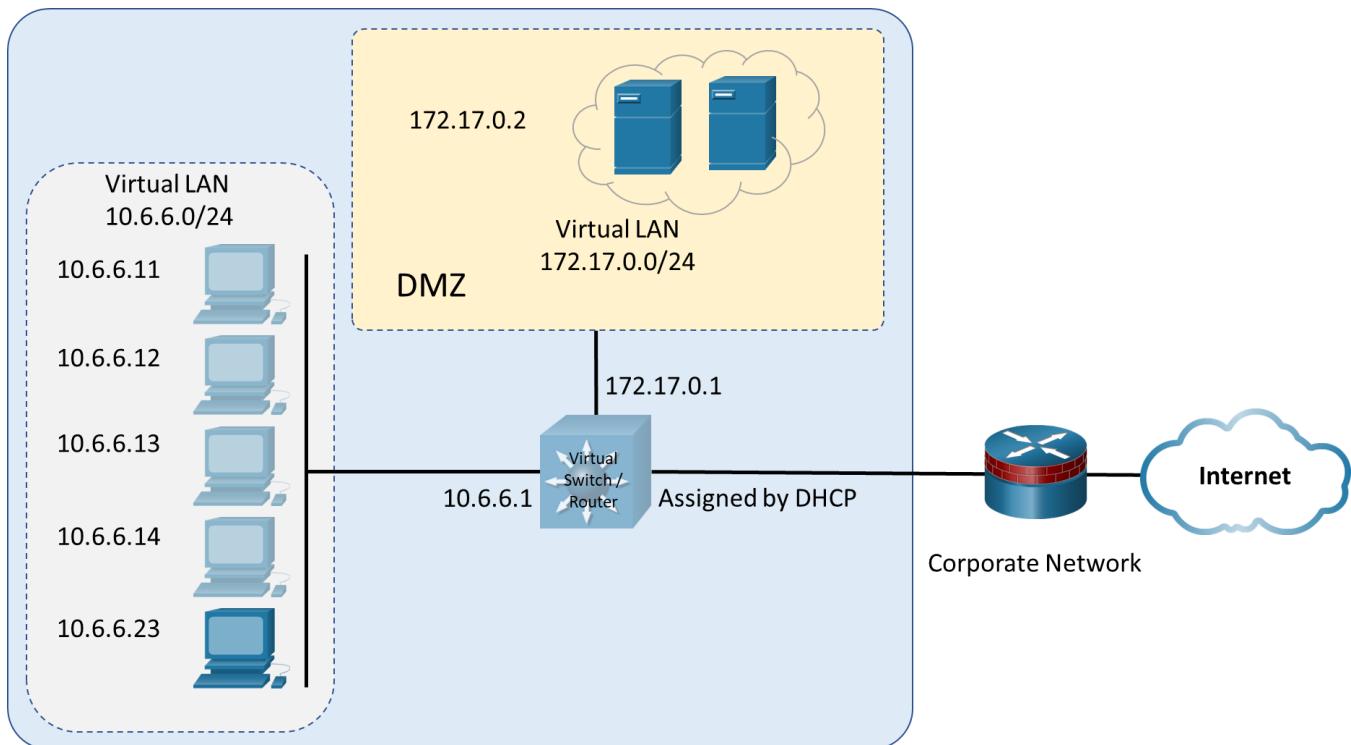


Práctica de laboratorio: Escaneo de vulnerabilidades SMB con enum4linux

Topología



Objetivos

Enum4linux es una herramienta para enumerar información de Windows y Samba. Samba es una aplicación que permite a los clientes de Linux y Apple participar en redes de Windows. Permite a los clientes que no son de Windows utilizar el protocolo Server Message Block (SMB) para acceder a los servicios de archivos e impresión. Los servidores Samba pueden participar en un dominio de Windows, tanto como cliente como servidor.

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Iniciar enum4linux y explore sus capacidades.
- Identificar los equipos con servicios SMB en ejecución.
- Use enum4linux para enumerar usuarios y recursos compartidos de archivos de red.
- Utilice smbclient para transferir archivos entre sistemas.

