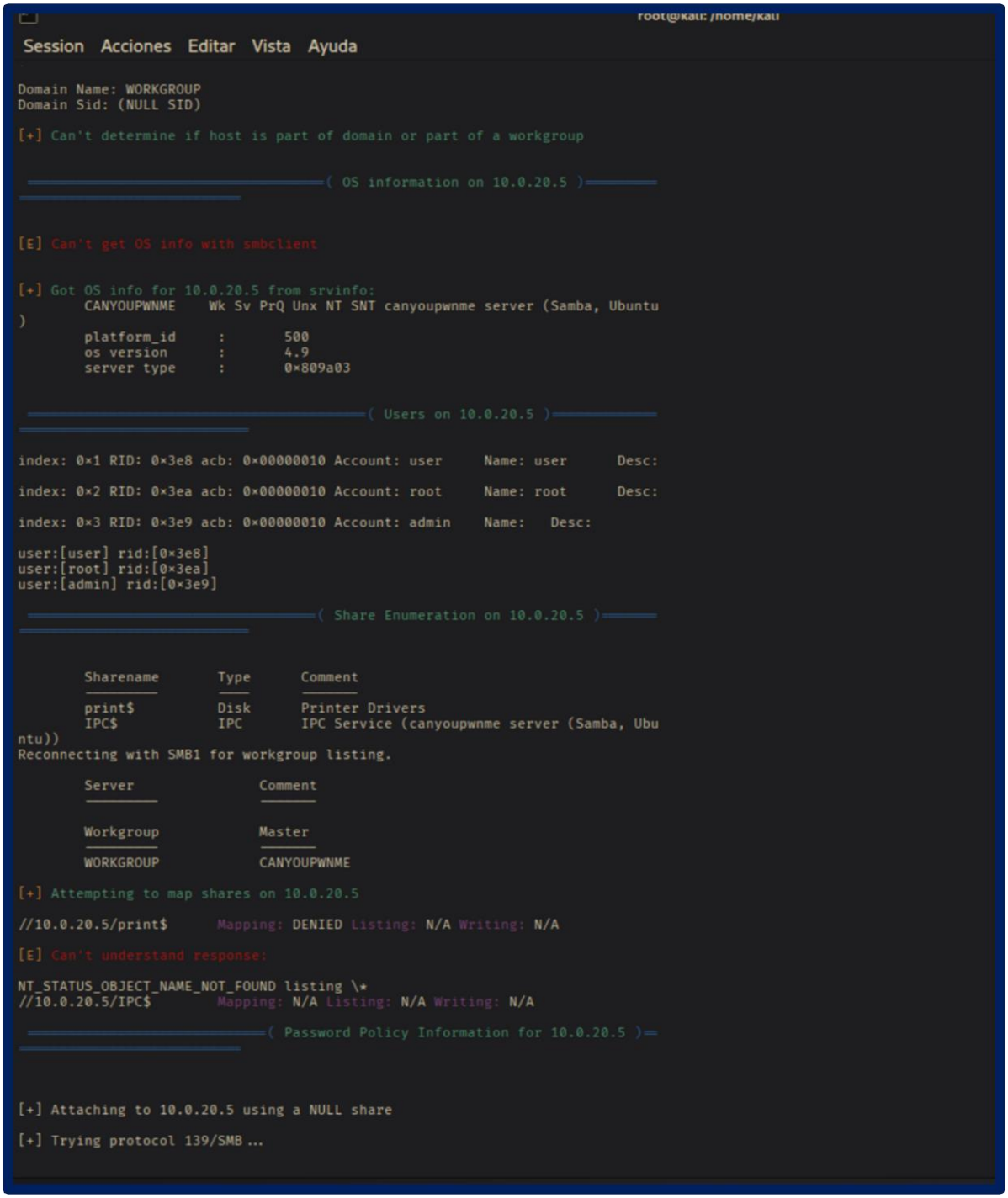
Carrera Ingeniería en Informática

