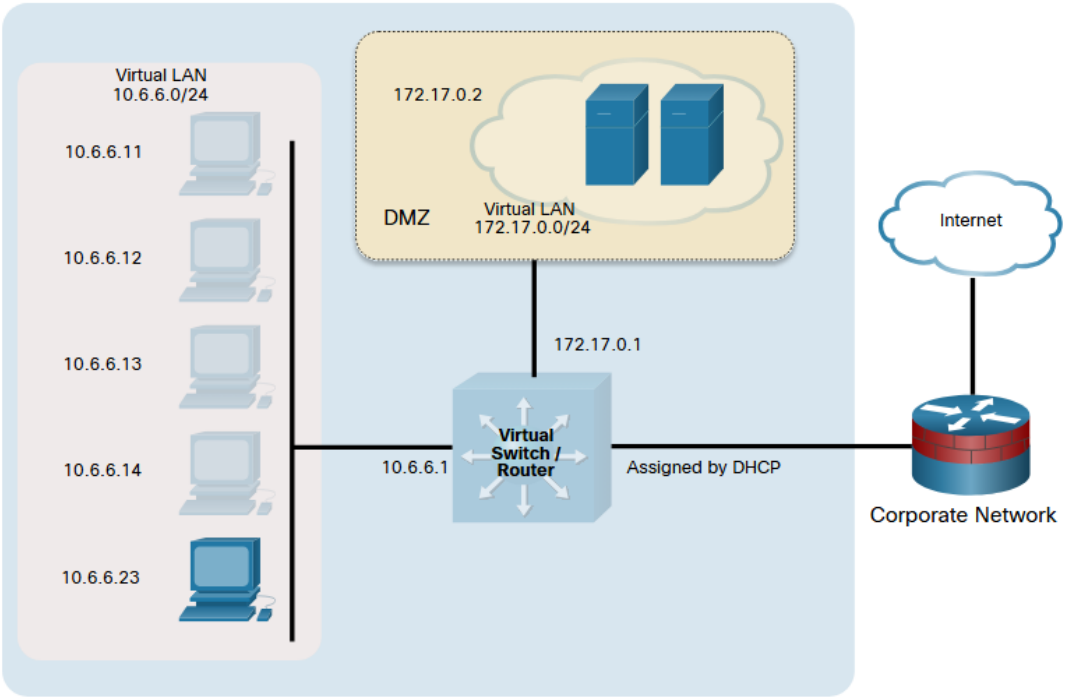
Módulo 5 – Explotación de vulnerabilidades basadas en la red:

Práctica de laboratorio - Análisis en busca de vulnerabilidades de SMB con enum4linux

Contenido

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.
- Usar enum4linux para enumerar usuarios y recursos compartidos de archivos de red.
- Utilizar smbclient para transferir archivos entre sistemas.

Trasfondo / Escenario

Las redes de servidores de Windows mal administradas y protegidas son un gran riesgo para la seguridad. Los pentesters 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, así que 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?

Respuesta: Dependancy info: You will need to have the samba package installed as this script is basically just a wrapper around ***rpcclient***, ***net***, ***nmblookup*** and ***smbclient***. Polenum from http://labs.portcullis.co.uk/application/polenum/ is required to get Password Policy info.

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) => RID (Relative Identifier) es un identificador único dentro de un SID (Security Identifier) en Windows, que distingue a usuarios, grupos o equipos dentro de un dominio

Identificador de seguridad (SID) => SID (Security Identifier) es un código único que Windows asigna a cada usuario, grupo o proceso para identificarlo dentro del sistema.

Controlador de dominio (DC) => Controlador de dominio (DC) es un servidor que gestiona la autenticación y permisos en una red basada en dominio.

Protocolo de acceso al directorio ligero (LDAP) => LDAP (Lightweight Directory Access Protocol) es un protocolo que permite acceder y gestionar información en servicios de directorio, como usuarios, permisos y recursos de red.

Grupo de trabajo => un grupo de equipos independientes que se administran de forma independiente.

Parte 2: Uso de Nmap para buscar servidores SMB.

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

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.