Aspectos básicos/Situación

Las redes de servidores de Windows mal administradas y protegidas son un gran riesgo para la seguridad. Los evaluadores de penetración deben descubrir cualquier vulnerabilidad en las funciones de uso compartido de archivos e impresoras que puedan dejar a una organización vulnerable a los ataques. En esta actividad, explorará las capacidades de la herramienta enum4linux para enumerar la información de uso compartido de

usuarios y archivos de los servidores Samba. Por último, utilizará la utilidad `smbclient` para transferir archivos entre sistemas.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker

Instrucciones

Parte 1: Inicie enum4linux y explore sus capacidades.

Paso 1: Verifique que enum4linux esté instalado y vea el archivo de ayuda.

- a. Cargue Kali Linux con el nombre de usuario **kali** y la contraseña **kali**. Abra una sesión de terminal desde la barra de menús en la parte superior de la pantalla.
 - b. La mayoría de los comandos enum4linux deben ejecutarse como root, por lo tanto, use el comando **sudo su** para obtener acceso root persistente.

En el indicador, ingrese el comando para ver el archivo de ayuda enum4linux.

```
└──(kali㉿kali)-[~]
└$ sudo su
[sudo] password for kali:
└──(root㉿kali)-[/home/kali]
└# enum4linux -help
```

El archivo de ayuda contiene la sintaxis y las opciones disponibles para enumerar la información del host y el servidor en las redes que usan SMB.Enum4linux requiere que Samba esté instalado en el sistema host, en este caso la computadora Kali Linux, porque depende de las utilidades integradas de Samba.

¿Qué utilidades de Samba indica el archivo de ayuda que utiliza la herramienta enum4linux?

rpcclient, net, nmblookup y smbclient

Paso 2: Investigue los términos asociados con las funciones de SMB.

Es posible que muchos términos utilizados en las funciones de Windows y SMB no le resulten familiares, por lo que el resultado de los comandos enum4linux puede ser difícil de interpretar al principio. Utilice un motor de búsqueda en Internet para encontrar la definición de los términos enumerados.

Identificador relativo (RID)

Identifica de forma exclusiva un usuario, un grupo, un sistema o un dominio.

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays the Wikipedia article 'Identificador relativo'. The page content describes the RID as a unique identifier assigned to objects at creation, used by Active Directory. It also mentions the 'maestro de ID relativo' (RID master) function. Below the main text, there are sections for 'Véase también' and 'Referencias'. On the right side of the page, there is a sidebar titled 'Apariencia' with various styling options like font size, color, and background. The bottom of the page includes a note about being a stub and categories like 'Kernel de Windows NT' and 'Esbozos de computación'.

Identificador de seguridad (SID)

The screenshot shows a Microsoft Edge browser window displaying the Microsoft Learn article 'Identificadores de seguridad'. The left sidebar contains a navigation menu with topics like 'Identidades especiales', 'Cuentas de servicio', 'Cuentas Microsoft', and 'Replicación de Active Directory'. The main content area starts with a section titled '¿Qué son los SID?'. It explains that a SID is a unique identifier for security entities. The article then discusses how SIDs are used in Windows Server, mentioning the SID master and its role in identifying users and groups. A note at the bottom states that the content applies to specific Windows versions. The right sidebar contains links to related articles such as '¿Qué son los SID?', 'Cómo funcionan los SID', and 'SID e identificadores únicos globales'.

Práctica de laboratorio: Escaneo de vulnerabilidades SMB con enum4linux

Identifica de forma exclusiva a usuarios y grupos dentro del dominio local. Único a nivel global, por lo que también puede funcionar entre dominios.

Controlador de dominio (DC)

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays the English Wikipedia article on "Controlador de dominio". The page content describes a domain controller (DC) as a server that handles authentication requests from users and manages group policies. It lists various software components like Windows Server, Active Directory, and LDAP. The sidebar on the left shows navigation links for the article, and the right side has a "Apariencia" (Appearance) settings panel.

El controlador de dominio es un servidor que administra las solicitudes de seguridad de red y de identidad. Autentica a los usuarios y determina si pueden acceder a los recursos de TI del dominio.