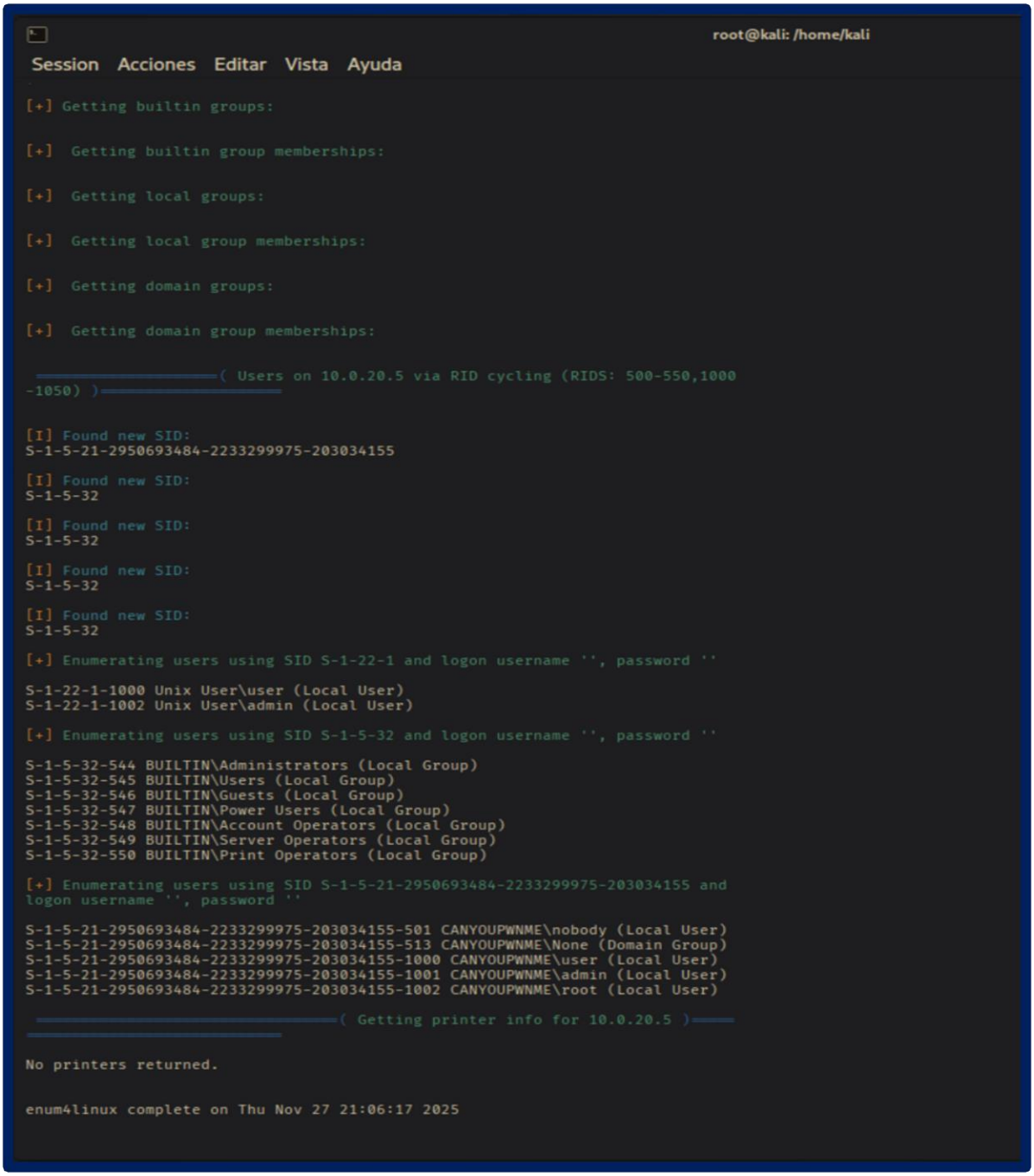
Contenido

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 N
IC)