Puertos abiertos más comunes en SMB:

• ***TCP 135 RPC**:* **R**emote **P**rocedure **C**all (Llamada a Procedimiento Remoto), permite que un cliente ejecute un procedimiento o función en un servidor como si lo estuviera haciendo local. Es muy usado en entornos Windows para la comunicación de servicios, aplicaciones y sistemas operativos. Active Directory y la Administración Remota de Windows dependen de RPC.

Este puerto abierto significa la presencia de un sistema Windows y el punto de partida para la enumeración de usuarios y servicios. También es muy usado para pivoting y ejecución de comandos a través del servicio Servicio de Acceso a Directorio (Directory Access Service).

• ***TCP 139 Sesión de NetBIOS**:* Es una API que permite la comunicación entre aplicaciones en una red local. Permite la gestión de nombres, datagramas y sesiones. Este puerto se usa para establecer una sesión entre dos dispositivos con NetBIOS. Antiguamente este protocolo se ejecutaba sobre SMB para compartir recursos e impresoras si no se conectaba por el puerto 445 de SMB. Este puerto se usa en sistemas Legacy porque actualmente, los nuevos dispositivos usan el 445.

• ***TCP 389 Servidor LDAP**:* Es un protocolo que funciona como una base de datos centralizada que almacena y organiza información sobre usuarios, grupos, dispositivos, y otros recursos de red. Su función principal es brindar un servicio de directorio, incluyendo => autenticación, para verificar la identidad de un usuario (cuando nos logueamos, las credenciales se autentican con un servidor LDAP), autorización, para determinar los límites de acceso, y almacenamiento de información, para guardar nombres de usuario, contraseñas, direcciones de correo electrónico y más. Por estas razones es muy utilizado en Active Directory. Este puerto es el estándar sin cifrar, el estándar seguro es el TCP 636 (LDAPS) que usa TLS/SSL. Este puerto es ideal para la enumeración de usuarios y grupos.

• ***TCP 445 Servicio de archivos SMB**:* Protocolo de Windows para compartir archivos, impresoras y otros recursos de red entre dispositivos en una red. Actualmente, el tráfico SMB pasa por este puerto. Una funcionalidad muy importante es que posee **IPC$**, **I**nter-**P**rocess **C**ommunication, un recurso compartido oculto y predeterminado que utiliza pipes con nombre (named pipes) para la comunicación entre programas y servicios en la red.

La vulnerabilidad más conocida para este protocolo es **EternalBlue** (ejecución de código remoto) => que en sistemas no parcheados fue aprovechada por **WannaCry** y **NotPetya.** Además, la falta de firmas en este protocolo puede hacer que las máquinas sean vulnerables a ataques de retransmisión de credenciales (SMB Relay), donde un atacante intercepta y reenvía los hashes de autenticación para desencriptarlos offline.

Otra vulnerabilidad es el **Credential Dumping**, donde las credenciales de usuarios se pueden extraer de sistemas comprometidos usando herramientas que interactúan con SMB.

• ***TCP 9389 Servicios web de Active Directory****:* Active Directory Web Services (ADWS), es un protocolo que proporciona una interfaz de servicio web (SOAP) para acceder y gestionar dominios de Active Directory. Permite que las aplicaciones de administración y los scripts (especialmente PowerShell) se comuniquen con AD de una forma mucho más flexible, en lugar de usar solo LDAP o RPC. La comunicación se realiza de manera segura sobre HTTPS, puede ser ideal para pivoting por el hecho de permitir la administración remota.

• ***TCP/ UDP 137 Servicio de nombres NetBIOS****:* Es el protocolo que se encarga de la resolución de nombres en redes que aún dependen de NetBIOS. Su función es similar a la de un DNS, pero para nombres NetBIOS, permite que los sistemas encuentren otros dispositivos en la red usando sus nombres (ej. PC-OFICINA), en lugar de sus direcciones IP. Usa TCP para el registro y renovación de nombres, como UDP para las consultas de nombres. Actualmente fue reemplazado por DNS, aunque en sistemas Legacy aún se sigue usando.