Protocolo de acceso al directorio ligero (LDAP)

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays the English Wikipedia article on "Protocolo ligero de acceso a directorios". The page defines LDAP as a standard protocol for directory services, used for authentication and authorization. It details its structure, operations (such as search, add, delete), and security features. The sidebar includes a "Protocolo ligero de acceso a directorios" summary table and a "Conjunto de protocolos de Internet" section listing related protocols like DNS, HTTP, and SSL/TLS. The right side has a "Apariencia" settings panel.

un protocolo de acceso al directorio que permite que los servicios y clientes que utilizan servicios de nombres LDAP se comuniquen.

Práctica de laboratorio: Escaneo de vulnerabilidades SMB con enum4linux

Grupo de trabajo

The screenshot shows a Wikipedia article page for "Grupo de trabajo (redes informáticas)". The page content discusses what a workgroup is in computer networking, mentioning it's a group of computers connected on a LAN that share resources. It also covers Windows Workgroups and their history in Windows versions. Below the main text are sections for "Véase también", "Referencias", and "Enlaces externos". On the right side of the page, there are settings for "Apariencia" (Appearance) including font size (Pequeño, Estándar, Grande), width (Ancho, Estándar, Extenso), and color (Automático, Luz, Oscuro). The bottom of the page includes a footer with categories like "Tecnología Windows", "Redes informáticas", and "Códigos auxiliares de Microsoft Windows".

un grupo de equipos independientes que se administran de forma independiente.

Parte 2: Utilice Nmap para buscar servidores SMB.

Paso 1: Escanee las redes virtuales para encontrar posibles objetivos.

Una forma de identificar posibles objetivos para la enumeración de SMB es examinar los puertos abiertos. En una práctica de laboratorio anterior, utilizó Nmap para buscar y enumerar los puertos abiertos en los sistemas de destino. Los puertos abiertos comunes en los servidores SMB son:

TCP 135	RPC
TCP 139	Sesión de NetBIOS
TCP 389	Servidor LDAP
TCP 445	Servicio de archivos SMB
TCP 9389	Servicios web de Active Directory
TCP/UDP 137	Servicio de nombres NetBIOS
UDP 138	Datagrama de NetBIOS

- Se incluyen dos redes virtuales en la VM de Kali con contenedores de Docker. Utilice el comando **nmap -sN** para buscar los servicios disponibles en los hosts de la red virtual 172.17.0.0.

Nota: **sudo** no es necesario si ejecutó el comando **sudo su** anterior.

```
└─(root㉿kali)-[~/home/kali]
└─# nmap -sN 172.17.0.0/24
```

¿Qué revela Nmap sobre los hosts en la red 172.17.0.0/24?

```
[root@Kali ~]# nmap -sT 172.17.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2025-11-03 08:15 UTC
Nmap scan report for metaspstable.vm (172.17.0.2)
Host is up (0.000050s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    filtered telnet
22/tcp    open/filterd ssh
23/tcp    open/filterd telnet
25/tcp    open/filterd smtp
80/tcp    open/filterd http
139/tcp   open  netbios-ssn
445/tcp   open/filterd microsoft-ds
443/tcp   open/filterd https
513/tcp   open/filterd login
1389/tcp  open/filterd msrpc
1399/tcp  open/filterd netregistry
1524/tcp  open/filterd ingreslock
2212/tcp  open/filterd netlogon-ftp
3389/tcp  open/filterd msrdp
5432/tcp  open/filterd postgresql
4444/tcp  open/filterd http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap scan report for 172.17.0.1
Host is up (0.000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 8.76 seconds
[root@Kali ~]
```

Solo hay un host. 172.17.0.2.

¿Qué puertos están abiertos en el host que identifican los servicios SMB en ejecución? ¿Cómo llama Nmap a estos servicios?

TCP 139 netbios-ssn y TCP 445 microsoft-ds

- b. Realice un análisis de **nmap -sN** en la subred **10.6.6.0/24**.

```
[root@kali ~]# nmap -sN 10.6.6.0/24
```

¿Hay posibles equipos de destino en esta subred que ejecuten servicios SMB? ¿Qué computadora o computadoras? ¿Cómo lo sabe?