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/enum4li
nux/ ) 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, no
ne


 ==========( 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:
CANYOUPWNME Wk Sv PrQ Unx NT SNT canyoupwnme server (Samba, Ubuntu
)
platform_id : 500
os version : 4.9
server type : 0×809a03
(Users on 10.0.20.5)
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: user Name: user Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: root Name: root Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: admin Name: Desc:
user:[user] rid:[0×3e8]
user:[root] rid:[0×3ea]
user:[admin] rid:[0×3e9]
(Share Enumeration on 10.0.20.5)
Sharename Type Comment
print$ Disk Printer Drivers
IPC$ IPC IPC Service (canyoupwnme server (Samba, Ubu
ntu))
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
WORKGROUP CANYOUPWNME
[+] 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 ...

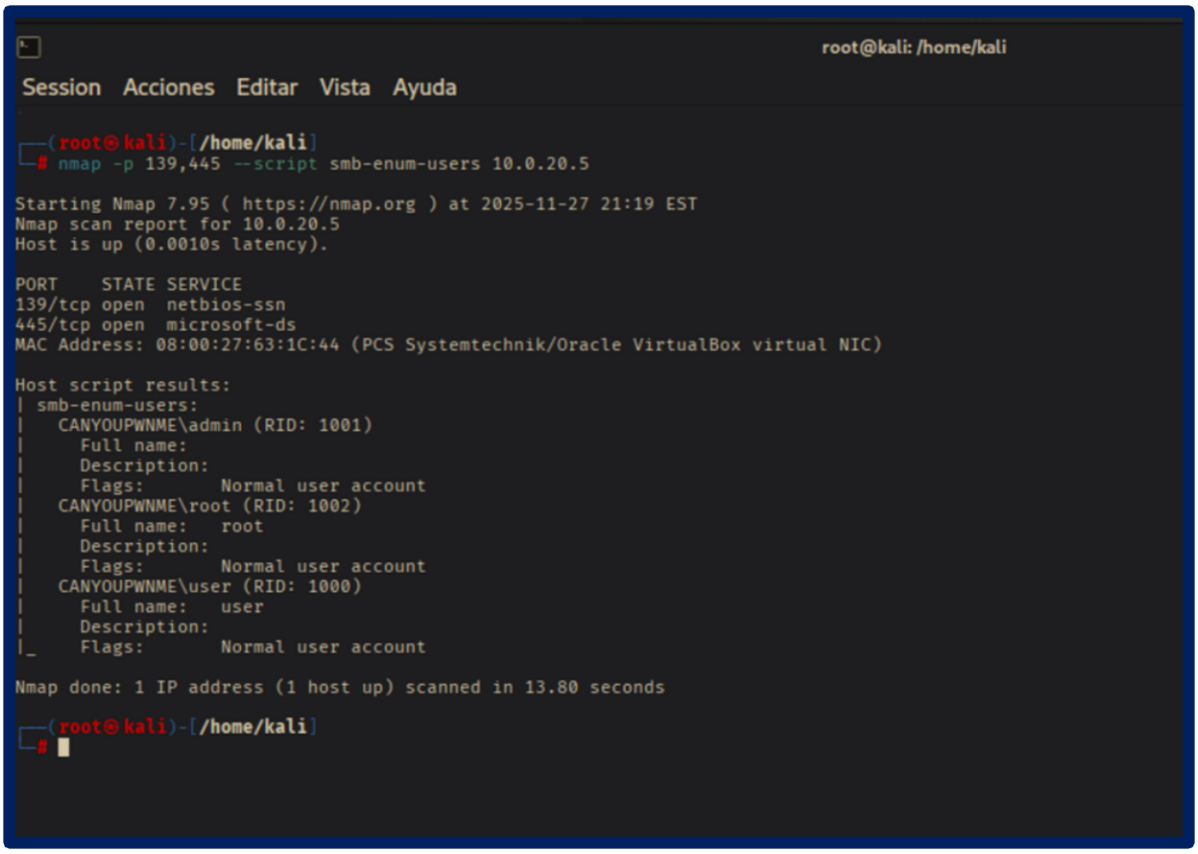


Hallazgos:

- 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.