• ***UDP 138 Datagrama de NetBIOS***: Protocolo que no establece y confirma una conexión, a diferencia del TCP Sesión NetBIOS. No garantiza la entrega del mensaje (una conexión típica UDP). Se usa principalmente para mensajes de difusión:

a_ Qué otros recursos y computadoras están disponibles en la red local, es el protocolo detrás de la lista de equipos que aparece en "Red" o "Entorno de red" de Windows.

b_ Los "Master Browsers" (servidores que mantienen la lista de recursos compartidos de la red) usan este puerto para anunciar su presencia y para que otros equipos se registren con ellos.

C_ Envío de mensajes cortos a una máquina específica o a un grupo.

Este protocolo ayuda a => Enumerar Hostnames (nombres de las computadoras activas en una red), Identificar Roles (si es un Master Browser por ejemplo) y realizar Ataques de Información (usando fugas de información a través de datagramas mal configurados o vulnerabilidades que permitan la interceptación de estos paquetes).

Aunque hoy en día la mayoría de las redes modernas dependen más de DNS y SMB directo en 445, el puerto UDP 138 sigue siendo un indicador de sistemas Windows (o Samba) y una fuente de información de red en entornos donde la compatibilidad NetBIOS aún se mantiene.

a. Se incluyen dos redes virtuales en la VM de Kali con contenedores de Docker. Utilice el comando **nmap -sN** para encontrar 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?

Respuesta:

```
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-10 16:11 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000030s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap scan report for 172.17.0.1
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.76 seconds
```

Solo el host 172.17.0.2 nos serviría.

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

Respuesta: ***TCP 139 netbios-ssn*** y ***TCP 445 microsoft-ds***. (puertos vistos anteriormente)

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

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sN 10.6.6.0/24
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-10 16:17 UTC
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0000030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE         SERVICE
8080/tcp open|filtered http-proxy
8888/tcp open|filtered sun-answerbook
9001/tcp open|filtered tor-orport
MAC Address: 02:42:0A:06:06:0B (Unknown)

Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE         SERVICE
3000/tcp open|filtered ppp
MAC Address: 02:42:0A:06:06:0C (Unknown)

Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.0000030s latency).
All 1000 scanned ports on dvwa.vm (10.6.6.13) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:42:0A:06:06:0D (Unknown)

Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.0000030s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE         SERVICE
80/tcp   open|filtered http
3306/tcp open|filtered mysql
MAC Address: 02:42:0A:06:06:0E (Unknown)

Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0000030s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE         SERVICE
21/tcp  open|filtered ftp
22/tcp  open|filtered ssh
53/tcp  open|filtered domain
80/tcp  open|filtered http
139/tcp open|filtered netbios-ssn
445/tcp open|filtered microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)