Práctica de laboratorio: Escaneo de vulnerabilidades SMB con enum4linux

```
(root㉿kali)-[~/home/kali]
└─# enum4linux -U 10.6.6.23
Starting Nmap 7.7.0 ( https://nmap.org ) at 2025-11-03 00:13:06 UTC
Nmap scan report for webgot.vm (10.6.6.11)
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE    SERVICE
80/tcp    open     http-proxy
8088/tcp  open/filtered http-proxybook
9881/tcp  open/filtered tor-port
MAC Address: 02:42:0A:0B:0C:0D (Unknown)

Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE    SERVICE
80/tcp    open     http
MAC Address: 02:42:0A:0B:0C:0E (Unknown)

Nmap scan report for dom1.vm (10.6.6.13)
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE    SERVICE
80/tcp    open     http
8080/tcp  open/filtered http
MAC Address: 02:42:0A:0B:0C:0F (Unknown)

Nmap scan report for multilidee.vm (10.6.6.14)
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE    SERVICE
3306/tcp  open/filtered mysql
MAC Address: 02:42:0A:0B:0C:0G (Unknown)

Nmap scan report for gravemin.vm (10.6.6.23)
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    filtered
22/tcp    open/filtered ssh
53/tcp    open/filtered domain
80/tcp    open     http
139/tcp   open/filtered netbios-ssn
445/tcp   open/filtered microsoft-ds
MAC Address: 02:42:0A:0B:0C:0H (Unknown)

Nmap scan report for 10.6.6.24
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE    SERVICE
80/tcp    open     http
8080/tcp  open/filtered http
MAC Address: 02:42:0A:0B:0C:0I (Unknown)

Nmap scan report for 10.6.6.23
Host is up (0.000020s latency).
```

Sí, 10.6.6.23. Tiene los puertos 139 y 445 abiertos.

Parte 3: Use enum4linux para enumerar usuarios y recursos compartidos de archivos de red.

En esta parte, usará enum4linux para descubrir más información sobre los dos objetivos potenciales.

Paso 1: Realice un análisis enum4linux en el destino 172.17.0.2.

En la parte 1, paso 1c, utilizó la página de ayuda de enum4linux para conocer las opciones disponibles para enumerar los posibles objetivos. Las opciones más comunes son:

- U busca usuarios configurados
- S obtiene una lista de archivos compartidos
- G obtiene una lista de los grupos y sus miembros
- P enumera las políticas de contraseñas
- i obtiene una lista de impresoras

- Utilice la opción **enum4linux -U** para enumerar los usuarios configurados en el 172.17.0.2 de destino. Recuerde que los comandos enum4linux requieren permisos de root para ejecutarse.

```
└─(root㉿kali)-[~/home/kali]
└─# enum4linux -U 172.17.0.2
```

Práctica de laboratorio: Escaneo de vulnerabilidades SMB con enum4linux

```
[root@kali:~/kali] enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov  3 00:37:00 2025
Target ..... 172.17.0.2
RID Range ..... 500-550,1000-1050
Username ..... 
Password ..... 
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[+] Got domain/workgroup name: WORKGROUP

[+] Session check on 172.17.0.2

[*] Server 172.17.0.2 allows sessions using username '', password ''

Domain Name: WORKGROUP
Domain SId: (NULL SID)
[*] Can't determine if host is part of domain or part of a workgroup

[+] Users on 172.17.0.2
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x1f6 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0x4 RID: 0x482 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x1f7 acb: 0x00000011 Account: ssh Name: ssh Desc: (null)
index: 0x6 RID: 0x0ba acb: 0x00000010 Account: user Name: just a user_113 Desc: (null)
index: 0x7 RID: 0x428 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x1f4 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x9 RID: 0x3f4 acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0x10 RID: 0x1f5 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x11 RID: 0x3e5 acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0x12 RID: 0x1f6 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0x13 RID: 0x1f7 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x14 RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0x15 RID: 0x4b2 acb: 0x00000011 Account: ssh Name: (null) Desc: (null)
index: 0x16 RID: 0x1f5 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x17 RID: 0x40d acb: 0x00000011 Account: ssh Name: (null) Desc: (null)
index: 0x18 RID: 0x1f4 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x19 RID: 0x1f5 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)

[+] Attempting to get domain SID with command: nmblookup -A '172.17.0.2'

[*] Got domain/workgroup name: WORKGROUP

[+] Session check on 172.17.0.2

[*] Attempting to make null session using command: nmbclient -W WORKGROUP //172.17.0.2/(null)->?_info?Z=41

[*] Server 172.17.0.2 allows sessions using username '' password ''

[+] Getting domain SID for 172.17.0.2

[*] Attempting to get domain SID with command: nmbclient -W WORKGROUP //172.17.0.2/(null)->?_info?Z=41
```

El resultado de este comando puede generar varias pantallas de información si se detectan muchos usuarios. Enum4linux agrega la salida de varias herramientas de Samba para producir un resultado conciso. Si desea ver cómo se usa cada función, use la opción detallada (**-v**) con el comando.