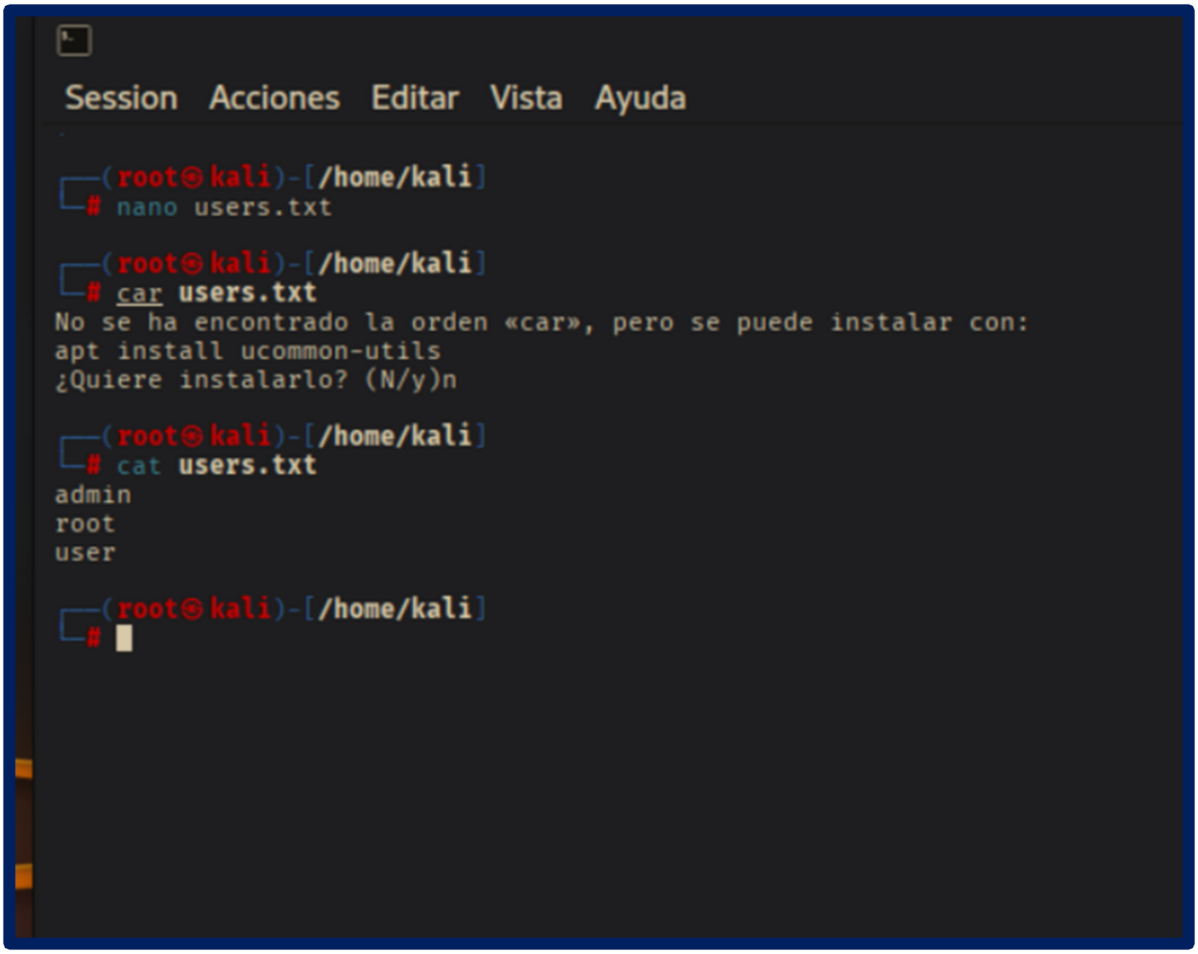


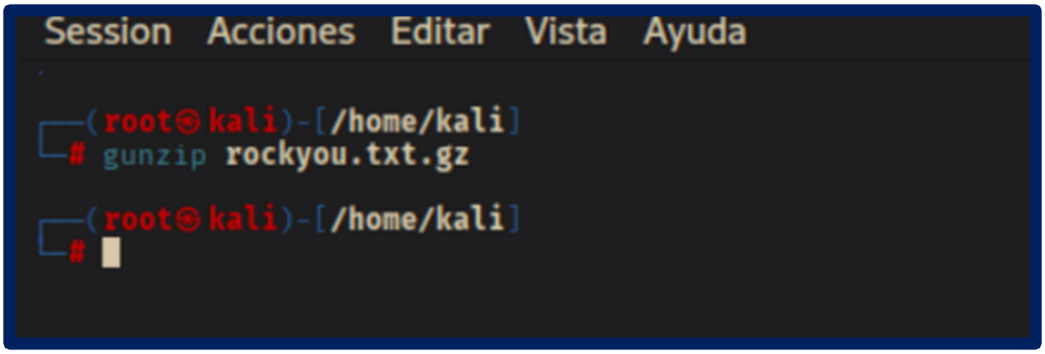
Lista de Usuarios Confirmados: Gracias a este script, se confirmaron los siguientes usuarios activos en el sistema:

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

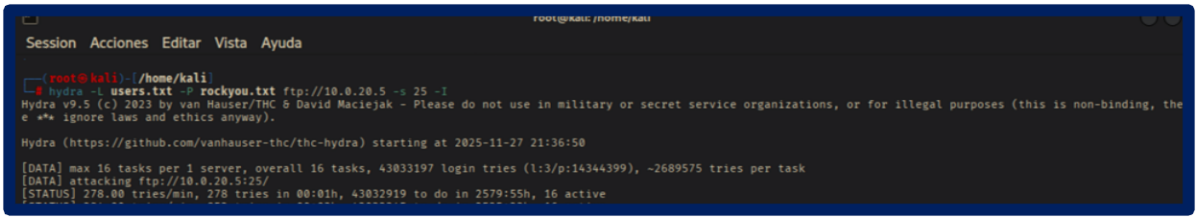
3. Preparación del Ataque

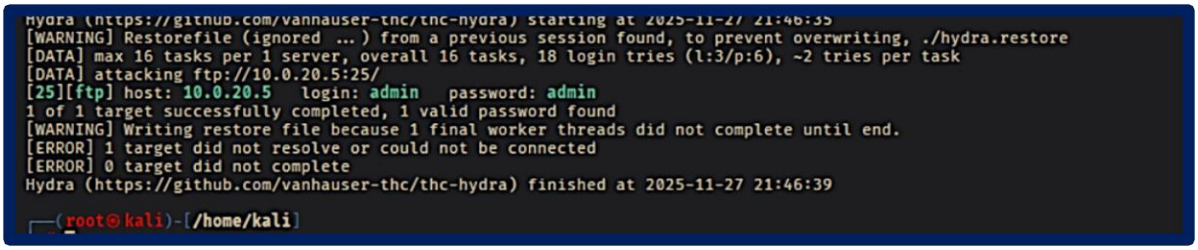
Con los usuarios identificados, se procedió a crear un archivo de objetivos (users.txt). Para las contraseñas, se preparó el entorno descomprimiendo el diccionario rockyou.txt.gz incluido en Kali Linux.





4. Ataque de Fuerza Bruta





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.