Nmap scan report for 10.6.6.100
```

```
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 256 IP addresses (7 hosts up) scanned in 4.65 seconds
```

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

Respuesta: Sí, el host 10.6.6.23 porque 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 objetivo 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

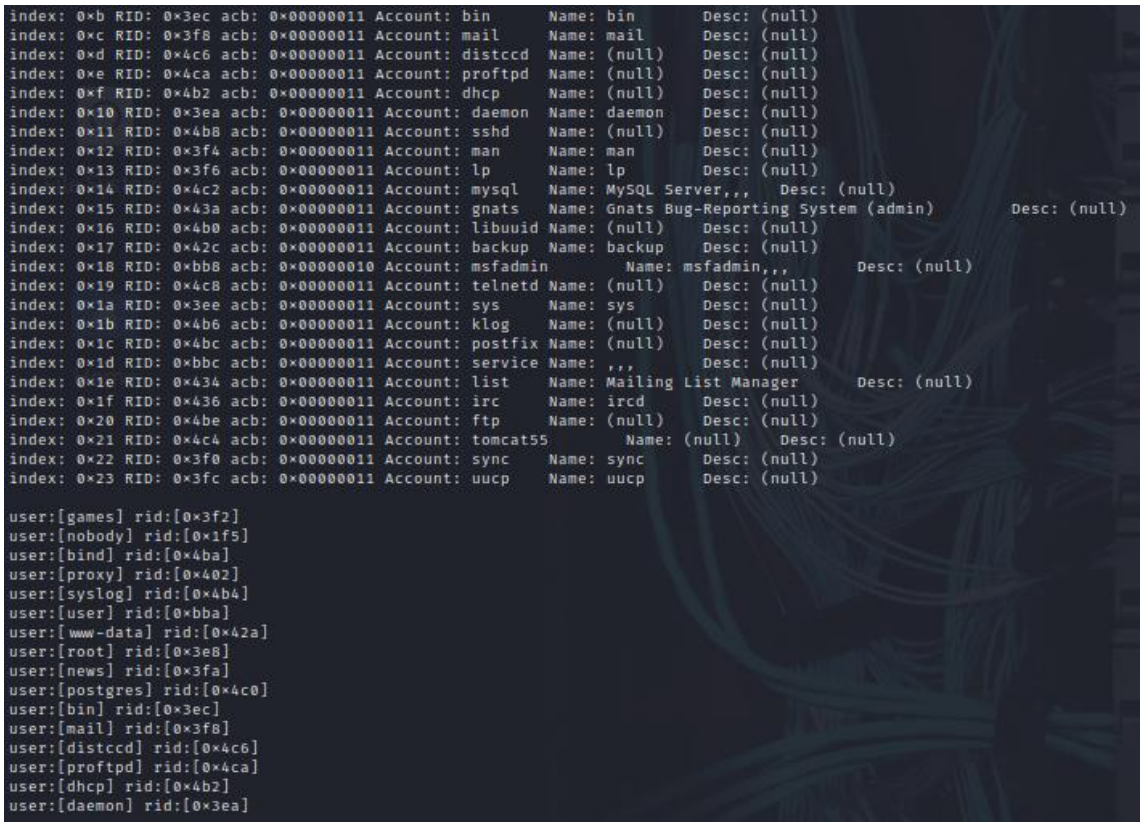
-P enumera las políticas de contraseñas

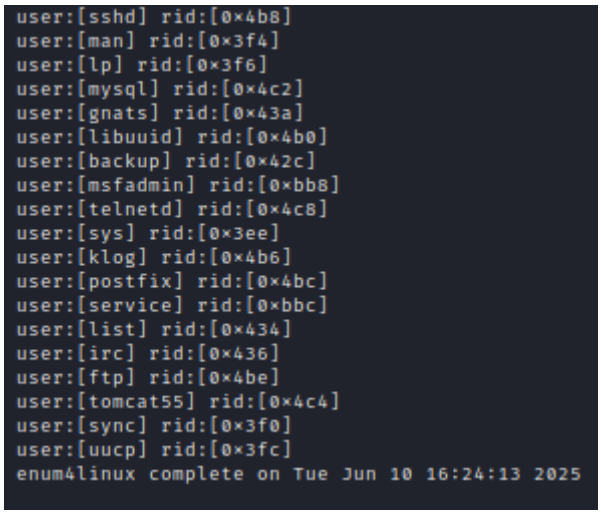
-i obtiene una lista de impresoras

a. 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
```

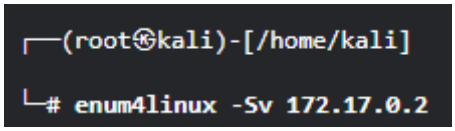
```
 ========================( Target Information )=========================

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 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: 0x4ba acb: 0x00000011 Account: bind     Name: (null)    Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy    Name: proxy     Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog   Name: (null)    Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data  Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root     Name: root      Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news     Name: news      Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,,      Desc: (null)
```