- b. Enumere los recursos compartidos de archivos disponibles en 172.17.0.2 mediante el comando **enum4linux -S**. Utilice la opción detallada para ver las herramientas de Samba que se utilizan para obtener la información.

```
└─(root㉿kali)-[/home/kali]
└─# enum4linux -Sv 172.17.0.2
```

Observe la **[V]** al comienzo de algunas de las líneas de salida. El modo detallado proporciona una descripción de cómo se obtuvieron los resultados. Por ejemplo, en la sección **Enumeración de grupo de trabajo / dominio** de la salida, enum4linux intentó obtener el nombre de dominio con el comando: **nmblookup -A '172.17.0.2'**.

¿Qué herramienta de Samba se utilizó para asignar los recursos compartidos de archivos?

```
[root@kali:~/kali] enum4linux -Sv 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov  3 00:37:15 2025
Target ..... 172.17.0.2
RID Range ..... 500-550,1000-1050
Username ..... 
Password ..... 
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[+] Got domain/workgroup name: WORKGROUP

[+] Session check on 172.17.0.2

[*] Attempting to get domain name with command: nmblookup -A '172.17.0.2'

[*] Got domain/workgroup name: WORKGROUP

[+] Session check on 172.17.0.2

[*] Attempting to make null session using command: nmbclient -W WORKGROUP //172.17.0.2/(null)->?_info?Z=41

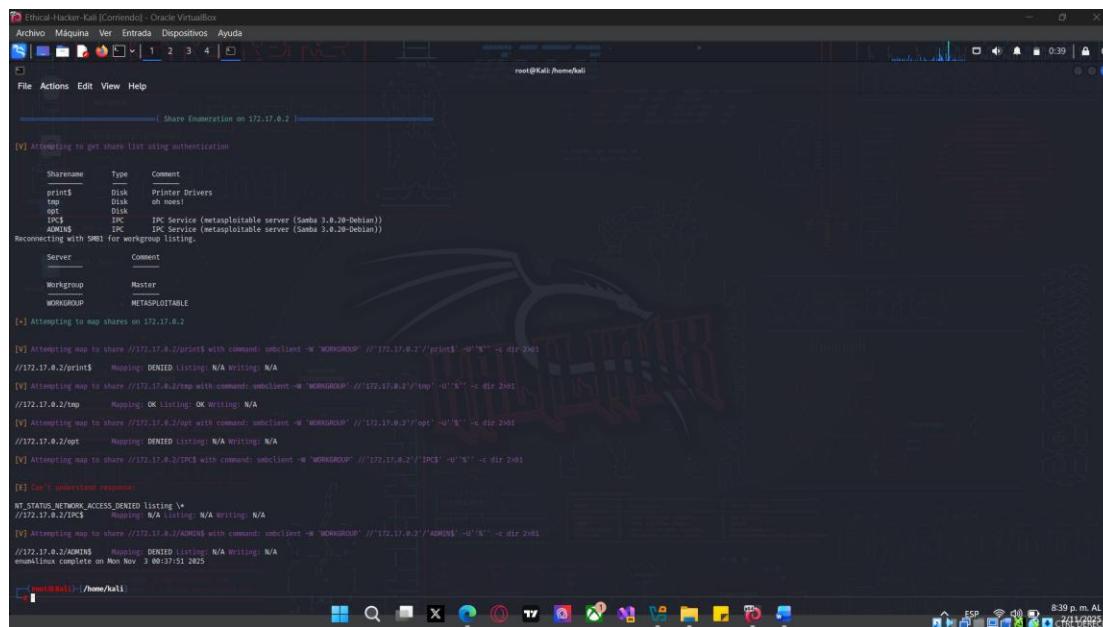
[*] Server 172.17.0.2 allows sessions using username '' password ''

[+] Getting domain SID for 172.17.0.2

[*] Attempting to get domain SID with command: nmbclient -W WORKGROUP //172.17.0.2/(null)->?_info?Z=41
```