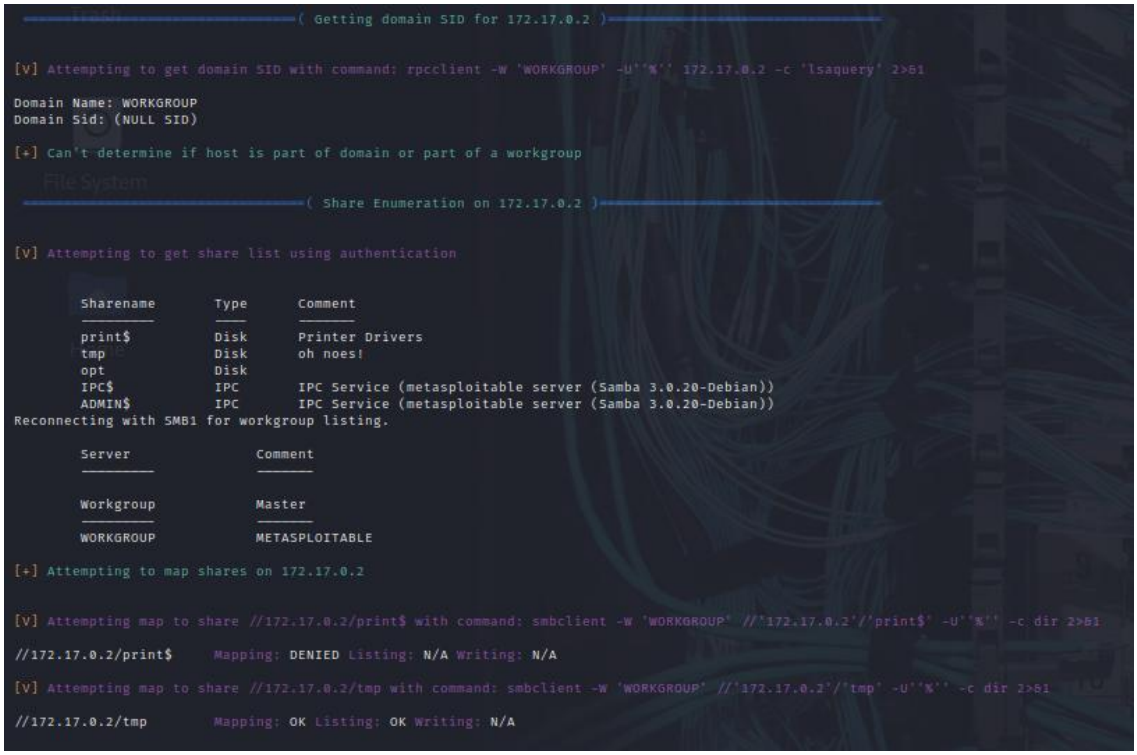


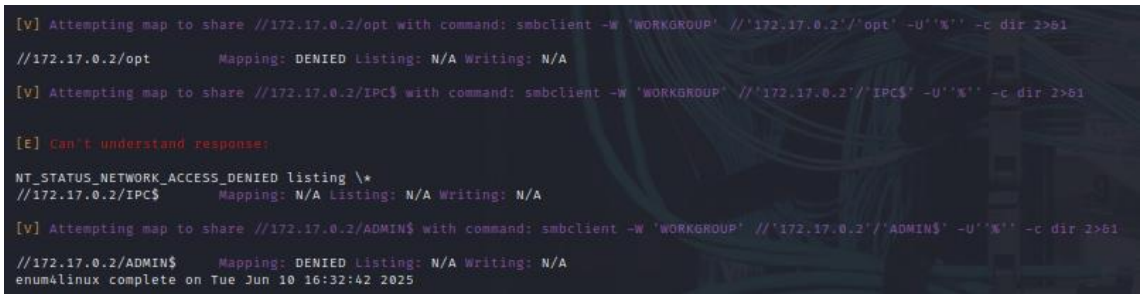
El resultado de este comando puede generar varias pantallas de información si se detectan muchos usuarios. Enum4linux agrega la salida de varias herramientas de Samba para producir un resultado conciso. Si desea ver cómo se usa cada función, use la opción detallada (**-v**) con el comando.

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.



Observe **[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 **Enumerating Workgroup/Domain** (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'**.





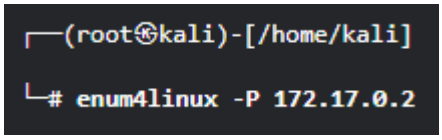
¿Qué herramienta de Samba se utilizó para asignar los recursos compartidos de archivos?

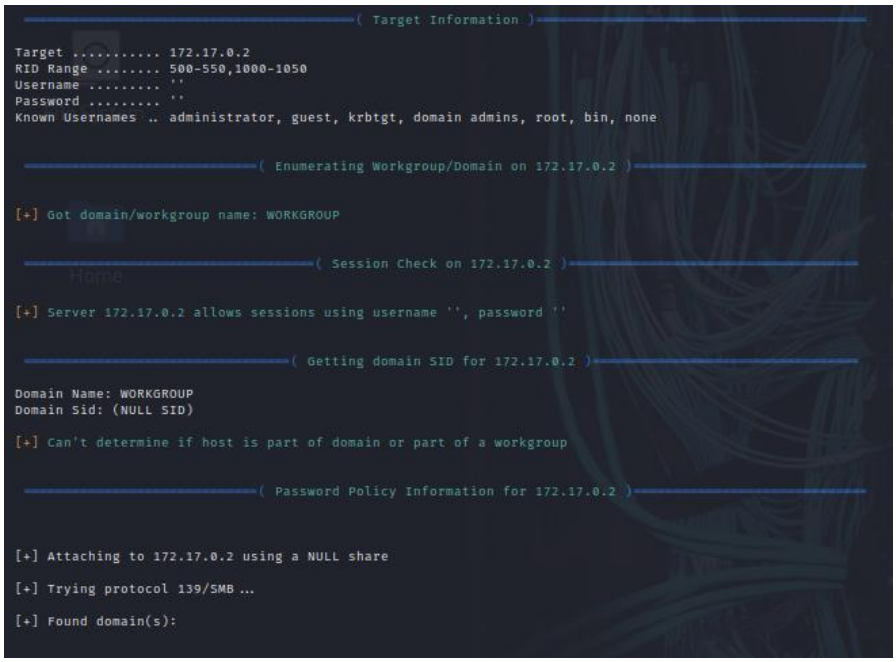
Respuesta: smbclient.

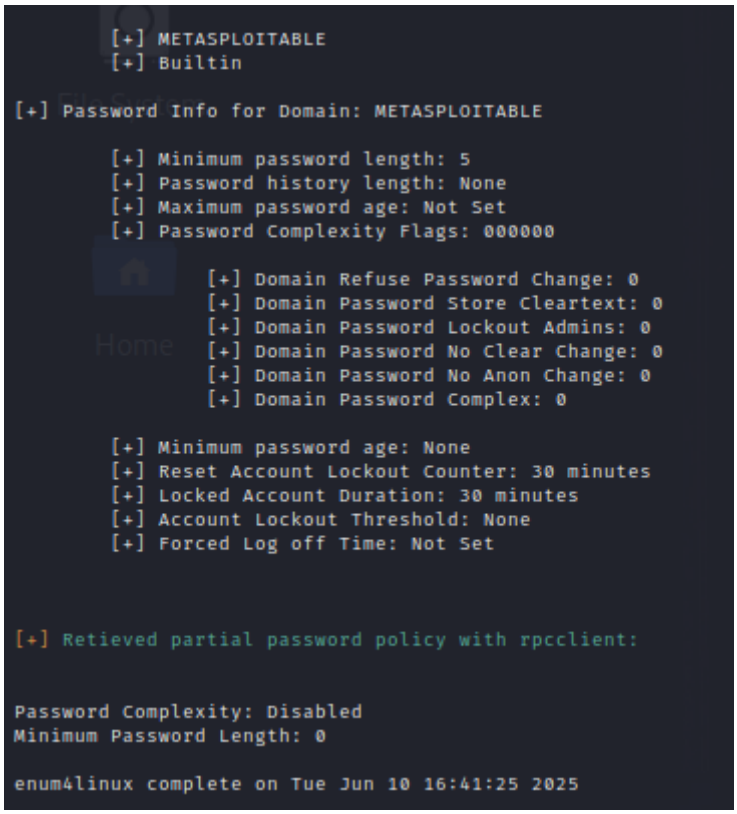
¿Cuántos recursos compartidos de archivos se enumeran para el objetivo 172.17.0.2? ¿Qué indica el $ al final del nombre del recurso compartido? (Es posible que deba investigar esta respuesta).

Respuesta: Se numeraron cinco recursos compartidos (print$, tmp, opt, IPC$ y ADMIN$). El signo $ al final significa que son archivos ocultos.

c. Es posible que los pentesters 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.







¿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?

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

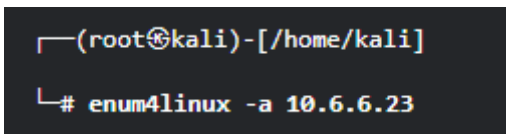
¿Cómo calificaría la seguridad de la política de contraseñas establecida para este dominio? ¿Baja, media o alta? Explique.