smbclient

¿Cuántos recursos compartidos de archivos se enumeran para el destino 172.17.0.2? ¿Qué indica el \$ al final del nombre del recurso compartido? (Es posible que deba investigar esta respuesta).



```
[root@Kali ~]# smbclient -L 172.17.0.2 -U % -m Samba3.0.20-Debian -w WORKGROUP -d 2>&1
[+] Attempting to get share list using authentication.

[+] Share enumeration on 172.17.0.2

[+] Attempting to get share list using authentication.

[+] Share enumeration on 172.17.0.2

[+] Reconnecting with SMB1 for workgroup listing.

[+] Attempting to map shares on 172.17.0.2

[+] Attempting map to share //172.17.0.2/print$ with command: smbclient -W "WORKGROUP" //172.17.0.2//print$ -U "%" -c dir >2>&1
//172.17.0.2/print$  Mapping: DENIED Listing: N/A Writing: N/A
[+] Attempting map to share //172.17.0.2/tmp with command: smbclient -W "WORKGROUP" //172.17.0.2//tmp$ -U "%" -c dir >2>&1
//172.17.0.2/tmp$  Mapping: OK Listing: OK Writing: N/A
[+] Attempting map to share //172.17.0.2/IPC$ with command: smbclient -W "WORKGROUP" //172.17.0.2//IPC$ -U "%" -c dir >2>&1
//172.17.0.2/IPC$  Mapping: OK Listing: N/A Writing: N/A
[+] Attempting map to share //172.17.0.2/ADMIN$ with command: smbclient -W "WORKGROUP" //172.17.0.2//ADMIN$ -U "%" -c dir >2>&1
//172.17.0.2/ADMIN$  Mapping: DENIED Listing: N/A Writing: N/A
[+] Can't understand response: NT_STATUS_NETWORK_ACCESS_DENIED Listing: N/A
//172.17.0.2/IPC$  Mapping: N/A Listing: N/A Writing: N/A
[+] Attempting map to share //172.17.0.2/ADMIN$ with command: smbclient -W "WORKGROUP" //172.17.0.2//ADMIN$ -U "%" -c dir >2>&1
//172.17.0.2/ADMIN$  Mapping: DENIED Listing: N/A Writing: N/A
enum4linux complete on Mon Nov 3 00:37:51 2025
[+] (root@kali) - [/home/kali]
```

Se enumeran cinco recursos compartidos de archivos para 172.17.0.2. El \$ indica acciones ocultas.

- c. Es posible que los evaluadores de penetración no hayan descubierto una combinación conocida de nombre de usuario y contraseña para avanzar en su ataque. En este caso, deben realizar un ataque de contraseña por fuerza bruta para obtener las credenciales necesarias. Es un beneficio conocer las políticas de contraseñas vigentes en el sistema de destino para estructurar el esfuerzo de fuerza bruta. Utilice el comando **enum4linux -P** para enumerar las políticas de contraseñas.

```
[root@kali ~]# enum4linux -P 172.17.0.2
```

¿Cuál es la longitud mínima de contraseña establecida para las cuentas en este servidor? ¿Cuál es la configuración del umbral de bloqueo de la cuenta?