Respuesta: Baja, porque la longitud mínima es demasiado pequeña y el indicar de complejidad indica que está en 0 (**000000**); este valor indica que no hay política de complejidad de contraseña y tampoco hay antigüedad de contraseña establecida.

Paso 2: Realice un escaneo de enumeración simple en el objetivo 10.6.6.23.

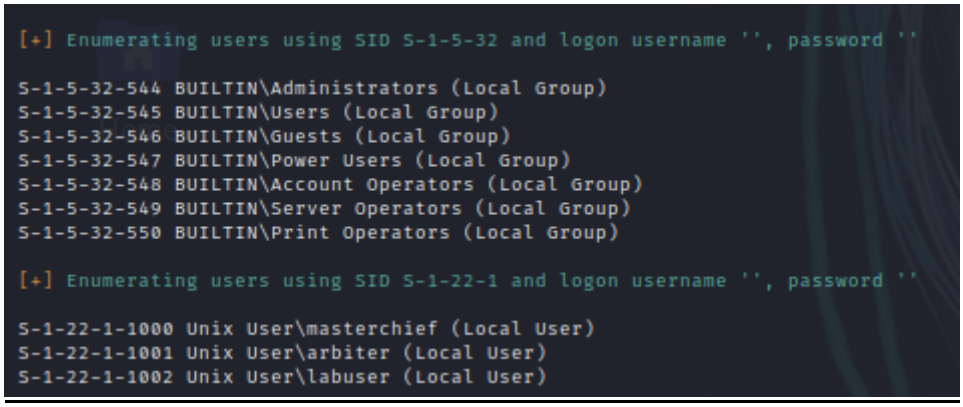
Enum4linux tiene una opción que combina las opciones -U, -S, -G, -P, -r, -o, -n, -i en un solo comando. Esto requiere el uso del argumento **-a**. Esta opción realiza rápidamente varias operaciones de enumeración de SMB en un escaneo.

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



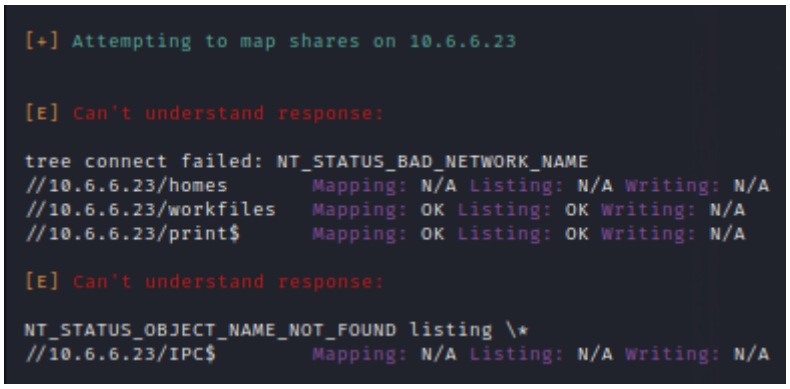
Este comando puede producir varias pantallas de salida.

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



Respuesta: Hay 7 grupos y 3 usuarios locales.

¿Cuáles son los recursos compartidos que se encuentran en este objetivo?



Respuesta: Hay 3 recursos compartidos (**homes, workfiles y print$**), IPC$ es un proceso especial, creado por el servidor de forma predeterminada.

Parte 4: Use smbclient para transferir archivos entre sistemas.

Smbclient es un componente de Samba que puede almacenar y recuperar archivos, de manera similar a un cliente FTP. Utilizará smbclient para transferir un archivo al sistema de destino en 172.17.0.2. Esto simula la explotación de un host de red con malware a través de una vulnerabilidad de SMB.

a. Cree un archivo de texto con el comando **cat**. Nombre el archivo **badfile.txt**. Ingrese el texto deseado. En este ejemplo, se utilizó **This is a bad file.** Asegúrese de conocer la ruta al archivo. Presione **CTRL-C** cuando haya terminado.

```
┌──(root㉿kali)-[/home/kali]
└─# cat >> badfile.txt

This is a bad file.

Press CRTL-C to write the file.
```

b. Observe las opciones disponibles con smbclient mediante el comando **smbclient –help**.