Práctica de laboratorio: Escaneo de vulnerabilidades SMB con enum4linux

```
root@Kali:~/home/kali# enum4linux -r 172.17.0.2 Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov 3 00:39:34 2025 ( Target Information ) Target ..... 172.17.0.2 RID Range ..... 500-550,1000-1050 Username ..... '' Password ..... Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none ( Enumerating Workgroup/Domain on 172.17.0.2 ) [+] Got domain/workgroup name: WORKGROUP ( Session Check on 172.17.0.2 ) [+] Server 172.17.0.2 allows sessions using username '', password '' ( Getting domain SID for 172.17.0.2 ) Domain Name: WORKGROUP Domain Sids: (NULL SID) [+] Can't determine if host is part of domain or part of a workgroup ( Password Policy Information for 172.17.0.2 ) [+] Attaching to 172.17.0.2 using a NULL share [+] Trying protocol 139/SMB... [+] Found domain(s): [+] METASPOITABLE [+] BuiltIn [+] Password Info for Domain: METASPOITABLE [+] Minimum password length: 5 [+] Password history length: None [+] Maximum password age: Not Set [+] Password Complexity Flags: 000000 [+] Domain Refuse Password Change: 0 [+] Domain Max Password Age: 0 [+] Domain Password Lockout Admins: 0 [+] Domain Password No Clear Changes: 0 [+] Domain Password Store Cleartext: 0 [+] Domain Password Complex: 0 [+] Minimum password age: None [+] Reset Account Lockout Counter: 30 minutes [+] Locked Account Lockout Duration: 30 Minutes [+] Domain Account Lockout Threshold: 0 [+] Forced Log off Time: Not Set [+] Retrieved partial password policy with rpyclient: Password Complexity: Disabled Minimum Password Length: 0 enum4linux complete on Mon Nov 3 00:39:34 2025
```

La longitud mínima de la contraseña es de cinco caracteres y no se establece ningún umbral de bloqueo de cuenta.

¿Cómo calificaría la seguridad de la política de contraseñas establecida para este dominio? ¿Baja, media o alta? Explique.

Baja La longitud mínima de la contraseña es demasiado corta. Además, el indicador de complejidad de la contraseña es 000000. Microsoft documenta este valor en el sentido de que no se establece ninguna política de complejidad de contraseñas. Además, no se configura una antigüedad mínima de la contraseña.

```
root@Kali:~/home/kali# enum4linux -r 172.17.0.2 Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov 3 00:39:34 2025 ( Target Information ) Target ..... 172.17.0.2 RID Range ..... 500-550,1000-1050 Username ..... '' Password ..... Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none ( Enumerating Workgroup/Domain on 172.17.0.2 ) [+] Got domain/workgroup name: WORKGROUP ( Session Check on 172.17.0.2 ) [+] Server 172.17.0.2 allows sessions using username '', password '' ( Getting domain SID for 172.17.0.2 ) Domain Name: WORKGROUP Domain Sids: (NULL SID) [+] Can't determine if host is part of domain or part of a workgroup ( Password Policy Information for 172.17.0.2 ) [+] Attaching to 172.17.0.2 using a NULL share [+] Trying protocol 139/SMB... [+] Found domain(s): [+] METASPOITABLE [+] BuiltIn [+] Password Info for Domain: METASPOITABLE [+] Minimum password length: 5 [+] Password history length: None [+] Maximum password age: Not Set [+] Password Complexity Flags: 000000 [+] Domain Refuse Password Change: 0 [+] Domain Max Password Age: 0 [+] Domain Password Lockout Admins: 0 [+] Domain Password No Clear Changes: 0 [+] Domain Password Store Cleartext: 0 [+] Domain Password Complex: 0 [+] Minimum password age: None [+] Reset Account Lockout Counter: 30 minutes [+] Locked Account Lockout Duration: 30 Minutes [+] Domain Account Lockout Threshold: 0 [+] Forced Log off Time: Not Set [+] Retrieved partial password policy with rpyclient: Password Complexity: Disabled Minimum Password Length: 0 enum4linux complete on Mon Nov 3 00:39:34 2025
```

Paso 2: Realizar un escaneo de enumeración simple en el destino 10.6.6.23.

Enum4linux tiene una opción que combina las opciones -U, -S, -G, -P, -r, -o, -n, -i en un solo comando. Esto requiere el uso del argumento **-a**. Esta opción realiza rápidamente varias operaciones de enumeración de SMB en un escaneo.

Use el comando **enum4linux -a** para realizar un escaneo en el posible destino del servidor Samba que identificó en la parte 2.

```
└── (root㉿kali) - [/home/kali]
    └── # enum4linux -a 10.6.6.23
```

Este comando puede producir varias pantallas de salida.

¿Cuántos usuarios y grupos locales hay en el objetivo 10.6.6.23?

3 usuarios locales y 7 grupos.

¿Cuáles son los recursos compartidos ubicados en este destino?

Los recursos compartidos son homes, workfiles y print\$. Tenga en cuenta que el recurso compartido de IPC \$ es para el proceso del servidor. Se crea de manera predeterminada.

```
root@Kali:~# enum4linux -a 10.6.6.23
Starting enum4linux v0.6.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov 3 00:41:41 2025
Target .....: 10.6.6.23
RID Range ....: 500-550,1000-1050
Username .....: .
Password .....: .
Known Usernames ..: administrator, guest, krbtgt, domain admins, root, bin, none

Enumerating Workgroup/Domain on 10.6.6.23

[!] Can't find workgroup/domain

[!] Netstat Information for 10.6.6.23

Looking up status of 10.6.6.23
No reply from 10.6.6.23

Session Check on 10.6.6.23

[*] Server 10.6.6.23 allows sessions using username '', password ''
[*] Getting domain SID for 10.6.6.23

Domain Name: WORKGROUP
Domain SID: (NULL SID)

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

OS Information on 10.6.6.23

[!] Can't get OS info with wmiclient

[*] Got domain for 10.6.6.23 from service:
        GRAVENING   Wk Sv Prc Dm NT DNT Samba 4.9.5-Debian
        platform_id : 500
        os version  : 6.1
        server type : 6+0x9a03

Users on 10.6.6.23
```

Práctica de laboratorio: Escaneo de vulnerabilidades SMB con enum4linux

```
Ethical-Hacker-Kali [Contenido] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit View Help
Sharename Type Comment
homes Disk All home directories
workfiles Disk Confidential Workfiles
print$ Disk Printer Drivers
IPC$ IPC IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
[+] Attempting to map shares on 10.6.6.23

[E] Can't understand response:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
//10.6.6.23\homes Mapping: N/A Listing: N/A Writing: N/A
//10.6.6.23\workfiles Mapping: OK Listing: OK Writing: N/A
//10.6.6.23\print$ Mapping: OK Listing: OK Writing: N/A
[E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing: N/A
//10.6.6.23\IPC$ Mapping: N/A Listing: N/A Writing: N/A
[+] Password Policy Information for 10.6.6.23

[+] Attaching to 10.6.6.23 using a NULL share
[+] Trying protocol 199/SMB...
[+] Found domain(s):
    [*] GRAVEMIND
    [*] BuiltIn
[+] Password Info for Domain: GRAVEMIND
    [*] Minimum password length: 5
    [*] Password history length: None
    [*] Maximum password age: 37 days 6 hours 21 minutes
    [*] Password Complexity Flags: 0x000000
        [*] Domain In Active Password Change: 0
        [*] Domain Password Store Cleartext: 0
root@Kali:~/home/kali
8:43 p.m. AL 8:43 p.m. AL
ESP WiFi 3 11/20/2025 CTR LERCHA

[+] Ethical-Hacker-Kali [Contenido] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit View Help
[+] Getting domain group memberships:
[+] Users on 10.6.6.23 via RID cycling (RID: 500-550,1000-1050)

[!] Found new SID: S-1-5-22-1
[!] Found new SID: S-1-5-32
[+] 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-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-547 BUILTIN\Guest User (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-1-22-1 and logon username "", password ""
S-1-22-1-1000 Unix User\masterchief (Local User)
S-1-22-1-1001 Unix User\arbitr (Local User)
S-1-22-1-1002 Unix User\tibusser (Local User)
[+] Enumerating users using SID S-1-5-21-3000196717-3701885971-2094638862 and logon username "", password ""
S-1-5-21-3000196717-3701885971-2094620862-501 GRAVEMIND\nobody (Local User)
S-1-5-21-3000196717-3701885971-2094620862-502 GRAVEMIND\nobody (Local User)
S-1-5-21-3000196717-3701885971-2094620862-1000 GRAVEMIND\masterchief (Local User)
S-1-5-21-3000196717-3701885971-2094620862-1001 GRAVEMIND\arbitr (Local User)
[+] Getting printer info for 10.6.6.23

No printers returned.

enum4linux complete on Mon Nov  3 08:42:23 2025
/home/kali
root@Kali:~/home/kali
8:43 p.m. AL 8:43 p.m. AL
ESP WiFi 3 11/20/2025 CTR LERCHA
```