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

c. Utilice el comando **smbclient -L** para enumerar los recursos compartidos en el host de destino. Este comando produce un resultado similar al que hizo el comando enum4linx en la parte 3. Cuando se le solicite una contraseña, presione Intro. El carácter doble / antes de la dirección IP y / son necesarios si el destino es una computadora con Windows.

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient -L //172.17.0.2/

Password for [WORKGROUPkali]: <Press enter>
```

```
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

d. Conéctese al recurso compartido **tmp** mediante el comando **smbclient** especificando el nombre del recurso compartido y la dirección IP.

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //172.17.0.2/tmp

Password for [WORKGROUPkali]: <Press enter>

smb: >
```

Tenga en cuenta que el indicador cambió a **smb: >**. Escriba **help** para ver qué comandos están disponibles.

```
                38497656 blocks of size 1024. 9357760 blocks available
smb: \> help
?              allinfo         altname         archive         backup
blocksize      cancel          case_sensitive  cd              chmod
chown          close           del             deltree         dir
du             echo            exit            get             getfacl
geteas         hardlink        help            history         iosize
lcd            link            lock            lowercase       ls
l              mask            md              mget            mkdir
more           mput            newer           notify          open
posix          posix_encrypt   posix_open      posix_mkdir     posix_rmdir
posix_unlink   posix_whoami    print           prompt          put
pwd            q               queue           quit            readlink
rd             recurse         reget           rename          reput
rm             rmdir           showacls        setea           setmode
scopy          stat            symlink         tar             tarmode
timeout        translate       unlock          volume          vuid
wdel           logon           listconnect     showconnect     tcon
tdis           tid             utimes          logoff          ..
!
smb: \>
```

e. Introduzca **dir** para ver el contenido del recurso compartido.

f. Cargue **badfile.txt** al servidor de destino mediante el comando **put**. La sintaxis del comando es:

```
 put local-file-name remote-file-name

smb: > put badfile.txt badfile.txt

Putting file badfile.txt as badfile.txt (19.5 kb/s) (average 19.5 kb/s)
```

g. Verifique que el archivo se haya cargado correctamente con el comando **dir - ls**.

```
smb: \> put badfile.txt badfile.txt
putting file badfile.txt as \badfile.txt (8.8 kb/s) (average 8.8 kb/s)
```

```
smb: \> ls
  .                                   D        0  Tue Jun 10 17:34:22 2025
  ..                                 DR        0  Mon Aug 14 09:39:59 2023
  .X11-unix                          DH        0  Mon Aug 14 09:35:14 2023
  .ICE-unix                          DH        0  Sun Jan 28 02:08:08 2018
  .X0-lock                           HR       11  Mon Aug 14 09:35:14 2023
  682.jsvc_up                         R        0  Mon Aug 14 09:35:26 2023
  badfile.txt                         A        9  Tue Jun 10 17:34:22 2025
  726.jsvc_up                         R        0  Tue Jun 10 04:08:59 2025
  826.jsvc_up                         R        0  Sun Jan 28 06:08:40 2018
  810.jsvc_up                         R        0  Sun Jan 28 02:54:31 2018
  1582.jsvc_up                        R        0  Sun Jan 28 03:01:49 2018
  1823.jsvc_up                        R        0  Sun Jan 28 01:57:44 2018
```

h. Escriba **quit** para salir de **smbclient** y volver al indicador de la CLI.

Reflexión

Está realizando un pentest de la red de un cliente. Ha obtenido acceso a una red interna mediante ingeniería social con el nombre de usuario y la contraseña de un servidor web ***ad hoc*** que no está detrás del cortafuego. Puede acceder de forma remota a la red desde una VM Kali configurada con la herramienta enum4linux.

¿Qué pasos seguiría para enviar un archivo de malware ficticio a los hosts de la red como parte de la prueba de penetración?

Respuesta:

1. Escanear la red con Nmap para identificar hosts que ejecutan SMB.

2. Escanear el host objetivo o la subred del host con enum4linux para enumerar los grupos de trabajo, las políticas de contraseñas y los recursos compartidos.

3. Ejecutar ***smbclient*** y usar el comando ***put*** para copiar el archivo ficticio en uno o varios hosts vulnerables.